

NAVAL COMMUNICATIONS SECURITY MATERIAL SYSTEM



EKMS-3E

**COMMUNICATIONS SECURITY (COMSEC) MATERIAL
SYSTEM (CMS) CENTRAL OFFICE OF RECORD (COR)
AUDIT MANUAL**

08 May 2017

DEPARTMENT OF THE NAVY
COMMUNICATION SECURITY MATERIAL SYSTEM

IN REPLY REFER TO:
5040
Ser N7/

LETTER OF PROMULGATION

1. **PURPOSE.** To promulgate guidance for use in the conduct of Central Office of Record (COR) Audits on COMSEC accounts within the Department of the Navy. The guidance in this manual is based on policy and procedures set forth in both National and Navy COMSEC publications.
2. **ACTION.** EKMS-3E is effective upon receipt and supersedes EKMS-3D dated 06 Feb 2015.
3. **REPRODUCTION.** EKMS-3E is authorized for reproduction, distribution and use in any operational environment and is available via the NCMS SIPRNET Collaboration at-Sea (CAS) website located at:
<http://www.uar.cas.navy.smil.mil/secret/navy/39/site.nsf>.
This manual is also available via NIPR on the INFOSEC website located at: <https://infosec.navy.mil>
4. **COMMENTS.** Submit comments, recommendations, and suggestions for changes to, Naval Communications Security Material System (NCMS) N7/N5.

J. A. LECOUNTE

LIST OF EFFECTIVE PAGES

	<u>PAGE NUMBER</u>	
Front Cover	(unnumbered)	ORIGINAL
Letter of Promulgation	i	ORIGINAL
List of Effective Pages	ii	ORIGINAL
Record of Amendments	iii	ORIGINAL
Record of Page Checks	iv	ORIGINAL
<u>Table of Contents</u>	v-vi	ORIGINAL
<u>Chapter 1</u>	1-1 thru 1-2	ORIGINAL
<u>Chapter 2</u>	2-1 thru 2-4	ORIGINAL
<u>Chapter 3</u>	3-1 thru 3-2	ORIGINAL
<u>Chapter 4</u>	4-1 thru 4-2	ORIGINAL
<u>(Annex A)</u>	A-1 thru A-52	ORIGINAL
<u>(Annex B)</u>	B-1 thru B-26	ORIGINAL
<u>(Annex C)</u>	C-1 thru C-4	ORIGINAL
<u>(Annex D)</u>	D-1 thru D-5	ORIGINAL
<u>(Annex E)</u>	E-1 thru E-2	ORIGINAL
<u>(Annex F)</u>	F-1	ORIGINAL
<u>(Annex G)</u>	G-1	ORIGINAL
Back Cover (Reverse Blank)	(unnumbered)	ORIGINAL

TABLE OF CONTENTS

**CHAPTER 1 - INTRODUCTION TO THE COMSEC MATERIAL SYSTEM (CMS)
CENTRAL OFFICE OF RECORD (COR) AUDIT PROGRAM**

101. Purpose

105. Scope and Application

- a. Source
- b. Scope
- c. Application
- d. Recommendations

110. Definitions

- a. Audit
- b. Client Platform Administrator (CPA)
- c. Client Platform Security Officer (CPSO)
- d. COR Audit Training/Pre-Audit Visit
- e. Communications Security (COMSEC)
- f. Electronic Key Management System (EKMS)
- g. Key Management Infrastructure (KMI)
- h. Key Management Infrastructure Operating Account (KOA)
- i. KMI Account Manager (KOAM)
- j. Physical Security Inspection
- k. Physical Security Survey (PSS)

115. Responsibility

- a. Naval Communications Security Material System (NCMS)
- b. Immediate Superior in Command/Immediate Unit
Commander (ISIC/IUC)
- c. EKMS/KOA Auditor

CHAPTER 2 - CMS COR AUDIT POLICY AND PROCEDURES

201. General Policy

205. CMS COR Audit Process

- a. CMS COR Audit
- b. Pre-audit Guidelines
- c. Approval of COMSEC Facilities
- d. Evaluation Criteria
- e. Re-audit

CHAPTER 3 - ASSIGNMENT OF CMS COR AUDITORS

301. Designation Requirements for CMS COR Auditors

305. Designation Guidelines

CHAPTER 4 - CMS COR AUDIT REPORTING PROCEDURES

401. Content and Submission Guidelines

405. EKMS/KOA Feedback Report

410. Privileged Nature of Audit Reports

LIST OF ANNEXES

ANNEX A: CMS COR AUDIT GUIDE, ACCOUNT MANAGER

ANNEX B: CMS COR AUDIT GUIDE, LOCAL ELEMENT

ANNEX C: VAULT INSPECTION GUIDE

ANNEX D: FIXED COMSEC FACILITIES INSPECTION GUIDE

ANNEX E: CMS COR AUDIT REPORT (EXAMPLE)

ANNEX F: CMS COR AUDIT FEEDBACK REPORT (EXAMPLE)

ANNEX G: ISIC/IUC EKMS/KOA AUDIT ENDORSEMENT (EXAMPLE)

**CHAPTER 1 - INTRODUCTION TO THE
COMSEC MATERIAL SYSTEM (CMS) CENTRAL OFFICE OF RECORD (COR)
AUDIT PROGRAM**

101. **PURPOSE.** The guidance contained herein is intended to be used as the official criteria for the conduct of COR audits at COMSEC accounts within the Department of the Navy (DON), including U.S. Navy, Military Sealift Command (MSC), U. S. Marine Corps (USMC), Coast Guard (USCG), and contracted support personnel.

Where reflected, the term COMSEC Account Manager (CAM) or "Manager" refers to either an EKMS Manager or KOAM. Questions in Annex A which are program specific (EKMS or KMI) are so identified.

105. **APPLICABILITY:**

a. **Applicability.** The requirements in this manual apply to DON (MSC, USCG, USMC, and USN) COMSEC accounts and ISIC/IUCs whose subordinate activities handle, distribute, account for, store or use COMSEC material, maintain a numbered COMSEC account and supported Local Elements (LE). Additional requirements may be imposed by the Commandant of the Marine Corps (CMC C4/CY), Coast Guard (USCG) C4ITSC, Fleet Commanders (FLTCDRS), Type Commanders (TYCOM), and Immediate Superiors in Command/Immediate Unit Commanders (ISIC/IUC) applicable to supported commands, units and activities.

b. **Recommendations.** Recommended changes to this manual will be submitted to the Naval Communications Security Material System (NCMS) Policy and Procedures Department (N5) and CMS Education & Training Department (N7), via the administrative chain of command.

110. **PHYSICAL SECURITY INSPECTIONS:**

a. **Physical Security Inspection.** An inspection intended to ensure area(s) being designated for storage of classified or sensitive material comply with minimum security requirements for safeguarding that material. These are different than COR Audits.

(1) **Marine Corps:** Physical security inspections are normally conducted as part of the command inspection program. Commanding Officers will establish local physical security inspection programs for subordinate commands. A specific, on-site examination of any facility or activity will be conducted by a trained physical security specialist (MOS 5814) to identify security weaknesses and recommend corrective measures. For additional information see [MCO 5530.14](#) (Series).

(2) **Coast Guard:** Physical security inspections are conducted to ensure proper protection and safeguarding, as well as to the prevent loss or compromise of COMSEC material, classified information and government property. For additional information, USCG personnel should consult COMDTINST M5530.1 (series).

b. **Physical Security Survey (PSS).** A PSS is an evaluation of the overall security posture of a given facility or activity. The survey should not be regarded as an inspection or investigation. Physical security surveys will be completed using [NAVMC 11121](#). The completed NAVMC 11121 may be used as part of the physical security inspection at the discretion of the Commanding Officer.

115. **RESPONSIBILITY:**

a. **Naval Communications Security Material System (NCMS).**

1. Serves as the Central Office of Record (COR) for the DON and USCG.

2. Administers the COMSEC Material System (CMS) COR Audit Program for the DON and USCG.

3. Responsible for the training of CMS auditors and is the final designating authority for auditors.

b. **Immediate Superior in Command/Immediate Unit Commander (ISIC/IUC).** ADCON ISICs/IUCs are responsible for oversight of subordinate units' COMSEC programs including the scheduling of COR Audits for subordinate units and for conducting initial facility approvals to store COMSEC material.

c. **CMS COR Auditor.** COR Auditors are responsible to the COR for the proper conduct of the COR Audits and reporting the findings in accordance with this manual.

CHAPTER 2 - CMS COR AUDIT POLICY AND PROCEDURES

201. **GENERAL POLICY:** Any designated CMS COR Auditor may conduct the COR Audit for any DON or USCG-managed account, except for accounts within their own unit. CMS COR audits shall **only** be performed by properly cleared, trained, certified and designated personnel who meet the requirements set forth in Article 301 herein. Audits consist of a review account management practices, an examination of records and re-certification of facilities for COMSEC material storage.

205. **CMS COR AUDIT PROCESS:**

a. **CMS COR Audit.** The audit shall be conducted in sufficient detail to properly evaluate the safeguarding, accounting and disposition of COMSEC material within a COMSEC account. The audit process will include the Local Account and all Local Element(s) (LEs). At accounts with external LEs, supported through a Memorandum of Agreement, a minimum of three external LEs must be audited. LEs not located within 50 miles of the supporting account **may be** exempted from the audit at the discretion of the auditor.

Annexes A through D, as applicable, of this manual will be used for conducting audits of all DON COMSEC accounts, as well as for semi-annual self-assessments by managers.

Individual Service Headquarters (HQMC, COGARD C4ITSC, and COMSC) Fleet Commanders, TYCOMS and ISIC/IUCs may evaluate additional COMSEC-related areas beyond the requirements set forth herein when such is promulgated in written instructions, policy or regulations the account is required to comply with.

Additional requirements incorporated into audit guidelines shall contain reference to source documents. Account Managers designated as CMS COR auditors are not authorized to conduct formal CMS COR audits on their own accounts or LEs supported by the parent account; however, they must conduct spot-checks, conduct training and provide oversight for LEs in accordance with EKMS-1(series).

1. The auditor is tasked with identifying non-compliance with applicable policies, analyzing factors or trends which impede effective account management and providing recommendations for improvement. Any audit process should encompass training and education in areas in need of improvement to enhance account management practices and training programs.

2. The audit may encompass querying Account Managers and LE personnel on policy or procedural matters or require a demonstration of commonly performed functions, i.e. inventorying COMSEC material, performing routine destruction, or conducting audit trail reviews. Weaknesses in these areas may reveal the

need for additional training to ensure COMSEC material is properly managed.

b. **Pre-Audit Guidelines.** At a minimum of 90 days prior to the audit deadline (2 years from date of last audit), the COR Audit Team will contact the account's ISIC to establish the ISIC's intention to accept/defer responsibility for the audit. The ISIC will be responsible for scheduling COR Audits for subordinate commands. Prior to conducting an audit, the auditor(s) shall:

(1) Review account management history to include:

- (a) Results of the previous CMS COR Audit.
- (b) Results of the most recent Self-Assessment.
- (c) Documentation related to corrective actions taken regarding previously identified deficiencies.
- (d) Documentation of COMSEC Incidents or Practices Dangerous to Security (PDSs) encountered by the unit.
- (e) Other areas of special interest identified by NCMS, ISIC/IUC or higher authority.

c. **Approval of COMSEC Facilities.** In accordance with Article 550.d to EKMS-1(series), initial facility approval is revalidated at a minimum of biennially during the COR Audit process. USMC units audited will provide the auditor a copy of the most recent Physical Security Survey (PSS).

d. **Evaluation Criteria.** Upon completion of the audit, an evaluation of either Satisfactory or Unsatisfactory will be assessed based on the minimum standards reflected below. Only matters identified during the conduct of the audit are to be included in the assessment of the account. Matters previously identified, documented and properly reported, as applicable by the unit prior to the audit are not to be used in the assessment, unless the same deficiencies are discovered to still exist. Discovery of the below equal to or in excess of the criteria reflected will result in an unsatisfactory assessment.

(1) One (1) COMSEC Incident.

or

(2) Three (3) Non-Reportable or Reportable Practices Dangerous to Security (PDS).

or

(3) Major administrative errors that exceed the criteria below based on the total number of line items held by the account:

- (a) up to 120 line items, maximum of 10 errors
- (b) 121 - 250 line items, maximum of 20 errors
- (c) 251 - 400 line items, maximum of 30 errors
- (d) 401 - 500 line items, maximum of 35 errors

(e) 501+ line items, maximum of 40 errors

NOTE: Repetitive minor administrative errors (e.g., missing initials on line-outs, required blocks not marked on a SF-153 to indicate the action denoted by the SF-153, i.e. received, inventoried, destroyed, witness, or other) should be and assessed by auditors as one error.

(4) COMSEC incidents of the same category discovered during the audit should be consolidated into a single report. Incidents of different categories, i.e. physical, cryptographic or personnel must be reported separately. If a unit has (2) physical incidents, a single report can be submitted for both. If (1) physical and (1) cryptographic incident is discovered during the audit, (2) separate incident messages are required.

(5) Even though accounts may be assessed as "Satisfactory", the auditor should note particular trends which may benefit from additional clarity in local policy, development of SOPs or training and includes such recommendations in the final report. A follow-up visit/audit by the ISIC/IUC on the areas in need of improvement is recommended to ensure the concerns do not become repetitive or ongoing in nature. When not possible due to distance, funding, etc... the unit audited should report actions taken to the ISIC/IUC via email, message, or official letter, as desired.

(6) Auditors shall include the overall condition of the EKMS/KOA account along with the number and description of any COMSEC Incidents, PDSSs, and administrative discrepancies discovered in the official audit report.

(7) The biennial audit performed by the COR Audit Team or ISIC/IUC is the only authorized, official CMS COR Audit. No other entities will conduct CMS COR audits.

e. **Re-Audit.** Should an account receive a grade of Unsatisfactory or fail to meet the requirements to obtain facility approval for storage of COMSEC material:

(1) A re-audit will be conducted by the COR Audit Team or ISIC/IUC within 90 days of the COR Audit. ISICs must coordinate with NCMS in the event subordinate commands are unable to satisfy this requirement due to operational commitments.

(2) In lieu of a re-audit, with concurrence from the auditor, NCMS, and ISIC, the account may report corrective actions taken to the ISIC and NCMS and once all discrepancies have been corrected, the account will be assessed as Satisfactory.

(3) Certification/Re-certification failure:

(a) Certification: The COMSEC facility must be modified to meet specifications and be re-inspected.

(b) Re-certification: The account must comply with waiver requirements as set forth in OPNAVINST 5530.14(series). When mandatory security requirements cannot be met, commands shall enter the discrepancy into Core Vulnerability Assessment Management Program (CVAMP) and request waivers or exceptions from CNO (N4) via their chain of command. If approved, the waiver will exempt the recipient from a specific security standard for a maximum of up to 12 months. Repairs should be affected as soon as possible, and the COMSEC facility re-inspected. For USN facilities, waiver requests must be forwarded to NAVFACENGCOM prior to submission to the CNO (N4), and an information copy to NCMS//N5//to continue to hold COMSEC material.

CHAPTER-3 - ASSIGNMENT OF CMS COR AUDITORS

301. **DESIGNATION REQUIREMENTS FOR CMS COR AUDITOR.** Auditors must meet the following minimum requirements prior to appointment:

a. U.S. citizen (immigrant aliens are not eligible).

b. Possess a clearance equal to or higher than the Highest Classification Indicator (HCI) of the account to be audited.

NOTE: CMS COR Auditors are **not** required to be SCI Indoctrinated.

c. Personnel conducting audits must hold the grade of E-6 (GS-9/Band 2 for Civilian Government Service employees) or higher.

d. Have successfully completed the formal course of instruction (COI) required to manage the type of COMSEC account to be audited (EKMS Manager or KOAM COI).

e. In addition to completion of formal training, personnel conducting audits of KMI accounts must complete the following NSA developed Computer Based Training (CBTs):

1. Client Platform Administrator (CPA)
2. Client Platform Security Officer (CPSO)
3. Token Security Officer (TSO)
4. Device Registration Manager (DRM)
5. Basic COMSEC Policy & Procedures Inter-Active Courseware (ICW) [when approved]

f. Complete the 304 section of the applicable NAVEDTRA 43462-1 or 43462-2 PQS for the type of account to be audited (EKMS or KMI) in accordance with Article 312 to EKMS-1(series).

g. Auditors must have previously served as an EKMS Manager, KOAM or Primary Alternate for a minimum of one year.

h. Attend the Auditor Training Seminar conducted by the local COR Audit Team.

i. Within 180 days of completion of the CMS COR Auditor Training Seminar:

(1) Accompany and observe at least one CMS COR Audit with a certified CMS COR Auditor; USCG personnel will observe 2 COR Audits.

(2) Conduct a minimum of two CMS COR audits Under Instruction with a certified CMS COR Auditor.

305. **DESIGNATION GUIDELINES.** Upon completion of the requirements set forth in Article 301, the local COR Audit Team will forward the CMS COR Auditor Qualification standards check list to NCMS (N7). NCMS will review the package for completeness, and then forward a designation letter to the individual's parent command certifying assignment as an EKMS/KOA COR Auditor. Appointment of personnel as auditors is not authorized by any organization other than NCMS. For USCG and USMC accounts, NCMS will send the designation letter to:

C4IT SERVICE CENTER
US COAST GUARD
ATTN: IAD-SCB
7323 TELEGRAPH RD MS 7340
ALEXANDRIA, VA
20598-7340

Headquarters U.S. Marine Corps FOB
ATTN: C4/CY EKMS Program Manager
2 Navy Annex, Room 3217
Washington, D.C.
20380-1775

a. Recertification is not automatic. To retain the Auditor Certification, personnel must re-attend the CMS COR Auditor Training Seminar through the local COR Audit team every 36 months while assigned as an EKMS/KOA COR Auditor. Upon completion, NCMS will forward a letter recertifying auditor for continued assignment.

b. Auditors whose certification has been expired for a year or longer or those who have not conducted at least one audit since certifying will be required to re-attend the training seminar and conduct one audit under the instruction of a certified COR auditor prior to recertifying.

NCMS reserves the right to withdraw an auditor's certification when disqualifying or questionable information becomes available. If withdrawn, NCMS will forward an official letter to the auditor's parent command. Parent organizations must notify NCMS in writing if a certified Auditor has his/her access to classified material suspended or security clearance revoked.

CHAPTER-4 - CMS COR AUDIT REPORTING PROCEDURES

401. **CONTENT AND SUBMISSION GUIDELINES:**

a. Significant deficiencies discovered by an auditor which appear to require action by higher-level authorities must be reported immediately to the Commanding Officer (CO) of the audited command.

b. At the conclusion of the audit, a formal out-brief must be provided by the Auditor to the Commanding Officer, Officer-In-Charge (OIC), or Staff CMS Responsibility Officer (SCMSRO), as applicable.

c. Formal CMS COR Audit reports must include comments to substantiate the evaluation, applicable references and recommendations for correcting deficiencies. (See Annex E for an example of a CMS COR Audit report.

d. Approval to continue to hold classified COMSEC material **must be** included in the audit report.

e. Formal audit reports will be submitted by the Auditor to the local COR Audit Team for serialization and review. The local COR Audit Team will then forward the serialized report to the appropriate ISIC/IUC for review and forwarding to the audited command. The audited unit shall correct the deficiencies identified and return a report of corrective actions completed within 30 days from the date of receipt of the audit to their ISIC/IUC. The Auditor will consult the Standard Navy Distribution List ([SNDL](#)) to determine the audited command's ISIC or contact NCMS for assistance.

405. **FEEDBACK REPORT.** Feedback regarding significant discrepancies or misinterpretation of COMSEC policy or procedures is an important management tool. ISICs/IUCs are encouraged to forward such information to NCMS to improve the Audit program and also the COMSEC system as a whole. The use of this report is strongly encouraged as it can provide NCMS with information, practices, or procedures, which may be applied advantageously throughout the DON and Coast Guard EKMS/KOA communities. A sample Feedback Report can be found in Annex F.

410. **PRIVILEGED NATURE OF AUDIT REPORTS.** Auditors serve as the COR's representatives for evaluating COMSEC account management. The release of audit reports prepared under the provision of this manual require appropriate restrictions on public access and access by governmental organizations external to the DON. All audit reports will be marked FOR OFFICIAL USE ONLY and will include the caveat(s) reflected below:

a. **Navy** "The information contained in this report relates to the internal practices of the Department of the Navy. This document is therefore an internal communication not releasable,

nor may its contents be disclosed outside the Department of the Navy without prior approval. This report may not be reproduced, in whole or in part, without approval from an appropriate superior authority. Requests for information contained in this report from an agency external to the Department of the Navy shall be promptly referred to the proper authority. The reviewing authority shall in turn refer the request, with recommended actions, to the appropriate Fleet Commander. Holders of this report shall strictly observe these restrictions."

b. **Marine Corps** "The information contained herein relates to the internal practices of the Department of the Navy and the U.S. Marine Corps. This report is not releasable, nor may its contents be disclosed in whole or in part, without prior approval of (the inspecting command), CMC (C4/CY) or NCMS. Requests for inspection reports, portions thereof, or correspondence related thereto, from a source external to the Department of the Navy shall be promptly referred to CMC (Information Assurance Division (C4/CY)). Holders of this report shall strictly observe this caveat."

c. **Coast Guard** "The information contained herein relates to the internal practices of the Department of Homeland Security and is an internal communication within the inspecting command. This report of (inspecting authority) is not releasable, nor may its contents be disclosed outside of original distribution, nor may it be reproduced in whole or in part, without prior approval of (inspecting authority), COGARD C4ITSC, or NCMS. Requests for inspection reports, portions thereof, or correspondence related thereto, from a source external to the Department of Homeland Security shall be promptly referred to (inspecting authority) who shall further refer the request with recommended action to the Commander, U.S. Coast Guard C4ITSC. Holders of this report shall strictly observe this caveat."

ANNEX A

CMS COR AUDIT GUIDE

PURPOSE. The purpose of this guide is to ensure all aspects of COMSEC management are covered by the CMS COR Auditor during the conduct of the audit. Where used, the term "Account Managers" pertains to the Account Manager and Alternates without regard to a specific account type (EKMS or KMI). Positions (roles) identified with an * are only applicable to a Key Management Infrastructure (KMI) Operating Account (KOA).

INITIAL REQUIRED DATA:

Date of Audit: _____

Command Audited: _____

EKMS/KOA Account Number: _____

Total Line items in EKMS/KOA Account: _____

Immediate Superior in Command: _____

Date of Last CMS COR Audit: _____

Name/Grade/Rate and Command of CMS COR Auditor:

Date of Last Facilities Approval: _____

Manager Name/Grade/Date of Appointment:

Primary Alternate Manager Name/Grade/Date of Appointment:

Identify the Following, as Applicable/Assigned:

Second Alternate Manager Name/Grade/Date of Appointment

Third Alternate. Manager Name/Grade/Date of Appointment

ANNEX A

CMS COR AUDIT GUIDE

Clerk Name/Grade/Date of Appointment (if applicable):

* Client Platform Administrator (CPA)

CPA Name/Grade/Rate: _____

* Client Platform Security Officer (CPSO)

CPSO Name/Grade/Rate: _____

Remarks: _____

ANNEX A

CMS COR AUDIT GUIDE

SECTION	AREA ASSESSED
<u>1</u>	Security
<u>2</u>	Account Manager Responsibilities
<u>3</u>	LMD/KP & MGC/AKP
<u>4</u>	Chronological File
<u>5</u>	Product Inventory/Accountable Items Summary (AIS)/Transaction Status Log
<u>6</u>	COMSEC Material Receipts/Transfers
<u>7</u>	Destruction Procedures/Reports
<u>8</u>	Inventory Reports
<u>9</u>	Correspondence, Message, and Directives File
<u>10</u>	COMSEC Library
<u>11</u>	Local Custody File
<u>12</u>	Report Retention/Disposition
<u>13</u>	Resealing/Status Markings
<u>14</u>	Page checks, Corrections and Amendments
<u>15</u>	Secure Terminal Equipment (STE) phone/IRIDIUM
<u>16</u>	Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer (OTAT) Data Transfer Device (DTD)/Simple Key Loader (SKL)/Tactical Key Loader (TKL))

ANNEX A

CMS COR AUDIT GUIDE

- [17](#) Management and Use of Modern Key
- [18](#) Emergency Protection of COMSEC Material
- [19](#) Emergency Destruction Plan (EDP)
- [20](#) Commanding Officer (CO, OIC, SCMSRO)
Responsibilities
- [21](#) Material Accountability Tracking
- [22](#) Client Platform Administrator (CPA), Client
Platform Security Officer and Token Security
Officer (TSO) Responsibilities (only application
to a KOA)
- [23](#) COMSEC Management Workstation Data Management
Device Power Station (CWMS/DMD PS)

ANNEX A

CMS COR AUDIT GUIDE

ACTION. The audit checklist contained herein has been updated to accommodate inspection of an EKMS or KMI Account and shall be used and completed, in its entirety, by the EKMS/KOA Auditor conducting the audit. The completed audit checklists should aid the Auditor in facilitation of the required out-brief and preparation of the official report. Per Chapter 2 and Article 401.c of this manual, audit reports shall include comments and references to substantiate the evaluation. Below each item, space is provided to annotate comments on any deficiencies or concerns noted during the inspection.

Note: Questions or sections specific to an EKMS or KMI Account are identified accordingly. If not specifically identified as applicable to a particular platform (EKMS Account or KMI Operating Account KOA), it applies to either.

ANNEX A

CMS COR AUDIT GUIDE

SECTION 1 - SECURITY

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	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	A	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	A	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	I	<p>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]</p> <p>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]</p> <p>Note: If personnel have access to keying material and are not reflected on the list or individual designation letter, assess as an incident (review watch-to-watch inventory, SF-153s, CMS-25s, SF-702 to determine (unauthorized access). If the access list is simply outdated, assess as admin discrepancy.</p>

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	I	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	I	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	A	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] Note: USMC accounts are required to have a Physical Security Survey (PSS) conducted biennially by a school trained Military Provost Officer. [Marine Corps Order 5530.14(Series)]
Yes / No	A	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	A	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	A	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	A	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	A	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]

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	I	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	A	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	A	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	A	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	A	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	I	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	A	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	A	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	A	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]

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	A	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	I	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	I	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	A	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	A/I	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? Note: Sealing both the A & B combinations to the TPI container in the same SF-700 could result in a loss of TPI (Physical Incident)
Yes / No	A	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 inspection findings documented on a locally generated log?

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	A	<p>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]</p> <p>Example: Effective, Secret keymat should not be stored with Reserve on Board, Secret keymat. Effective, Top Secret keymat should not be stored with effective, Confidential keymat.</p>
Yes / No	A	<p>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]</p> <p>Note: https://infosec.navy.mil/crypto/- "Hot Topics" - Cryptographic Equipment Battery Information (MIP/MRC tab) and (Battery Information Tab)</p>
Yes / No	I	<p>28. Is COMSEC material properly stored when not in use or under the direct control of authorized personnel? [EKMS-1 (Series), Article 520.a]</p>
Yes / No	A	<p>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]</p>
Yes / No	A	<p>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]</p>
Yes / No	I	<p>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]</p> <p>Randomly select devices issued and</p>

ANNEX A

CMS COR AUDIT GUIDE

		<p>verify it is compliant with the latest version authorized and directed by NCMS via ALCOM message. Record the below information for each device verified.</p> <p>Short Title Serial Number LE</p> <hr/> <hr/> <hr/>
--	--	---

ANNEX A

CMS COR AUDIT GUIDE

SECTION 2 - ACCOUNT MANAGER RESPONSIBILITIES

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A/I	<p>01. Has a formal Letter of Appointment (LOA) been completed for the Manager, Alternate(s) and Clerk(s)? [EKMS-1 (Series), Articles 412, 414 and Annex F; EKMS-1 Supp-1, Article 407.b]</p> <p>Notes: (1) The absence of an appointment letter (required) when the person has the combinations to the vault and access to the LMD/KP or the MGC/AKP would constitute "unauthorized access" for Managers, Alternates and LE Issuing and Alternates; (2) If 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 Admin Hit. (3) Address a missing Clerk Appointment letter as an Admin Hit unless they also had access to keying material and no other written authorization existed signed by the CO.</p>
		<p>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]</p>
Yes / No	A	<p>a. Executed and on file for all personnel with access to "S" or "TS" cryptographic information, including Account Managers?</p>
Yes / No	A	<p>b. Retained for 90 days after the individual no longer requires access to COMSEC material, transfers or retires?</p>

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	A	<p>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]</p> <p>Note: If formal training not completed within 90 days of appointment for manager or 180 days for alternate a waiver from NCMS is required.</p>
Yes / No	A	<p>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]</p>
Questions 05 - 13 apply only to a KOA.		
Yes/No/NA	A	<p>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]</p>
Yes/No	A	<p>06. 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]</p>
Yes/No	P	<p>07. 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]</p> <p>Note: A separate appointment letter is not required for the KOAM or Alternate if he or she is also fulfilling the role of the Client Platform Administrator (CPA).</p>

ANNEX A

CMS COR AUDIT GUIDE

Yes/No	I	08. Does the CPA have a minimum SECRET security clearance? [EKMS-1(Series) Supp-1, Articles 411.e, 805.c; DOC 042-12] Note: If performed by the KOAM or an Alternate, the clearance must be equal to/higher than the HCI of the account.
Yes/No	A	09. 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	A	10. 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	A	11. Has 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	I	12. 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	A	13. 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	A	14. Has the each Account Manager completed the DON Basic COMSEC Policy & Procedures Inter-Active Courseware (ICW) every three years? [EKMS-1(Series) Supp-1 Ch. 6]
EKMS and KOA Accounts		
Yes / No	A	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]

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	P	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	A	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	A	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	A	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	A	20. Does the Letter/Memorandum of Agreement address the minimum areas in accordance with [EKMS-1 (Series) Annex G?]
Yes / No	A	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	I	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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 3 - LMD/MGC

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Questions 01 - 10 apply to both an EKMS Account and a KOA		
Yes/No	I	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	P	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	P	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] Note: Per the DON Authorization to Operate (ATO) the "root" password is set to infinite by default and should remain as such.

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	I	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	A	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	P	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 inspection 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	A	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	I/A	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] Note: If not and discovered in use, document as an incident; if not in use address as an Admin Hit.

ANNEX A

CMS COR AUDIT GUIDE

Yes/No/NA	I	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	A	<p>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]</p> <p>Note: N/A for submarines at-sea.</p> <p>To verify in LCMS:</p> <ol style="list-style-type: none"> 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" <p>To verify in MGC:</p> <ol style="list-style-type: none"> 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

ANNEX A

CMS COR AUDIT GUIDE

		<p>"Related Log ID" column to find Log #</p> <p>5. Look under the "Log ID" column to find the Log ID number which will be the IRST for that Inventory.</p> <p>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"</p>
Questions 11 - 22 apply to an EKMS Account only		
Yes/No/NA	A	11. Does each Manager have a (unique) LMD/KP Operator ID and CIK? [EKMS-1 (Series), Annex Q, Paragraph 12]
Yes/No/NA	A	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	A	<p>13. Are REINIT 1 and NAVREINIT 2 CIKS properly registered in LCMS? [EKMS-1 (Series), Article 1140]</p> <p>To verify, in LCMS go to: Registration - COMSEC Material.</p> <p>a. Are REINIT 1 keys reflected on the AIS as "AIDS" and accounted for as ALC-1?</p> <p>b. Are NAVREINIT 2 keys reflected on the AIS as "Equipment" and accounted for as ALC-4?</p>
Yes/No/NA	A	14. Does the account have a minimum of two LCMS/KP System Administrators registered? [EKMS-1 (Series), Annex Q, Paragraph 9]
Yes / No	P	<p>15. Are KP PINs changed every 90 days? [EKMS-1 (Series) Article 520.i, 1005.a]</p> <p>Note: This can be verified through LCMS activity data, the MGC Windows Security Logs or SF-700s.</p>
Yes/No/NA	I	16. Has a KP changeover been performed every 3 months (92 days maximum)? [EKMS-1 (Series), Article

ANNEX A

CMS COR AUDIT GUIDE

		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 Note: Failure to perform a changeover within the prescribed interval is a cryptographic incident.
Yes/No/NA	I	17. Has the KP in use been recertified within the current (3) years? [EKMS-1 (Series), Article 945.c, 1185.e] Note: Prior to assessing as an incident, inquire to determine; (a) Has the replacement one been received? or; (b) Was the corresponding Transit CIK received, or; (c) has the unit submitted a waiver for continued use of the existing AKP/KP due to a hardware failure or (d) does the account require a new FF Vector Set and/or MSK (if so did they order it?)
Yes / No	A	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	P	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	P/A	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] Note: Improper labeling constitutes Administrative error.
Yes/No/NA	P	21. Are backups being performed on the following as required? [EKMS-

ANNEX A

CMS COR AUDIT GUIDE

		1 (Series), Articles 718.d, 1005.a]
		a. LCMS Database: After every session that modifies the Account Item Summary and Transaction Status log?
		b. Unix maintenance backups on monthly basis (i.e. Root and U)?
Yes / No	P	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]
Question 23 - 35 Apply to a KOA only		
Yes/No/NA	P	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	I	24. Has a changeover been performed at a minimum of every 12 months? [EKMS-1 (SERIES) Supp-1 Articles 207.d, 805.a] To determine, have the Manager or Alternate logon to MGC, navigate to the "KMI Navigation" pane on the left: MGC Management - AKP Configuration - AKP Changeover. The pane on the right will then display the current changeover version.
Yes/No/NA	P	25. Are monthly visual inspections for the AKP conducted and documented properly in the AKP Inspection Log? [EKMS-1 (SERIES) Supp-1, Articles 201.d, 903.a] Note: Log will include Short Title, Serial No., Inspection Date, and signature and printed name of inspector
Yes/No/NA	P	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	I	27. Has the AKP in use been recertified within current (7) years? [EKMS 1B Supp-1, Articles 207.g, 805.a]

ANNEX A

CMS COR AUDIT GUIDE

Yes/No/NA	I	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	P	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	P	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	A	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	P	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	P	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	A	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	P	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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 4 - CHRONOLOGICAL FILE

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
		01. Does the CHRONOLOGICAL FILE contain the following: [EKMS-1 (Series) Article 703.a, Annex M]
Yes / No	P	a. COMSEC material accounting reports (conversion, destruction, generation, possession, receipts, relief from accountability, transfer reports). Note: Missing accounting reports could result in an incident if the material is "In Stock" to the account but not accounted for at the account level.
Yes / No	A	b. EKMS Accounts only: Up-to-date Accountable Item Summary (AIS) or up-to-date printed COAL inventory [see EKMS-1 (Series) Art 706.a, 63.c note]
Yes / No	A	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	P	d. Consolidated inventory reports (including ALC 4 & 7 inventories) and reconciliation notices
Yes / No	A	e. Transaction Status Log
Yes / No	A	f. USTRANSCOM Form-10
Yes / No	A	g. CMS Form 1 (if required)
Yes / No	A	h. SD Form 572
Yes / No	A	i. EKMS CF Special Notices
** The below are required to be held by KOAs only **		
Yes / No	A	j. KMI Form 004 - KMI Human User Agreement Form [EKMS-1(SERIES) SUPP-1 Article 321.d, 409.a] Note: To be retained by the PLT1RA for 7 years or length of appointment, whichever is longer.
Yes / No	A	k. KMI Form 005 - KMI Transition Checklist [EKMS-1(SERIES) SUPP-1 Article 401.b]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 5 - ACCOUNTABLE ITEM SUMMARY (AIS)/PRODUCT INVENTORY)/TRANSACTION STATUS LOG

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Item/Area Checked
Yes / No	P/I	<p>01. 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]</p> <p>EKMS Accounts only - Randomly record the short title, serial number, and edition off at least 3 items and do the following:</p> <p>Logon to the LMD - Accounting - Accountable Item Summary - (Change the display to Account). Is the item reflected on the Accountable Item Summary (AIS) and is it reflected as "On-Hand"?</p> <p>KOA only - Logon to MGC - Accounting - Product Inventory - (Change the display to Account) vice all. Is the item reflected on the Product Inventory and is it reflected as "On-Hand"?</p> <p>Note: If COMSEC accountable items are discovered not to be properly accounted for, only assess as an incident if it involves classified keying material, unclassified keying material designated as "CRYPTO" or CCI. Otherwise, document and report per Article 1015.</p>
Yes / No	P	<p>02. 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]</p>
Yes / No	A	<p>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]</p>

ANNEX A

CMS COR AUDIT GUIDE

SECTION 6 - COMSEC MATERIAL RECEIPTS/TRANSFERS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	P	01. 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	A	02. 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	P	03. 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	A	04. Has the receipt of Two Person Control (TPC) material been reported per CJCSI 3260.01? [EKMS-1 (Series), Article 255.c]
Yes / No	A	05. Are pending tracers processed within the required timeframes? [EKMS-1 (Series), Articles 743.e, 945.e]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 7 - DESTRUCTION PROCEDURES/REPORTS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	I	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	I	02. Are destruction records completed to document destruction of all COMSEC material? [EKMS-1 (Series), Article 736.b, Annex M]
Yes / No	P/I	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; DOC 024-12]] Note: Regardless of form, electronic or physical, superseded key must be destroyed within the prescribed time frames. If the material has been documented as destroyed and found to exist, report as a COMSEC Incident. If destroyed late and the key is not NATO, document as a non-reportable PDS.
Yes / No	P	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] Note: Failure to complete blocks 14 & 16 should be treated as an Administrative Discrepancy.

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	I/P	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] Note: If physical (including equipment) or NATO material is destroyed late, assess as a COMSEC incident; for electronic key and non-NATO material, assess as a PDS.
Yes/No/NA	P	06. EKMS Accounts only - 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 paragraph 10] <ul style="list-style-type: none"> - FF Vector Set: USFAU 0000000333 - Message Signature Key: USFAU 4294967297 - Transit CIK: USKAU B7121 - KG Rules: USKAD BU71260 880091
Yes/No/NA	P	07. KOA Only - 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) Supp-1, Articles 207.b, 207.c, 903, EKMS-1(Series) Article 1005.A] <ul style="list-style-type: none"> - FF Vector Set: USFAU 0000000333 - Message Signature Key(MSK): USFAU 4294967297 - KG-250 key AFAU 1401600001
Yes / No	P	08. Have consolidated destruction records been signed by the CO/OIC/SCMSRO (Block 17)? [EKMS-1 (Series), Annex N, paragraph 7.a]
Yes/No/NA	P	09. 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	I	10. 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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 8 - INVENTORY REPORTS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	P	<p>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]</p> <p>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.</p>
Yes / No	P	<p>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]</p>
Yes / No	A	<p>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</p>
Yes / No	A	<p>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</p>
Yes / No	P	<p>05. Have discrepancies on the Inventory Reconciliation Status Report (IRST) been communicated to the COR and resolved? [EKMS-1 (Series), Article 766.b]</p>
Yes / No	P	<p>06. Was the CCIR or Combined Inventory, as applicable conducted for a change of command signed by the <u>outgoing</u> Commanding Officer? [EKMS-1 (Series), Articles 766.a, 766.b]</p>

ANNEX A

CMS COR AUDIT GUIDE

SECTION 9 - CORRESPONDENCE, MESSAGE AND DIRECTIVES FILE

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
		01. Does the Correspondence and Message File contain the following <u>required</u> files: [EKMS-1 (Series), Article 709.a]
Yes / No	A	a. Account establishment correspondence? Note: Only required for accounts established after 01 Jul 93; optional for previously established accounts.
Yes / No	A	b. Manager, Alternates and Clerk appointment correspondence (EKMS or KOAMs)? Note: Do not assess as a separate discrepancy if assessed under Section 2 herein.
Yes / No	P	c. CPA and CPSO appointment correspondence? Note: Do not assess as a separate discrepancy if assessed under Section 2 herein.
Yes / No	A	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	A	e. COMSEC Incident and Practice Dangerous to Security reports (this includes documentation on non-reportable PDSs)? Note: If an incident or PDS is discovered and no documentation exists to reflect it was reported to the appropriate level, it must be assessed as discovered, documented and reported.
Yes / No	A	f. Correspondence relating to command allowance and authorization to store classified COMSEC material?
Yes / No	A	g. The <u>previous CMS COR Audit report</u>
Yes / No	I	h. List of personnel authorized access to keying material and the LMD/KP or MGC/AKP, as applicable?

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	A	02. 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	A	03. 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	A	04. 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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 10 - COMSEC LIBRARY

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
		<p>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]</p> <p>Note: USCG units refer to USCG COMSEC Advisory 02-09 for USCG-specific library requirements.</p>
Yes/No/NA	A	a. EKMS Accounts only: LMD/KP Operators Manual EKMS 704(series)
Yes/No/NA	A	b. KOA Only: Operations and Maintenance Manual (OMM) for the KMI Client Node (classified)
Yes/No/NA	A	c. EKMS Accounts only: EKMS Managers JQR
Yes/No/NA	A	d. COMUSFLTFORCOM/COMPACFLT/COMUSNAVEURISNT C2282.1 (series) Basic Shipboard Allowance of COMSEC material (USN Surface Ships only)
Yes / No	A	e. EKMS-1 (series) Policy and Procedures Manual
Yes / No	A	f. EKMS-3 (series) EKMS/KOA COR Audit Manual
Yes / No	A	g. EKMS-5 (series) EKMS Cryptographic Equipment Manual
Yes/No/NA	A	h. COMDTINST 5510.23 (USCG only)
Yes/No/NA	A	i. NAG-53 (series) - Keying Standard for Non-Tactical KG-84/KIV-7 Point to Point Circuits (shore-based accounts only)
Yes / No	A	j. NAG 16 (series) Field Generation and Over-the-air distribution of tactical Electronic Key
Yes/No/NA	A	k. NSA Mandatory Modification Verification Guide (MMVG)
Yes / No	A	l. OPNAVINST 2221.5 (series) Release of COMSEC material to U.S. Industrial Firms Under contract to USN
Yes / No	A	m. SECNAV M5510.30 (series) DON Personnel Security Program
Yes / No	A	n. SECNAV M5510.36 (series) DON Information Security Program

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	A	o. OPNAVINST 5530.14 (series) Physical Security and Loss Prevention
Yes / No	A	p. SECNAVINST 5040.3 (series) Naval Command Inspection Program (if applicable)
Yes / No	A	q. OPNAVINST 2221.3 (series) Qualifications of Maintenance Personnel
Yes/No/NA	A	r. CJCSI 3260.01 (series) Joint Policy Governing Positive Control Material Devices (Required only if SAS material held)
Yes/No/NA	A	s. SDIP 293 NATO Cryptographic Instruction (Required only if account holds NATO material)
Yes/No/NA	A	t. AMSG-600 NATO Communications Security Information. (Required only if the account holds NATO material)
Yes/No/NA	A	u. Operational Security Doctrine for Key Management Infrastructure (KMI) KOV-29 (sKey6500)
Yes/No/NA	A	v. Operational Security Doctrine for the Key Management Infrastructure (KMI) Management Client (MGC)
Yes/No/NA	A	w. Operational Security Doctrine for KG-250X - High Assurance Internet Protocol Encryptor (HAIPE)
Yes/No/NA	A	x. Process Security Doctrine for the Registration of KMI Operating Accounts and KMI Users
Yes/No/NA	A	y. Type 1 Certificate Policy (CP)
Yes/No/NA	A	z. MGC Operations and Maintenance Manual for the KMI Client Node

ANNEX A

CMS COR AUDIT GUIDE

SECTION 11 - LOCAL CUSTODY FILE

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	<p>01. Does the local custody file contain signed, effective, local custody documents for each item of COMSEC material issued <i>including electronic key issued to a DTD, SKL or TKL</i>? [EKMS-1 (Series), Articles 712.a, 945.e; Annex M, Annex T paragraph 17, Tab 1 paragraph 3]</p> <p>EKMS Accounts only - Logon to LCMS and do the following: Accounting - Accountable Item Summary - (highlight the desired LE), i.e. Radio, click on "Material History", Select the entry "Issue Initiating" - then "View Transaction". Note the date of the report and TN. Pull the Local Custody file for the LE and verify the corresponding SF-153(s) are on file and properly completed/signed.</p> <p>KOA only - Logon to MGC and Select: Products - Inventory - Product Inventory. The "All Products" tab should be highlighted. In the filter block below "All Products", type "issued". Highlight an entry labeled "Issued", select the location the material was issued to and ask the Manager to see the corresponding SF-153 and verify completeness with all required signatures.</p>
Yes / No	I	<p>02. Are local custody documents retained for a <u>minimum</u> 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]</p>

ANNEX A

CMS COR AUDIT GUIDE

SECTION 12 - REPORT RETENTION/DISPOSITION

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	01. Are inactive records awaiting expiration of the required retention period clearly labeled with the appropriate classification, downgrading instructions and the authorized destruction date? [EKMS-1 (Series), Article 715.c]
		Have the following been retained for the minimum retention period of one (1) year : [[EKMS-1 (Series) Annex M]
Yes / No	A	a. Receipts for official messenger mail, DCS courier mail and registered mail
Yes / No	A	b. Terminated Letters of Agreement
Yes / No	A	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	A	b. General correspondence and messages pertaining to COMSEC matters relating to account holdings?
Yes/No/NA	P	c. LMD/KP PIN/CIK log
Yes / No	P	d. Spot Checks (or log) / Self-Assessments
Yes / No	I/P	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.
		02. Have the following been retained for the minimum retention period of two (2) years (current year plus previous 2 full years):
Yes / No	P	a. Inventory Reports (SAIRS, CCIRs, Combined, etc..) for all material (ALC 1,2,4,6,7) Note: working copies can be purged upon receipt of a RCC, as discussed in Annex M to EKMS-1 (Series)

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	I	<p>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; Local Destruction Reports for ALC-4/7 material, and working copies of SF-153s generated for account/LE destruction)?</p> <p>Note: For material reflected in Tier 1 as "In Stock" the account must have the material or Destruction, ROA or Transfer Report.</p>
----------	---	---

ANNEX A

CMS COR AUDIT GUIDE

SECTION 13 - RESEALING/STATUS MARKINGS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	I/P	<p>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]</p> <p>Note: Except as indicated in article 769.g.1 note, if keying material is prematurely extracted, it must be documented on the CMS-25 as a non-reportable PDS. If found not documented on a CMS-25, report the matter as a Physical Incident.</p>
Yes/No/NA	A	<p>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]</p>
Yes/No/NA	I	<p>03. Are keytape canisters free of locally applied labels which may conceal attempted penetration or prevent inspection of protective packaging, as applicable? [EKMS-1 (Series), Article 760.e, 945.e]</p>
Yes / No	A	<p>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]</p>
		<p>EKMS Accounts only - To verify on the LMD, from the desktop - Distribution - Effective Date Tool - Record a Hard Copy Effective Date</p> <p>KOA only - To verify on the MGC, from the desktop - Products - Effective Dates</p>

ANNEX A

CMS COR AUDIT GUIDE

SECTION 14 - PAGE CHECKS, CORRECTIONS AND AMENDMENTS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	A	01. 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	a. <u>Unsealed COMSEC keying material</u> : upon initial receipt; during account inventories; during watch inventories; prior to transfer; and upon destruction?
Yes/No/NA	A	b. <u>Unsealed maintenance and operating manuals</u> : 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? Note: The Inspector must review the Record of Page Checks to verify the dates of the page checks coincide with account inventories, including those conducted for Change of Command or Change of Manager.
Yes/No/NA	A	c. <u>Unsealed amendments</u> : 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	A	d. <u>Maintenance and repair kits</u> : upon initial receipt; upon installation of modification; during inventories; prior to transfer of the Q(repair kits); and upon destruction? Note: Randomly open 3 - 5 Q-kits and verify; (a) that an actual inventory is contained in the kit, (b) that the inventory document is

ANNEX A

CMS COR AUDIT GUIDE

		signed/dated by the individuals who sight-inventoried the cards and (c) if any card has been removed, the inventory reflects this and the appropriate documentation is in the kit in place of the removed card.
Yes/No/NA	A	e. <u>Equipment</u> : upon receipt (i.e., uncrating); during account and watch inventories; prior to transfer; and upon destruction?
Yes/No/NA	A	f. <u>Resealed keying material</u> : during account inventories; prior to transfer; and upon destruction?
Yes/No/NA	A	02. 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	I/P	03. Are page check discrepancies being reported? [EKMS-1 (Series), Articles 757.h, 945.e, 1015; Annex O] Note: Page check discrepancies must be reported as a Physical Incident for classified material; for unclassified material not marked or designated as crypto or nomenclated as CCI, report per Article 1015 to EKMS-1 (Series).
Yes/No/NA	A	04. Are corrections to a publication made with black or blue-black ink only? [EKMS-1 (Series), Article 787.g]
Yes/No/NA	A	05. 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	A	06. 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	A	07. 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	I	08. Is classified & unclassified amendment residue destroyed within five days of amendment entry? [EKMS-1 (Series), Articles 540.g, 945.e]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 15 - SECURE TERMINAL EQUIPMENT (STE)/IRIDIUM

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	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	A	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	P	03. Is keying material successfully filled in KSV-21 cards reflected on the account's reportable destruction report NLT 5 th day of the month following the loading as "Filled in End Equipment" [EKMS-1 (Series), Article 1005.a; Annex T paragraph 17]
Yes / No	A	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	P	05. Are in use STE/SCIP products rekeyed at a minimum of annually? [EKMS-1 (Series), Article 1005.a]
Yes/No/NA	A	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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 16 - OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR TRANSFER (OTAT) & DATA TRANSFER DEVICE (DTD)/SIMPLE KEY LOADER(SKL)/TACTICAL KEY LOADER (TKL)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	P	01. 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	A	02. Does the Manager conduct periodic reviews of OTAT/OTAR local accounting logs? [EKMS-1 (Series), Article 1105]
Yes / No	I	03. 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	I	04. Is unrestricted access to Supervisory CIKs or SSO passwords for the DTD/SKL/TKL or Talon Card, as applicable, limited to only those individuals who are authorized to perform all of the associated privileges? [CNSSI 3021, DOC 005-15]
Yes / No	I/P	05. 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] Note: Loss of a CIK is only a COMSEC Incident if the device was lost with the CIK or the device and CIK may have been accessed by unauthorized personnel; otherwise document as a non-reportable PDS.
Yes / No	P	06. 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]

ANNEX A

CMS COR AUDIT GUIDE

Yes / No	I	07. 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	I	08. 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	P	09. 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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 17 - MODERN KEY

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P= PDS)	Area/Item Reviewed
Yes / No	A	01. 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	A	02. 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	A	04. Are FTRs registered as ALC-1, material type "Equipment"? [EKMS-5 (Series), Article 107]
Yes / No	P	05. 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	A	06. Does the Manager make use of the Modern Key Tracking Tool? Annex U, paragraph 8.d]
Yes / No	P	07. 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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 18 - EMERGENCY PROTECTION OF COMSEC MATERIAL

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P= PDS)	Area/Item Reviewed
Yes / No	A	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	A	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	A	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	A	04. Does the Manager maintain the COMSEC portion of the command EAP? [EKMS-1 (Series), Annex H, paragraph 1]
Yes/No/NA	A	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	A	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?

ANNEX A

CMS COR AUDIT GUIDE

		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	A	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	A	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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 19 - 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	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	A	09. Does the COMSEC account have an EDP incorporated into their EAP? [EKMS-1 (Series), Annex H, paragraph 2.c]
Yes/No/NA	A	10. 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	A	11. 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	A	12. Are the sensitive pages of KAMs prepared for ready removal (i.e., upper left corner clipped) and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [EKMS-1 (series), Annex M, paragraph 5.e]
Yes / No	A	13. Are the priorities of destruction indicated in the plan? [EKMS-1 (Series), Annex M, paragraph 8]
Yes / No	A	14. 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	A	15. Is the EDP divided into two parts: one for precautionary and one for complete destruction? [EKMS-1 (Series), Annex H, paragraph 7]
Yes / No	A	16. Does the EDP provide for adequate

ANNEX A

CMS COR AUDIT GUIDE

		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	A	17. 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	A	18. 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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 20 - COMMANDING OFFICER (CO, OIC, (SCMSRO) RESPONSIBILITIES

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No		01. Has the Commanding Officer:
	A/I	<p>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]</p> <p>Note: If the Manager, Alternates or LE Issuing and LE Issuing Alternates have the combination to the vault or containers used at this level and are not appointed in writing, assess as a Physical Incident (unauthorized access)</p>
Yes / No	A/I	<p>b. established, in writing, a list of personnel authorized access to keying material. [EKMS-1 (Series), Article 450.c]</p> <p>Note: If the list has not been updated annually, assess as an Admin discrepancy, if personnel have access to COMSEC Keying Material who are not on the list, assess as a Physical Incident. To determine review inventories, CMS-25s, SF-153s, and SF-702s</p>
Yes / No	A	<p>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]</p>
Yes / No	A	<p>d. ensured that COMSEC incident reports are promptly submitted and action taken as required. [EKMS-1 (Series), Articles 450.e, 960]</p>
Yes/No/NA	I	<p>e. Only extended crypto periods as authorized, up to two hours. [EKMS-1 (Series), Article 450.f]</p>

ANNEX A

CMS COR AUDIT GUIDE

		Note: If extended beyond 2 hours and such is not authorized by the Controlling Authority assess as a Cryptographic Incident.
Yes / No	A	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	P	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	A	h. received debriefings from CMS COR Audit Teams and CMS Auditors. [EKMS-1 (Series), Article 450.j]
Yes / No	A	i. ensured that the Emergency Action Plan (EAP)/Emergency Destruction Procedures (EDP) were established and tested. [EKMS-1 (Series), Article 450.m]
Yes / No	A	j. ensured any collateral duties assigned to Manager did not interfere with COMSEC responsibilities. [EKMS-1 (Series), Article 450.o]
Yes / No	A	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]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 21 - MATERIAL ACCOUNTABILITY TRACKING

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	<p>01. Randomly select 10 Short Titles from the accounts Accountable Item Summary or Product Inventory and verify these items are in the vault, have been properly issued or transferred and the corresponding SF-153 is on file.</p> <p>EKMS Accounts Only - Login to LMD - Accounting - Accountable Item Summary - (If desired, change the filter from "all" to "sub-account", LE, etc...), Highlight the appropriate level (local account, sub-account, LE), click "Select", Highlight one or more Short Titles, Select "Detailed Data", Select the Item, Click on Material History, for any item not reflected as "On-Hand", Select "View Transaction" review the corresponding SF-153 for completeness.</p> <p>KOA only- Login to the MGC - Products - Inventory - Product Inventory - the "ALL Products" tab should be highlighted - In the filter block under "All Products" type "Issued", "Open Storage" or "Transfer Pending", as desired. Ask the Manager to see the corresponding SF-153 and verify completeness with all required signatures.</p>
Yes / No	I	<p>02. Randomly select 10 Short Titles held by the account with regular, monthly supersession and request the Manager produce the destruction reports reflecting the Short Titles selected for the previous month.</p> <p>Verify the working copies were signed by a minimum of two personnel and the consolidated reports reflect three signatures and that the date of report and TNs match those in MGC. [EKMS-1 (Series), Article 1005.a.4, Annex M Para 2]</p>

ANNEX A

CMS COR AUDIT GUIDE

SECTION 22 - CLIENT PLATFORM ADMINISTRATOR (CPA), CLIENT PLATFORM SECURITY OFFICER (CPSO), TOKEN SECURITY OFFICER (TSO) RESPONSIBILITIES - THIS SECTION IS ONLY APPLICABLE TO KOAS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	A	01. Is the MGC compliant with mandatory software upgrades or IAVA patches? [EKMS-1(SERIES) Supp-1, Article 219.b]
Yes/No/NA	I	02. Has the CPA established and maintains unique Microsoft Windows user-accounts and permissions on the Client Host? Note: To verify, have the CPA logon go to the MGC then go to - Start - Settings - Control Panel - Administrative Tools - Computer Management - Local User Groups. [EKMS-1(SERIES) Supp-1, Articles 501.e, 805.c]
Yes/No/NA	P	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	P	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	P	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	P	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	I	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	I	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]

ANNEX A

CMS COR AUDIT GUIDE

Yes/No/NA	A	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	A	10. Does the CRP discuss lost token to include revocation procedures? [EKMS-1(SERIES) Supp-1, Article 215.a]
Yes/No/NA	I	11. Is the TSO the TSO for their own token? [EKMS-1(SERIES) Supp-1 Articles 103.s, 305.n, 411.c, 805.b]

ANNEX A

CMS COR AUDIT GUIDE

SECTION 23 - COMSEC MANAGEMENT WORKSTATION DATA MANAGEMENT
DEVICE POWER STATION (CMWS/DMD PS)

<p>This section is only applicable if the account utilizes a (CMWS/DMD PS) at the account level. If held at the LE level, assess in Annex B.</p>		
Yes/No/NA	I	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	A	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	I	03. Is use of the CMWS/DMD PS restricted to "Black Key" only? [EKMS-1 (Series), Annex W, paragraph 3.b]
Yes/No/NA	I	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	I/P	06. 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.

COMMENTS :

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

PURPOSE. The purpose of this audit guide is to ensure all aspects of COMSEC management are covered by the EKMS/KOA Auditor during the account audit. The criteria contained in this annex apply to either a Local Element (LE) Issuing or LE Using unless otherwise identified in the specific section or question.

INITIAL REQUIRED DATA:

Date of Audit: _____

Command Audited: _____

EKMS/KOA Account number: _____

Total Line items in EKMS/KOA account: _____

Immediate Superior in Command: _____

Date of Last EKMS/KOA Audit: _____

Name/Grade/Rate and Command of EKMS/KOA Auditor:

Date of Last Facilities Approval: _____

Local Element Name/Grade: _____

Alternate Local Element Name/Grade/Date of Appointment:

Identify Following, as Applicable/Assigned:

Second Alternate Local Element Name/Grade/Date of Appointment:

Third Alternate Local Element Name/Grade/Date of Appointment:

Clerk Name/Grade (if applicable):

Remarks: _____

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION IDENTIFICATION

- 1 - Security
- 2 - Local Element Responsibilities
- 3 - Accountable Items Summary (AIS) & Local Custody File
- 4 - Local Element Inventories/Page Checks
- 5 - Resealing/Status Information
- 6 - Corrections and Amendments
- 7 - Routine Destruction
- 8 - Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer (OTAT)
 - Data Transfer Device (DTD)/Simple Key Loader (SKL)/Tactical Key Loader (TKL)/TALON Cards (TCT)
 - Management and Use of Modern Key
- 09 - COMSEC Management Workstation Data Management Device Power Station (CMWS/DMD PS)
- 10 - Emergency Action Plan (EAP)
- 11 - Emergency Destruction Plan (EDP)

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

ACTION. The following audit checklist shall be used and completed, in its entirety, by the EKMS/KOA Auditor conducting the audit. Per Chapter 2 and Article 401.c of this manual, audit reports shall include references and comments to substantiate the evaluation. Below each item reviewed, space is provided to annotate comments to any question that receives a negative response. The inclusion of the audit checklists should greatly aid both auditors and the audited activity in conducting the out-brief, as well as in preparation of the official report.

SECTION 1 - SECURITY

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	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	A	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	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	I	03. Is unescorted access limited to individuals whose duties require access and who meet access requirements? [EKMS-1 (Series), Article 505] Note: See Annex A #4 (Part B) for when such could result in a COMSEC Incident.
Yes / No	A	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	I	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	I/A	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] Note: If personnel have access to keying material and are not reflected on the list or individual designation letter, assess as an incident (review watch-to-watch inventory, SF-153s, CMS-25s, SF-702 to determine (unauthorized access). If the access list is outdated, assess as an administrative discrepancy.
Yes / No	I	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	A	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	A	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	I	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	A	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	I	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	A	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	A	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	A	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	I	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	A	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes/No/NA	A	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	A	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	A	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	I	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	I	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/I	a. Individually wrapped and protectively packaged in an SF-700 envelope? Note: Sealing the A & B combination to a TPI container together could result in a physical incident should a single person have access to the space and container.
Yes / No		b. Are SF-700s sealed using transparent lamination or plastic tape?

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	A	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 inspection 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	A	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	I	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	A	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	A	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	A	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	I	<p>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]</p> <p>Randomly select devices issued to LEs and verify it is compliant with the latest version authorized and directed by NCMS via ALCOM message. Record the below information for each device verified.</p> <p>Short Title Serial Number LE</p> <hr/> <hr/> <hr/>
----------	---	--

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 2 - LOCAL ELEMENT RESPONSIBILITIES

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	A	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	A	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	A	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	A	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	A	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	A	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	I	a. LE personnel authorized access to keying material in writing
Yes / No	A	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	A	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	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	A	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	I	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	I/A	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	A	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	A	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	A	14. LE Issuing only. Does the (Issuing) LE maintain required files as directed by the parent account EKMS Manager? [EKMS-1 (Series), Article 703]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	P	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	A	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	P	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

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 3 - ACCOUNTABLE ITEM SUMMARY & LOCAL CUSTODY FILE

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	A	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	I/A	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] Note: For a LE Using, if the material is being properly inventoried on a watch-to-watch inventory and a copy of the LCI is held by the Manager, assess as an administrative discrepancy; if the Manager does not have the LCI document assess as incident in Annex A.
Yes/No/NA	P	03. For LE Issuing only. Do local custody documents (i.e., SF 153, or locally prepared equivalent), contain the <u>minimum</u> required information? [EKMS-1 (Series), Article 769.c]
Yes / No	A	05. Are inactive files/records labeled to reflect the authorized date of destruction? [EKMS-1 (Series), Article 715.c]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 4 - LE INVENTORIES AND PAGECHECKS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	P	01. 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	P	02. 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	P	03. Has the inventory been properly signed and dated for each change of watch? [EKMS-1 (Series), Article 775.d, 1005.a]
Yes/No/NA	A	04. 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]
Yes/No/NA	A	05. Are required page checks being accomplished as follows: [EKMS-1 (Series), Article 775.e, 778.d; Annex P]
Yes/No/NA		a. <u>Unsealed COMSEC keying material.</u> Upon initial receipt; during account and watch inventories; and prior to destruction?
Yes/No/NA		b. <u>Resealed keying material.</u> During Fixed-Cycle and Change of EKMS/KOA Manager inventories; and upon destruction?

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes/No/NA	A	c. <u>Unsealed maintenance and operating manuals</u> . 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. <u>Equipment</u> . Upon initial receipt (uncrating); during Fixed-Cycle and Change of EKMS/KOA Manager inventories; during watch inventories; and upon destruction?
Yes/No/NA	I	06. Are page check discrepancies being reported? [EKMS-1, Articles 757.h, 945.e, 1015; Annex O] Note: Page check discrepancies must be reported as a Physical Incident for classified material; for unclassified material not marked or designated as crypto or nomenclated as CCI, report per Article 1015 to EKMS-1 (Series).

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 5 - RESEALING/STATUS INFORMATION

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	I/P	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		a. A statement the keytape segment(s) were unintentionally removed?
Yes / No		b. The date of the removal?
Yes / No		c. Identity of the keytape segment(s) actually removed?
Yes / No		d. Signatures of the individuals who removed the key? Note: Except as authorized in Article 769.g note 1, premature extraction is a non-reportable PDS when properly documented on the CMS-25; when not documented, report as a Physical Incident (Unexplained removal of key)
Yes/No/NA	A	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	A	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	A/I	04. Are key tape canisters free of <u>locally applied</u> labels and stickers which may conceal attempted penetration or prevent inspection 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.

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 6 - CORRECTIONS and AMENDMENTS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes/No/NA	A	01. Are corrections to publications made with black or blue-black ink only? [EKMS-1 (Series), Article 787.g]
Yes/No/NA	A	02. 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	A	03. 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	A	04. 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	A	05. 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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 7 - ROUTINE DESTRUCTION

Yes / No	I	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	P	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	A	e. Classification and Declassification markings? Derived from: NSTISSI 4002 Declassify on: DD Month YYYY
Yes / No		
Yes / No		
Yes / No	P	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	A/I	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] Note: If the material was properly destroyed and documented on a local destruction record and a copy of the LCI is held by the Manager, assess as an administrative discrepancy; if the Manager does not have the local destruction document assess as an incident under Section 13 to Annex A.

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	P	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	A	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	P	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 8 - OVER-THE-AIR-REKEY/OVER-THE-AIR
TRANSFER & DATA TRANSFER DEVICE (DTD)/SIMPLE KEY
LOADER (SKL)/TACTICAL KEY LOADER (TKL) & MANAGEMENT OF
MODERN KEY

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	<u>Area/Item Reviewed</u>
Yes/No/NA	P	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	P	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	A	03. If <u>Top Secret key is stored in a DTD, SKL, etc... is the device, handled, stored and safeguarded under TPI?</u> [EKMS-1 (Series) Article 510; CNSSI-3021; DOC 005-15]
Yes / No	I	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	I	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	I/P	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] Note: Loss of a CIK is only a COMSEC Incident if the device was lost with the CIK or the device and CIK may have been accessed by unauthorized personnel otherwise document as a non-reportable PDS.

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	P	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	I	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	I	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] Note: Assess as N/A if a SSO or Supervisory User is not appointed at the LE level and assess in Annex A.
Yes/No	P	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	P	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] Note: Loss or unauthorized copying of a CIK is a COMSEC Incident. Loss is considered such when the associated device has not been; stored properly, under the direct control of authorized personnel or failure to delete a lost/stolen CIK from its associated device.
Yes/No/NA	P	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]

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

Yes / No	I	<p>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]</p> <p>Note: Do not report broken equipment in which the source of damage is known as a COMSEC incident unless it is being used with a breach in the housing.</p>
Yes / No	P	<p>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]</p>
Yes / No	A	<p>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]</p>
Yes / No	P	<p>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]</p>

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 9 - COMSEC MANAGEMENT WORKSTATION DATA MANAGEMENT
DEVICE POWER STATION (CMWS/DMD PS)

This section is only applicable if the LE uses the (CMWS/DMD PS).		
Yes/No/NA	I	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	A	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	I	03. Is use of the CMWS/DMD PS restricted to "Black Key" only? [EKMS-1 (Series), Annex W, paragraph 3.b]
Yes/No/NA	I	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	I/P	06. 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.

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 10 - EMERGENCY ACTION PLAN (EAP)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed	
Yes / No	A	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	A	02. Are EAP training exercises conducted annually? [EKMS-1 (Series), Annex H, paragraph 6.d]	
Yes / No	A	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	A	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	A	05. When planning for natural disasters, does the EAP provide for: [EKMS-1(Series), Annex H, paragraph 4]	
Yes / No	A	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?	

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

SECTION 11 - EMERGENCY DESTRUCTION PLAN (EDP)

Unless otherwise 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	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	01. Does the LE have an Emergency Destruction Plan (EDP) incorporated into its EAP? [EKMS-1 (Series), Annex H, paragraph 2.c]
Yes / No	A	02. 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	A	03. 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	A	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 H, paragraph 5.e]
Yes / No	A	05. Are the priorities of destruction indicated in the plan? [EKMS-1 (Series), Annex H, paragraph 8]
Yes / No	A	06. Is the EDP divided into two parts: one for precautionary and one for complete destruction? [EKMS-1 (Series), Annex H, paragraph 7]
Yes / No	A	07. 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	A	08. Does the EDP stress that accurate information concerning the extent of

ANNEX B

LOCAL ELEMENT (ISSUING AND USING)

		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	A	09. 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	A	10. 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]

COMMENTS :

ANNEX C

VAULT INSPECTION GUIDE

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the Auditor conducting the EKMS/KOA Audit. The criteria in this Annex applies to shore-based vaults used to store keying material constructed and approved prior to 01 Jan 2013. Shore-based vaults used to store keying material which are constructed or structurally modified 01 Jan 2013 or later must obtain facility approval based on ICD-705 requirements.

Per Chapter 2 and Article 401.c of this manual, Audit Reports evaluated as unsatisfactory shall include references and comments to substantiate the evaluation. Below each item reviewed, space is provided to respond to any questions that receive a negative response in order to aid EKMS/KOA Auditors and commands when conducting the out-brief and writing the official report of inspection results.

Note: Non-compliance with a particular item contained in either Annex C or D, as applicable may not translate to a specific COMSEC incident or PDS as defined in EKMS - 1(series) articles 945 and 1005. When not defined otherwise, discrepancies will be noted as Administrative Discrepancies and counted as such when assessing the account in the final report (for biennial audits). The minimum construction requirements derived from EKMS - 1(series) Annexes N and O, as applicable must be met prior to an activity receiving facility approval and biennially thereafter for continued storage of classified COMSEC material. Initial facility approval or continued approval (in the form of the COR Audit Report) should not be granted without consulting NCMS and requesting a waiver for any non-compliant items noted.

VAULT CHECKLIST

Answer	Area/Item Reviewed
Yes / No	<p>1. For class "A" vault, (authorized for storage of TOP SECRET and below keying material), are the following constructed properly and with approved materials? [EKMS-1(Series), Annex I, Paragraph 2]</p> <p>a. <u>Floors and walls</u>: Poured, reinforced concrete, <u>minimum 8" thick reinforcing rods</u> at least 3/8" in diameter, mounted vertically and horizontally on center not less than two inches and not greater than ten inches. Wall shall connect solidly with the vault roof and floor.</p>
Yes / No	<p>b. <u>Roof</u>: Single piece, reinforced-concrete slab of a thickness to be determined by structural requirements, but not less than the walls and floors.</p>
Yes / No	<p>c. <u>Ceiling</u>: Where existing floor-to-ceiling exceeds 12 feet, a vault roof, structurally equal to the vault walls, may be constructed at a height determined by structural limitations, size of equipment to be enclosed, optimum utilization of existing enclosed air space, and specific user requirements.</p> <p>Note: Where the existing roof does not conform to the vault roof requirements stated above, a vault roof, which is structurally equal to the vault walls shall be constructed.</p>
Yes / No	<p>d. <u>Vault Door and Frame Unit</u>: Shall afford protection not less than that provided by a Class 5 vault door specified in Interim Federal Specification AA-D-600 (GSA-FSS), Door, Vault, Security.</p>
Yes / No	<p>e. <u>Lock</u>: A combination lock that conforms to the Underwriters' Laboratories, Inc. Standard No. 768, for Group 1R or Group 1. The specific lock model used shall bear a valid UL Group 1R or Group 1 label.</p> <p>Note: Vault doors procured after 14 April 1993 must be equipped with a GSA-approved combination lock that meets, at a minimum the requirements of Federal Specifications FF-L-2740/A. [EKMS-1 (Series), Annex I , paragraph 2]</p>
	<p>2. Are shore based CMS storage vaults equipped with the following <u>minimum</u> safety requirements: [EKMS-1 (Series), Annex I , paragraph 5.a]</p>
Yes / No	<p>a. A luminous type light switch? [May be painted with fluorescent paint]</p>
Yes / No	<p>b. Is emergency lighting installed?</p>
Yes / No	<p>c. An interior alarm switch or device? (e.g.,</p>

	telephone, intercom)
Yes / No	d. A decal containing emergency instructions on how to obtain release if locked inside the vault?
	3. If an emergency escape device is considered necessary, have the following <u>minimum</u> requirements been met: [EKMS-1 (Series), Annex I, paragraph 5.b]
Yes / No	a. Is it permanently attached to the inside of the door and <u>cannot</u> be activated by the exterior locking device, or otherwise accessible from the outside?
Yes / No	b. Is it designed and installed so that drilling and rapping the door from the outside will <u>not</u> give access to the vault by activating the escape device?
Yes / No	c. Does the device meet the requirements of GSA Federal Specification AA-D-600 series (GSA-FSS) paragraph 4.4.8, regarding an exterior attack on the door?
	4. If an emergency escape device is not provided, have the following approved Underwriters Laboratories (UL), Inc., devices been installed in the vault: [EKMS-1 (Series), Annex N, paragraph 5.c]
Yes / No	a. A UL Bank Vault Emergency Ventilator?
Yes / No	b. At least one UL approved fire extinguisher situated in a position near the vault door?
Yes / No	5. Are emergency destruction tools readily available? [EKMS-1 (Series), Annex H, paragraph 5.d and 6.c]
Yes / No	6. Is the space/compartments or vault which contains COMSEC material outwardly identified as "RESTRICTED AREA/AUTHORIZED PERSONNEL ONLY"? [OPNAVINST 5530.14 (series), Articles 210 and 218.]
Yes/No/NA	7. 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	8. Is a central record of combinations maintained in a security container, approved for storage of the highest classification of the material protected by the combination locks, for each vault used for the storage of COMSEC material? [EKMS-1 (Series), Article 515.e]

Yes / No	<p>9. If the original security integrity of the vault has been degraded in any way, have approved repairs been made and documented? [SECNAV-M 5510.36, Article 10-15]</p> <p>Note: If external modifications are made after 01 Jul 93, the container or vault door is no longer authorized to store <u>any</u> classified material. [EKMS-1 (Series), Article 520.f]</p>
Yes / No	<p>a. Is the gate frame made of not less than 3/8" by 1 1/2" steel members, and equipped with a locking device arranged to permit locking and unlocking of the gate from the inside?</p>

ANNEX D

FIXED COMSEC FACILITY INSPECTION GUIDE

PURPOSE: To provide a checklist for use by personnel tasked with certifying/recertifying a vault used for storage of COMSEC material to ensure it meets the minimum physical security safeguards. *[As stated in EKMS-1(series), COMSEC Facilities approved by an Accrediting Official in accordance with ICD-705 (SCIF) or JAFAN 6/9 (SAPF) standards shall be assumed to comply with the standards contained herein and do not require separate facility approval or further inspection by COMSEC personnel].*

INITIAL REQUIRED DATA:

Date of Audit: _____

Command Audited: _____

EKMS/KOA Account number: _____

Immediate Superior in Command: _____

Date of Last CMS COR Audit: _____

Name/Grade/Rate and Command of CMS COR Auditor:

Date of Last Facilities Approval: _____

EKMS/KOA Manager Name/Grade: _____

Alternate EKMS/KOA Manager Name/Grade/Date of Appointment:

Identify Following, as Applicable/Assigned:

Second Alt. EKMS/KOA Manager Name/Grade/Date of Appointment

Third Alt. EKMS/KOA Manager Name/Grade/Date of Appointment

Remarks: _____

ACTION. The following audit checklist shall be used and completed in its entirety by the Auditor conducting the CMS COR Audit. Per Chapter 2 and Article 401.c of this manual, unsatisfactory Audit Reports shall include references and comments to substantiate the evaluation. Below each item reviewed, space is provided to respond to any questions that receive a negative response and will aid CMS COR Auditors and commands when conducting the out-brief and writing the official report of audit results.

Note: Non-compliance with a particular item contained in either Annex C or D, as applicable may not translate to a specific COMSEC incident or PDS as defined in EKMS - 1(series) articles 945 and 1005. When not defined otherwise, discrepancies will be noted as Administrative Discrepancies and counted as such when assessing the account in the final report (for biennial audits). The minimum construction requirements derived from EKMS - 1(series) Annexes I and J, as applicable must be met prior to an activity receiving facility approval and bi-annually thereafter for continued storage of classified COMSEC material. Initial facility approval or continued approval (in the form of the COR Audit Report) should not be granted without consulting NCMS and requesting a waiver for any non-compliant items noted.

FIXED COMSEC FACILITY CHECKLIST

Answer	Area/Item Reviewed
Yes / No	1. Is the facility constructed of solid, strong materials that deter and detect unauthorized penetration? [EKMS-1 (Series), Annex J, paragraph 2]
Yes / No	2. Does the facility provide adequate attenuation of internal sounds that would divulge classified information through walls, doors, windows, ceilings, air vents, and ducts? [EKMS-1 (Series), Annex J, paragraph 2]
Yes / No	3. Are walls constructed from true floor to true ceiling? [EKMS-1 (Series), Annex J, paragraph 3.a]
Yes / No	4. Are ceilings at least as thick as the outer walls and offer the same level of security as the outer walls? [EKMS-1 (Series), Annex J, paragraph 3.b]
Yes / No	5. If <u>false</u> ceilings are used, are additional safeguards used to resist unauthorized entry (e.g., installed, approved intrusion detection system (IDS) in the area above the false ceiling)? [EKMS-1 (Series), Annex J, paragraph 3.c]
Yes / No	6. Is only one door used for <u>regular</u> entrance to the facility, though other doors may exist for emergency exit and entry or removal of bulky items? [EKMS-1 (Series), Annex J, paragraph 4]
Yes / No	7. Do all doors remain closed during facility operations and only opened to admit authorized personnel or materials? [EKMS-1 (Series), Annex O, paragraph 4.a]
Yes / No	8. Do the main entrance facility doors comply with the following standards: [EKMS-1 (Series), Annex J, paragraph 4.b]
Yes / No	<p>a. Does the door have sufficient strength to resist forceful entry? (In preference order, examples of acceptable doors are: GSA-approved vault doors, Standard 1-3/4" internally reinforced, hollow metal industrial doors, <u>or</u> metal-clad or solid hardwood doors with a <u>minimum</u> thickness of 1-3/4").</p> <p>Note: Unattended telecommunications facilities constructed after 1993 shall have only one door.</p>
Yes / No	<p>b. Is the door frame securely attached to the facility and fitted with a heavy-duty/high security strike plate, and hinges installed with screws long enough to resist removal by prying?</p>

Yes / No	c. Is the door installed as to resist removal of hinge pins? (This can be accomplished by either installing the door so that the hinge pins are located inside the facility, or by set screwing/welding the pins in place.)
Yes / No	d. If the facility is <u>not</u> continuously manned, is the door equipped with a GSA-approved, electro-mechanical lock meeting, at a minimum Federal Specification FF-L-2740/A? [EKMS-1 (Series), Annex J, paragraph 4.b]
Yes / No	9. If the <u>facility</u> is continuously manned (a built-in lock is <u>not</u> required), is the door designed so that a GSA-approved electro-mechanical lock Meeting Federal Specification FF-L-2740/A and dead bolt can be affixed to the outside should it ever become necessary to lock the facility? (e.g., in case of emergency evacuation.) [EKMS-1 (Series), Annex J, paragraph 4.b] Note: An electronically activated lock (e.g., cipher lock or keyless push-button lock) may be used on the entrance door to facilitate the admittance of authorized personnel when the facility is operationally manned. However, these locks do <u>not</u> afford the required degree of protection and <u>may not</u> be used to secure the facility when it is not manned.
Yes / No	10. Do other doors (e.g., emergency exit doors and doors to loading docks) meet the same installation requirements as the main facility entrance doors, and designed so that they can only be opened from <u>inside</u> the facility? [EKMS-1 (Series), Annex J, paragraph 4.b] Note: Approved panic hardware and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the <u>interior</u> surfaces of other doors to the facility.
Yes / No	11. Is the entrance area equipped with a device which affords personnel desiring admittance the ability to notify personnel within the facility of their presence? [EKMS-1 (Series), Annex J, paragraph 4.b(4)]
Yes / No	12. Is a method employed to establish <u>positive</u> visual identification of a visitor before entrance is granted? [EKMS-1 (Series), Annex J, paragraph 4.b]
Yes / No	13. Is the entrance designed in such a manner that an individual cannot observe classified activities until cleared for access into the restricted spaces? [EKMS-1 (Series), Annex J, paragraph 4.b]

Yes / No	14. Where windows exist, are they secured in a permanent manner to prevent them from being opened? (COMSEC facilities should not normally contain windows.) [EKMS-1 (Series), Annex J, paragraph 5]
Yes / No	15. Are windows alarmed and/or barred to prevent their use as an access point? [EKMS-1 (Series), Annex J, paragraph 5.a]
Yes / No	16. Is observation of internal operations of the facility denied to outside viewing by covering the windows from the inside, or otherwise screening the secure area from external viewing? [EKMS-1 (Series), Annex J, paragraph 5.b]
Yes / No	17. Are other openings such as air vents, ducts, or any similar openings which breach the walls, floor, or ceiling of the facility, appropriately secured to prevent penetration? [EKMS-1 (Series), Annex J, paragraph 6]
Yes / No	18. Do openings which are less than 96 square inches, have approved baffles installed to prevent an audio or acoustical hazard? [EKMS-1 (Series), Annex J, Paragraph 6.a]
Yes / No	19. If the opening exceeds 96 square inches, are acoustical baffles supplemented by either hardened steel bars or an approved intrusion detection system (IDS)? [EKMS-1 (Series), Annex J, paragraph 6.b]

ANNEX E

CMS COR AUDIT REPORT

EXAMPLE

From: (CMS COR Auditor)
To: (ISIC/IUC)
Commanding officer, Naval Communications Security
Material System

Subj: REPORT OF CMS COR AUDIT OF (COMMAND TITLE)

Ref: (a) EKMS-3(Series)

1. Title of command audited: _____
EKMS/KOA Manager: _____
Primary Alternate Manager: _____
EKMS/KOA ID Number: _____
Date audited: _____
Audited by: _____
(Name, Rank/Rate/Grade)
CMS COR Auditor Certification: _____
(Date Certified/Re-certified)
Audited Command ISIC/IUC: _____
Certifying COR Auditor: _____

2. Evaluation of the command or unit audited, [GRADE: (SAT or UNSAT)] and comments as required to substantiate the evaluation. Evaluation Criteria is in accordance with reference (a) Article 205.d.3.

COMSEC INCIDENTS:
REPORTABLE/NON-REPORTABLE PDS:
ADMINISTRATIVE ERRORS:
OVERALL: SAT/UNSAT

3. Findings:

a. List each finding/discrepancy which is significantly important to require action. Cite the appropriate reference(s) for each finding/discrepancy noted.

Do not list items of a minor administrative nature.

b. Immediately below each finding, list and briefly discuss any corrective actions recommended to resolve the discrepancies listed above.

4. Any additional comments or remarks.

5. The facility meets all physical security standards and continued approval to hold classified COMSEC material up to the level of is authorized.

6. [In accordance with reference (a), copies of this report, portions thereof, or correspondence related thereto, from a source external to the Department of the Navy shall include the appropriate caveat included in Articles 410.a - 410.c to EKMS-3(Series), as applicable]

7. Commands must provide a written report describing what actions were taken to correct discrepancies that were noted during the inspection. This report shall be forwarded to the ISIC/IUC and NCMS//N7// within 30 days from the day of the audit.

R. U. UNDERWAY

ANNEX F

CMS COR AUDIT FEEDBACK REPORT

EXAMPLE

FM (ISIC/IUC)
TO NCMS WASHINGTON DC
INFO CHAIN OF COMMAND
CMS COR AUDIT XXXXXXXXXXXX (X = LOCAL COR AUDIT TEAM)
BT
UNCLAS //N02201//
MSGID/GENADMIN/(ORIG ISIC/IUC PLA)/MONTH//
SUBJ/EKMS/KMI ACCOUNT FEEDBACK REPORT//
REF/A/DOC/NCMS/XXAPR2017//
AMPN/REF A IS EKMS-3(SERIES)//
POC/R. U. UNDERWAY/ITCS(SW)/EDDIE.UNDERWAY@NAVY.MIL/-/DSN:321-
7654//
RMKS/1. IAW ARTICLE 405 TO REF A, THE FOLLOWING FEEDBACK AND
RECOMMENDATIONS FOR CHANGE ARE SUBMITTED HEREIN. BE SURE TO
PROVIDE APPLICABLE SUPPORTING DOCUMENTATION.//

BT

ANNEX G

CMS COR ISIC/IUC AUDIT ENDORSEMENT

EXAMPLE

From: ISIC/IUC

To: Audited Command

Subj: ENDORSEMENT ON (INSPECTED COMMAND) CMS COR AUDIT DATED DD
MMM YY LTR (SERIAL NUMBER OF AUDIT REPORT)

Ref: (a) EKMS-1 (Series) Article 110.e
(b) Audit Report

1. In accordance with reference a, you are hereby directed to complete the corrective actions on the deficiencies noted in reference b.

2. A follow-up report is required to be sent to your (ISIC/IUC) no later than 30 days after receipt of the formal audit report.

R. U. Underway
CTF 99, N61