NAVAL COMMUNICATIONS SECURITY MATERIAL SYSTEM

EKMS 3C

ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) INSPECTION MANUAL

5 Apr 2010

DEPARTMENT OF THE NAVY
COMMUNICATION SECURITY MATERIAL SYSTEM

IN REPLY REFER TO:
5040
Ser N7/

LETTER OF PROMULGATION

1. **PURPOSE.** The Electronic Key Management System Inspection Manual (EKMS 3C) promulgates policy and procedures for conducting EKMS Inspections of Department of the Navy (DON) and Coast Guard commands, including contracted support personnel. The guidance in this manual is based on policy and procedures set forth in both National and Navy COMSEC publications.

2. **ACTION.** EKMS 3C is effective upon receipt and replaces all previously issued and dated EKMS inspection guidance.

3. **REPRODUCTION.** EKMS 3C is a web-based publication which is available for viewing and downloading via the NCMS unclassified website located at:
https://www.portal.navy.mil/cyberfor/NCMS/default.aspx
under the EKMS Managers – COMSEC Library tab. EKMS 3C is authorized for reproduction and use in any operational environment.

4. **COMMENTS.** Submit comments, recommendations, and suggestions for changes to, Naval Communications Security Material System (NCMS).

/s/

M. C. KESTER

KESTER.MARK.C.1037481765
Digitally signed by KESTER.MARK.C.1037481765
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=KESTER.MARK.C.1037481765
Date: 2013.04.25 11:35:44 -04'00'

LIST OF EFFECTIVE PAGES

PAGE NUMBER

Front Cover	(unnumbered)	ORIGINAL
Letter of Promulgation	i	ORIGINAL
List of Effective Pages	ii	AMD 7
Record of Amendments	iii	ORIGINAL
Record of Page Checks	iv	ORIGINAL
Table of Contents	v-vi	AMD-7
Chapter 1	1-1 thru 1-4	AMD-7
Chapter 2	2-1 thru 2-4	AMD-7
Chapter 3	3-1 thru 3-3	AMD-7
Chapter 4	4-1 thru 4-3	AMD-7
(ANNEX A)	A-1 thru A-49	AMD-7
(ANNEX B)	B-1 thru B-30	AMD-7
(ANNEX C)	C-1 thru C-27	AMD-7
(ANNEX D)	D-1 thru D-4	AMD-7
(ANNEX E)	E-1 thru E-6	AMD-7
(ANNEX F)	F-1 thru F-2	AMD-7
(ANNEX G)	G-1 thru G-2	AMD-7
(ANNEX H)	H-1	AMD-7
(ANNEX I)	I-1	AMD-7
BACK COVER (REVERSE BLANK)	(unnumbered)	ORIGINAL

RECORD OF AMENDMENTS

Identification of Amendment	Date Entered (YYMMDD)	By Whom Entered(Signature, Rank or Rate, Command Title)
AMD 1 (ALCOM 108/10)	2010/07/06	M. J. Phillips, IA-04, NCMS PHILLIPS.MILLARD.J.III.1114056975 Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PHILLIPS.MILLARD.J.III.1114056975 Date: 2013.04.25 11:29:08 -04'00'
AMD 2 (ALCOM 161/10)	2010/10/29	M. J. Phillips, IA-04, NCMS PHILLIPS.MILLARD.J.III.1114056975 Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PHILLIPS.MILLARD.J.III.1114056975 Date: 2013.04.25 11:29:27 -04'00'
AMD 3 (ALCOM 020/11)	2011/01/29	M. J. Phillips, IA-04, NCMS PHILLIPS.MILLARD.J.III.1114056975 Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PHILLIPS.MILLARD.J.III.1114056975 Date: 2013.04.25 11:29:41 -04'00'
AMD 4 (ALCOM 085/11)	2011/04/30	M. J. Phillips, IA-04, NCMS PHILLIPS.MILLARD.J.III.1114056975 Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PHILLIPS.MILLARD.J.III.1114056975 Date: 2013.04.25 11:29:54 -04'00'
AMD 5 (ALCOM 213/11)	2011/12/29	M. J. PHILLIPS, IA-04, NCMS PHILLIPS.MILLARD.J.III.1114056975 Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PHILLIPS.MILLARD.J.III.1114056975 Date: 2013.04.25 11:30:07 -04'00'
AMD 6 (ALCOM 111/12)	2012/06/29	M. J. PHILLIPS, GG-13, NCMS PHILLIPS.MILLARD.J.III.1114056975 Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PHILLIPS.MILLARD.J.III.1114056975 Date: 2013.04.25 11:30:22 -04'00'
AMD 7 (ALCOM 079/13)	2013/04/23	M. J. PHILLIPS, GG-13, NCMS PHILLIPS.MILLARD.J.III.1114056975 Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PHILLIPS.MILLARD.J.III.1114056975 Date: 2013.04.25 11:30:41 -04'00'

RECORD OF PAGECHECKS

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

TABLE OF CONTENTS

LIST OF ANNEXES

CHAPTER 1 – INTRODUCTION TO THE ELECTRONIC KEY MANAGEMENT SYSTEM

(EKMS) INSPECTION/AUDIT PROGRAM

101. PURPOSE. This manual prescribes policies and procedures related to conducting formal Communications Security (COMSEC) inspections of Electronic Key Management System (EKMS) accounts within the Department of the Navy (DON), including U.S. Navy, Military Sealift Command (MSC), Marine Corps, Coast Guard (COGARD), and contracted support personnel. Annexes A through F pertain.

105. SCOPE AND APPLICATION:

a. **Source.** The policies and procedures in this manual are derived from National, Department of Defense (DOD), and DON COMSEC policy manuals

b. **Scope.** EKMS-3C establishes certification standards for EKMS Inspectors and criteria for conducting EKMS inspections. Additional requirements may be imposed by the Commandant of the Marine Corps (CMC //C4/CY//), Coast Guard (COGARD) C4ITSC, Fleet Commanders (FLTCOMS), Type Commanders (TYCOM), Immediate Superiors in Command (ISIC/IUC), and Immediate Unit Commanders (IUC) for supported commands, units and activities.

c. **Application.** The COMSEC requirements in this manual apply to all DON (MSC, USCG, USMC, USN) EKMS accounts and ISIC/IUCs whose subordinate activities maintain a numbered EKMS account.

d. **Recommendations.** Recommended changes to this instruction will be submitted to Naval Communications Security Material System (NCMS), EKMS Education and Training Department (N7), via the administrative chain of command.

110. DEFINITIONS:

a. **Audit/Inspection.** A formal, independent review and examination of records and activities conducted to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. The examination shall be conducted by an authority from a different organization than that of the inspected facility. The examination shall be concluded with a formal out-brief to

recommend necessary changes in controls, policies, or procedures.

b. **CMS A&A Periodic Training Visit**. On-site refresher training is not to be used in lieu of the unannounced biennial EKMS inspection in the management and handling of COMSEC material. CMS A&A Periodic Training Visits are mandatory for DON accounts (MSC, USCG, USMC, and USN) and may be conducted as early as 12 Months after the last inspection but not later than 90 days prior to the required 24 month "biennial" inspections. ISIC/IUCs will track and enforce compliance during command EKMS inspections.

c. **Electronic Key Management System (EKMS)**. The logistics and accounting system through which electronic key is accounted, distributed, generated, controlled, destroyed and safeguarded. It also provides management of physical key and non-key COMSEC-related items.

d. **Communications Security (COMSEC)**. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning National security; protective measures taken to ensure the authenticity of such telecommunications.

e. **Follow-up**. The process of ensuring an inspected account has completed the necessary corrective actions on deficiencies and recommendations noted in an inspection report. The inspected account shall complete this action by sending a follow-up report to their ISIC/IUC no later than 30 days after receipt of the formal inspection

f. **Physical Security Inspection**. An examination by a Certified Inspector of an activity's physical security and loss prevention programs to determine compliance with physical security policy. Annexes E and F pertain. Categories of inspections include:

(1) Navy and Military Sealift Command. A physical security inspection is normally conducted by the ISIC/IUC. Follow-up action to correct noted deficiencies is required.

(2) 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 their subordinate commands.

(3) Coast Guard. A specific, on-site examination of any facility or activity conducted by authorized COMSEC or physical security personnel to determine vulnerabilities and compliance with physical security policies as established in COMDTINST M5530.1 (series).

g. **Physical Security Survey**. 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. At the discretion of the Commanding Officer, the completed NAVMC 11121 may be used as part of the physical security inspection.

> **NOTE**: For USMC accounts – 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.

115. RESPONSIBILITY:

a. **Commander, Navy Cyber Forces**. COMNAVCYBERFOR implemented the EKMS Inspection Program for the DON and U.S. Coast Guard.

b. **Naval Communications Security Material System (NCMS)**. NCMS administers the EKMS Inspection Program for the DON and the Coast Guard.

c. **Immediate Superior in Command/Immediate Unit Commander (ISIC/IUC)**. The ISIC/IUC is responsible for conducting required EKMS Inspections (Annexes A and B) and facility approvals (Annexes C and D) for their subordinate activities. Within the Marine Corps, the ISIC/IUC is the command with administrative control over a unit.

d. **EKMS Inspection Team Leader**. The senior certified EKMS Inspector assigned to and in charge of the EKMS Inspection Team. The EKMS Inspection Leader is responsible to the ISIC/IUC for the proper conduct and reporting of the EKMS Inspection in accordance with this instruction and supplementary guidance provided by the ISIC/IUC.

e. **EKMS Inspection Team Member**. EKMS Inspection Team Members are responsible to the EKMS Inspection Team Leader for properly conducting that portion of the EKMS Inspection assigned. All discrepancies identified by an EKMS Inspection Team Member will be validated by the EKMS Inspection Team

Leader.

120. SPECIAL NOTES:

a. **Electronic Key Management System (EKMS) Manager**. An individual, designated in writing by the Commanding Officer, responsible for maintaining required files and ensuring the proper safeguarding, storage, and disposition of COMSEC material/equipment assigned to a command's EKMS numbered account.

b. **Local Element (LE)**. Individual responsible for maintaining requires files and ensuring the proper safeguarding, storage and usage of COMSEC material issued from an EKMS numbered account or from another Local Element (Issuing).

CHAPTER 2 – EKMS INSPECTION POLICY AND PROCEDURES

201. GENERAL POLICY: ISIC/IUCs must conduct **unannounced** EKMS Inspections of their subordinate commands and units every 24 months (biennially). ISIC/IUCs are also responsible for initial physical security facility approval and re-certification for COMSEC material storage. EKMS inspections shall **only** be performed by Certified Inspectors who meet the designation requirements in Article 301 of this manual and are appointed in writing by their Parent Command. **A copy of all EKMS Inspection reports must be forwarded to NCMS//N7//.**

> **NOTE:** Within the Marine Corps, the inspected command will provide the EKMS Inspector with a copy of the most recent physical security survey to be used as a basis for initial physical security facility approval and re-certification.

205. EKMS INSPECTION PROCESS:

a. **EKMS Inspection**. The EKMS Inspection shall be conducted in detail to evaluate the safeguarding, accounting and disposition of COMSEC material within a COMSEC account. An inspection will include the Local Account and **all** Local Element(s) (LEs). The inspection checklists, contained in Annexes A through E, will be used as inspection guidelines. However HQ CMC, COGARD TISCOM, MSC, FLTCINCs, TYCOMs and ISIC/IUCs may supplement Annexes A through E with additional, service-specific requirements. Additional requirements incorporated into the inspection guides shall contain references of source documents that reflect the most current COMSEC policy and procedures. EKMS Managers who are also designated as EKMS Inspectors are not authorized to conduct formal EKMS Inspections on their own accounts or their LEs; however, they may conduct spot-checks at their discretion.

> **NOTES:** 1. At accounts where a significant portion of LE's are external LE's supported through a Letter of Agreement, a minimum of three must be inspected.

2. LEs which are not collocated within a 50 mile radius of the inspected command may be exempted from the inspection at the discretion of the inspecting command.

3. The EKMS Inspection process is specifically designed to assess both the handling of COMSEC material and the

accounts management practices. The EKMS Inspector is tasked with identifying both non-compliance with applicable policies and also analyzing factors or trends impeding effective account management and offering recommendations for improvement. Although the primary purpose of the inspection is to ensure compliance with applicable Navy policy in COMSEC handling, the opportunity to train and educate should be incorporated into the process to enable the command inspected to implement effective practices and training programs to properly account for, maintain and use COMSEC material required to support mission readiness.

4. At the discretion of the inspector, to gain some insight as to the knowledge and understanding in policy and procedural matters of both EKMS Managers and LE personnel, the inspection may encompass either querying such personnel on policies and procedures or a demonstration of commonly performed functions, i.e. inventorying COMSEC material, performing routine destruction, or conducting audit trail reviews. Weaknesses in such areas may be an indication of deficiencies or the need for additional training to ensure COMSEC material is properly managed.

b. **Pre-Inspection Guidelines**. Prior to conducting an EKMS Inspection, the Inspector(s) shall:

(1) Become familiar with other available regulations and directives of higher authority that apply to the command or unit to be inspected.

(2) Research the most recent history on the management of the EKMS account to include:

(a) Previous EKMS Inspections.

(b) Previous CMS A&A Periodic Training Visits.

(c) Documentation of previously identified deficiencies and status of corrective actions taken to mitigate to mitigate re-occurrence.

(d) Information related to COMSEC incidents or Practices Dangerous to Security (PDS's) encountered by the unit.

(3) Review areas of special interest identified by NCMS, ISIC/IUC or higher authority.

c. **Approval of COMSEC Facilities**. In accordance with EKMS-1 (Series) article 550.

d. **Evaluation Criteria**. Upon completion of the inspection, an evaluation of either Satisfactory or Unsatisfactory will be assigned. The following minimum standards will be used to evaluate inspection results as unsatisfactory:

(1) One (1) COMSEC Incident. (Incidents identified by the Inspector during the course of inspection.)

or

(2) Three (3) Practices Dangerous to Security (PDS). (Includes Reportable and Non-reportable PDS's **identified by the Inspector during course of inspection.**)

or

(3) Major administrative errors that exceed: The inspector must obtain the total line items from the most current inventory. Accounts with:

(a) up to 120 line items, maximum of 10 errors.

(b) between 121 and 250 line items, maximum of 20 errors

(c) between 251 and 400 line items, maximum of 30 errors

(d) between 401 and 500 line items, maximum of 35 errors

(e) 501 or greater line items, maximum of 40 errors

NOTE: During the review of the administrative process, Inspectors should also attempt to identify trends of common repetitive errors (e.g., repeatedly missing initials on line-outs, appropriate blocks not marked on a SF-153 to indicate the applicable action denoted by the SF-153. i.e. received, inventoried, destroyed, witness, or other. Repetitive administrative errors should be graded as one error.

(4) If an account receives a grade of Satisfactory but the Inspector has noted particular trends or other avenues which could benefit from either additional clarity in local policy or training, such recommendations will be included in the final

report. A follow-up visit/inspection by the ISIC/IUC on the areas in need of improvement is recommended to ensure the concerns to not become repetitive or ongoing in nature. When not possible due to distance, funding, etc… the unit inspected should report actions taken to the ISIC/IUC via email, message, or official letter, as desired.

(5) Inspectors shall include the overall condition of the EKMS account along with the number and description of any administrative discrepancies, PDS's, and/or COMSEC Incidents discovered in the official inspection report.

(6) The biennial inspection performed by the ISIC/IUC (or, in the absence of a qualified inspector at the unit's ISIC/IUC, an inspector assigned by NCMS//N7//) is the only authorized, formal EKMS Inspection. **No other entities will conduct COMSEC inspections.**

e. **Re-Inspection**. If an account being inspected receives a grade of Unsatisfactory on an EKMS Inspection or fails their COMSEC/Physical storage facility certification/re-certification:

(1) An EKMS re-inspection will be conducted at the discretion of the ISIC/IUC but no later than 90 days from the date of failure.

(2) 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) Appendix IV.

> **NOTE:** Per OPNAVINST 5530.14(series) Appendix IV, approved waivers 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 Naval facilities, waiver requests must be forwarded to CNO//N09N//, information copy to NCMS//N5//, in order to continue to hold COMSEC material.

CHAPTER-3 - ASSIGNMENT OF EKMS INSPECTORS

301. DESIGNATION REQUIREMENTS FOR EKMS INSPECTORS. ISIC/IUCs must ensure that their personnel meet the following minimum requirements prior to appointment as EKMS Inspectors:

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

b. Possess a Top Secret clearance.

NOTE: EKMS Inspectors and CMS A&A Training Team members are **not** required to be SCI Indoctrinated unless an EKMS Inspector is also a manager of an account validated for SCI/SI material. If an EKMS Inspector is a manager of an account validated for SCI/SI material they must be SCI indoctrinated in accordance with EKMS-1(series).

c. Inspection Team Leaders must be E-7 (GS-9/Band 2 for Civilian Government Service employees) or higher.

d. Inspection Team Members must be E-6 (GS-7/Band 1 for Civilian Government Service employees) or higher.

e. Inspection Team Leaders must have previously served as an EKMS Manager or alternate for at least one year within the previous 24 months.

f. Team Members must have served at least as an EKMS alternate and should be thoroughly knowledgeable of COMSEC policies and procedures.

g. Attend a classroom EKMS Inspector Training Seminar conducted by one of the CMS Advice and Assistance (A&A) Teams as listed in EKMS-1 (Series).

h. Within 60 days after completing the EKMS Inspector Training Seminar:

(1) Assist with a minimum of two CMS A&A Periodic Training Visits.

(a) Observe one CMS A&A Periodic Training Visit.
(b) Conduct one CMS A&A Periodic Training Visit using all applicable Annexes from this publication.

(2) Participate in two EKMS Inspections with a Certified EKMS Inspector. This requirement is waived for the re-

certification of current EKMS Inspectors.

(a) Observe one EKMS Inspection with a Certified EKMS Inspector.

(b) Conduct one EKMS Inspection while being observed by a Certified EKMS Inspector **(USN/USMC)**.

NOTE: USCG personnel must conduct a minimum of four EKMS Inspections with a certified EKMS Inspector.

305. RECOMMENDATION FOR ASSIGNMENT. Upon completion of the requirements in Article 301, the CMS A&A team providing the training will forward the EKMS Inspector Qualification standards check list to NCMS N7. NCMS will review the package for completeness, then forward a certification letter to the individuals Parent Command (via the servicing A&A Team) recommending assignment as an EKMS Inspector. The Parent Command will then appoint the Inspector in writing. For Marine Corps accounts NCMS will send the recommendation letter to:

Headquarters U.S. Marine Corps FOB
2 Navy Annex, Room 3217
ATTN: C4/C4IA EKMS PROGRAM MANAGER
WASHINGTON, D.C. 20380-1775.

In order for an EKMS Inspector to retain their certification, personnel must re-attend the EKMS Inspector Training Seminar under the following situations:

a. Every 36 months while assigned as an EKMS Inspector.

b. Personnel re-assigned as an EKMS Inspector that have been out of the program for a period exceeding 12 months, provided no other designation requirements were previously waived found to be out of compliance.

c. Additional training, as directed.

Upon completion of a subsequent EKMS Inspector Training Seminar, NCMS will forward a letter of recommendation for continued assignment as an EKMS Inspector to the individual's command.

NOTES: (1) Letters of Certification for Coast Guard personnel will be forwarded to Coast Guard TISCOM (TS-OPS-4). Letters of Certification for Marine Corps personnel will be forwarded to Headquarters U.S. Marine Corps,

C4/C4IA.

(2) NCMS reserves the right to withdraw inspector certification recommendations when disqualifying or other questionable information becomes available. Withdrawal of the recommendation by NCMS will be via official letter to the Inspector's Parent Command. Additionally, the Inspectors parent organization must notify NCMS via official channels if a certified Inspector has his/her access to classified material suspended or security clearance revoked.

310. EKMS INSPECTOR ASSISTANCE. On occasion, an ISIC/IUC may require assistance in assigning an EKMS Inspector due to the unavailability of a qualified EKMS Inspector on staff. ISIC/IUC's shall first request assistance from the next senior in command. If an Inspector is not available, a request for assistance shall be forwarded to NCMS WASHINGTON DC//N7//. Requests should be submitted 90 days prior to the inspection date to facilitate scheduling. NCMS will identify a qualified EKMS Inspector in the geographical area of the account and coordinate, as needed. The assigned EKMS Inspector will conduct the EKMS Inspection on behalf of and under the authority of the requesting ISIC/IUC. The ISIC/IUC should assist the assigned EKMS Inspector in obtaining any unique supplemental requirements, which apply to the inspected command as outlined in Article 205. The requesting ISIC/IUC is responsible for and must provide the necessary funding data for travel and per diem costs required by the EKMS Inspector and/or supported personnel prior to the travel being executed.

CHAPTER–4 - EKMS INSPECTION REPORTING PROCEDURES

401. CONTENT AND SUBMISSION GUIDELINES:

a. Significant deficiencies discovered by the inspecting officials that appear to require action by higher-level authorities must be reported immediately to the Commanding Officer (CO) of the inspected command.

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

c. Formal EKMS Inspection reports must include references and comments to substantiate the evaluation. All formal EKMS Inspection reports must contain recommendations for correcting deficiencies. (See Annex F for an example of an EKMS Inspection report.

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

e. Formal EKMS Inspection reports will be submitted by the EKMS Inspector to the appropriate ISIC/IUC for endorsement and forwarding to the inspected command. The endorsement **will direct the inspected command to correct the deficiencies and return a report of corrective measures per Article 110.e.** and Annex I of this manual. In certain situations (i.e. Echelon Two commands), the EKMS Inspector may have difficulty determining the ISIC for the command inspected, in this circumstance, contact NCMS//N7// immediately for additional guidance.

f. ISICs/IUCs are required to submit **semi-annual** EKMS reports to NCMS WASHINGTON DC//N7// IAW Annex G of this manual.

> **NOTE:** Marine Corps IUCs must submit their **semi-annual** EKMS report to both NCMS and CMC //C4/CY//.

405. EKMS FEEDBACK REPORT. NCMS views feedback regarding significant discrepancies or misinterpretation of COMSEC policy or procedure as an important management tool. ISIC's/IUC's are encouraged to forward such information to improve not only the EKMS inspection program but 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 communities. Annex H provides an example of an EKMS feedback report message.

410. PRIVILEGED NATURE OF INSPECTION REPORTS. Inspectors serve as the ISIC/IUC's representative for evaluating EKMS account management of subordinate commands. The release of EKMS Inspection reports prepared under the provision of this manual require appropriate restrictions on public access and access by governmental organizations external to the DON. The release of reports outside the original distribution as designated by the ISIC/IUC would inhibit the exchange of full and open views between the Inspector and those being inspected and would seriously impair the effectiveness of this process as a management tool. In addition to being marked FOR OFFICIAL USE ONLY, the following caveat shall be included on all EKMS Inspection reports:

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. In accordance with EKMS-3(series) ~~this~~ and other related regulations, requests for, or correspondence related to this report coming from outside sources 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 //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 thereon to the Commander, U.S. Coast Guard C4ITSC. Holders of this report shall strictly observe this caveat."

ANNEX A
EKMS INSPECTION GUIDE
EKMS MANAGER

PURPOSE. The purpose of this inspection guide is to ensure all aspects of COMSEC management are covered by the EKMS Inspector during the account inspection.

INITIAL REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

EKMS Account number: _____

Total Line items in EKMS Account: _____

Immediate Superior in Command: _____

Date of Last EKMS Inspection: _____

Date of Last CMS A&A Periodic Training Visit:_____

Name/Grade/Rate and Command of EKMS Inspector_____

Date of Last Facilities Approval: _____

EKMS Manager Name/Grade: _____

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

Identify Following, as Applicable/Assigned:

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

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

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

Remarks: _____

SECTION IDENTIFICATION

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the EKMS Inspector conducting the inspection. Per Chapter 2 and Article 401.c, inspection reports shall include references and comments to substantiate the evaluation. As such, below each item reviewed space is provided to annotate comments to any question that receives a negative response. The inclusion of the inspection checklists should aid Inspectors and the inspected 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	1. 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 5510.30A, Article 11-1 paragraph 2,3; SECNAV-M 5510.36, Article 7-11; EKMS-1 (Series), Article 550.e]
Yes / No	A	2. Is a visitor's register maintained and retained for one year? (consecutive years in one book authorized) [EKMS-1 (Series), Article 550.e, Annex T]
Yes / No	I	3. Is **unescorted** access limited to individuals whose duties require such access and who meet access requirements? [EKMS-1 (Series), Article 505] **NOTE:** See #5 (Part B) for when such could result in/constitute a COMSEC Incident
Yes / No	A	4. Are the names of individuals with regular duty assignments in the COMSEC facility on a formal access list and signed by the current CO/OIC/SCMSRO? [EKMS-1 (Series), Article 505.d,550.e]

Yes / No	I	5. PART 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]
Yes / No		PART 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(2)] **NOTE:** If personnel have access to keying material and are not reflected on the list or individual designation letter, access as an incident (review watch-to-watch inventory, SF-153's, CMS-25's, SF-702 to determine (unauthorized access). If the access list is outdated, assess as admin discrepancy.
Yes / No	A	6. Is security clearance data for personnel whose duties require access to COMSEC material maintained by the Command Security Manager? [SECNAV-M 5510.30A, Article 9-5 paragraphs 2,3,4,5] **NOTE:** For Marine Corps, documented in the Management Manpower System (MMS). For Coast Guard, documented in the Personnel Management Information System (PMIS).
Yes / No	I	7. If the account holds material for SCI/SI circuits, are Account Managers SCI eligible and indoctrinated or has temporary access been granted by DON CAF? {EKMS-1 (Series), Article 412.d;SECNAV M5510.30 Art 9-4.4

Yes / No	A	8. 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(1)] **NOTE:** Marine Accounts are required to have a Physical Security Survey (PSS) conducted on a **biennial** basis by a school trained Military Provost Officer. [Marine Corps Order 5530.14(Series)
Yes / No	A	9. 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	10. Is the space/compartment or vault which contains COMSEC material outwardly identified as "RESTRICTED AREA"? [OPNAVINST 5530.14(Series), Articles 210.g.4 and 218.a.4. [**MCO 5530.14(Series) USMC accounts only**]
Yes / No	A	11. Are applicable security controls (e.g., guards and alarms) in place in accordance with SECNAV-M 5510.36, Chapter 10? [EKMS-1 (Series), Article 520.a(3)] [**MCO 5530.14(Series) USMC accounts only**]
Yes / No	I	12. 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] **NOTE:** Effective 01 July 93 commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized to store any
		classified material. [EKMS-1 (Series) Article 520.f]

Yes / No	A	13. Is a Maintenance Record for Security Containers and Vault Doors (Optional Form 89) maintained for each security container and retained within the container? EKMS-1 (Series), Article 520.b(3)]
Yes / No	A	14. Are all damages, repairs or alterations to the container or parts of the container (e.g., Group 1R locks, locking drawer, drawer head, etc.) properly documented on an Optional Form 89? [SECNAV-M 5510.36, Article 10-15, paragraph 3; EKMS-1 (Series), Article 520.f, NOTE]
Yes / No	I	15. Do storage containers conform to the two person integrity (TPI) requirements for the protection of Top Secret COMSEC keying material? [EKMS-1 (Series), Article 520.e]
Yes / No	A	16. 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(1)]
Yes / No	A	17. 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(2)]
Yes / No	A	18. Are completed SF-702's retained for 30 days beyond the last date recorded {EKMS-1 (Series} Article 520.b(2) NOTE, SECNAV-M5510.36 Article 7.11
Yes / No	I	19. Except in an emergency, are combinations to the COMSEC Account vault/COMSEC Facility/security containers restricted to the EKMS
		Manager and alternates only? [EKMS-1 (Series), Article 515.c(1)]

Yes / No	A	20. 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(3)(a)]
Yes / No	A	21. In a **non-continuously** manned COMSEC facility, are security checks conducted prior to departure of the last person and documented on a Activity Security Checklist (SF-701)? [EKMS-1 (Series), Article 550.d(3)(b); SECNAV-M 5510.36, Article 7-11]
Yes / No	A	22. Are completed SF-701's retained for 30 days beyond the last date recorded [EKMS-1 (Series} Article 550.d(3)(c), SECNAV-M5510.36 Article 7.11]
Yes / No	A	23. 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(3)(c)]
Yes / No	I	24. Does any one person have knowledge of both combinations to any one TPI container??? EKMS-1 (Series), Article 515.c.2;945.e] **NOTE:** A yes would constitute a loss of TPI (COMSEC Incident), no indicates compliance.
Yes / No	I	25. Are all 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]

Yes / No	A	26. 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	27. Are SF-700's protected as follows: [EKMS-1 (Series), Article 515.f] a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope? **NOTE:** The sealing of the A & B combination to a TPI container could result in a single person having access to the container (A Physical Incident)
Yes / No	A	b. Are SF-700's sealed using transparent lamination or plastic tape?
Yes / No	A	c. Names, addresses and phone numbers of individuals authorized access to the combination clearly recorded on the front of the envelope? **NOTE:** The use of see recall roster is not authorized.
Yes / No	A	d. Proper classification and downgrading markings on Part 2 and 2A
Yes / No	A	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	A	28. Is COMSEC material stored separately from other classified material (e.g., separate container or drawer to facilitate emergency removal or destruction), and segregated by status, type and classification? [EKMS-1 (Series), Article 520.a(4)]
		Examples: 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.

Yes / No	A	29. Are software-designed devices in storage at the account level covered as part of the units 3M or other service-specific maintenance program? {EKMS-5(Series), Article 313 **NOTE:** A list of the devices can be found at: https://infosec.navy.mil/crypto/ **under "Hot Topics" Cryptographic Equipment Battery Information (MIP/MRC tab) and (battery information tab)**
Yes / No	I	30. When not being used and under the direct control of authorized personnel, is **all** COMSEC material properly stored? [EKMS-1 (Series), Article 520.a(2)]
Yes / No	A	31. 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	32. Are classified COMSEC files, records and logs properly marked with highest classification level based on the contents and annotated applicable downgrading instructions reflected below ? [EKMS-1 (Series), Article 715.d; SECNAV-M 5510.36, Article 6-3, 6-26] Derived from: EKMS-1 (Series) Declassify on: 22 September 2028

SECTION 2 – EKMS MANAGER RESPONSIBILITIES

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed

Yes / No	A	33. Has the EKMS Manager completed the EKMS Manager's Course of Instruction (COI) V-4C-0013 prior to appointment or within the prescribed timeframe? [EKMS-1 (Series), Article 412.f] **NOTE:** If not, have they completed the JQR or is there an NCMS approved waiver in place?
Yes / No	A	34. Has the EKMS Manager promulgated written guidance, concerning the proper handling, accountability, and disposition of COMSEC material and STE's when associated with a KSV-21 card to all LE personnel? [EKMS-1 (Series), Article 455.e, 721 (NOTE)]
Yes / No	A	35. Does the EKMS Manager provide the CO/OIC/SCMSRO and other interested personnel with general information about new or revised CMS/EKMS policies or procedures? What is the method of informing interested personnel? [EKMS-1 (Series), Article 455.a]
Yes / No	P	36. Are self-assessments and spot checks conducted by the EKMS Manager and/or Alternates at a minimum of quarterly or monthly, as applicable and **are the results of both on file**, as required? [EKMS-1 (Series) Articles 315.b note, 450.i.3, 455.y, 455.z, Annex T Para 2.x].
Yes / No	A	37. Has the EKMS Manager ensured that training is conducted monthly and is properly documented and retained in accordance with command directives and EKMS-1(Series)? [EKMS-1 (Series), Article 455.f, Annex T;]
Yes / No	A	38. Are "COMSEC Responsibility Acknowledgement Forms" completed and handled as follows: [EKMS-1 (Series), Article 769.b(2); Annex K]

Yes / No	A	a. Properly completed for each individual that handles COMSEC material and filed in the Chronological File? b. Are executed COMSEC Responsibility Acknowledgement Forms retained for 90 days after the individual no longer requires access to COMSEC material, transfers or retires? [EKMS-1 (Series) Annex T]
Yes / No	A	39. Prior to releasing COMSEC material to a contractor, has the EKMS Manager ensured the provisions of OPNAVINST 2221.5(Series) have been met? [EKMS-1 (Series), Article 505.g]
Yes / No	A	40. If the account has LEs which are responsible to a CO other than the account EKMS Manager's CO, has the EKMS Manager ensured that Letters of Agreement were exchanged and are signed by the current CO? [EKMS-1 (Series), Article 445, Annex L]
Yes / No	A	41. Does the Letter of Agreement address the minimum issues in accordance with EKMS-1 (Series)? [EKMS-1 (Series), Annex L]
Yes / No	A	42. Is the original or a signed copy of the Letter of Agreement held by the EKMS Manager in the Directives File? [EKMS-1 (Series), Article 709.c]
Yes / No	A	43. Has coordination been made with the area Defense Courier Service (DCS) station to establish a DCS account by submission of a USTC IMT Form 10 and signed by the **current** CO/OIC/SCMSRO? [EKMS-1 (Series), Articles 405.h, 751.b and Annex D paragraph 6]
Yes / No	I	44. Does the EKMS Manager ensure that all cryptographic maintenance personnel that perform maintenance within his/her account, have DD-1435(s) documented and on file and are authorized to perform cryptographic maintenance in writing? [EKMS 5 (Series), Article 111]

Yes / No	A/I	45. Has a formal designation Letter or Memorandum of Appointment (LOA/MOA) been completed for the EKMS Manager, Alternate(s) and EKMS Clerk(s)? [EKMS-1 (Series), Articles 412, 414 and Annex J] **NOTE:** (1) The absence of an appointment letter (required) when the person has the combinations to the vault and access to the LMD/KP would constitute "unauthorized access" for Managers, Alternates and LE Issuing and Alternates. (2) If the Manager/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 Admin Hit. (3) Clerks are prohibited from having combinations. Address a missing Clerk Appointment letter as an administrative discrepancy unless they also had access to keying material and no other written authorization existed signed by the CO.
Yes / No	A	46. If the account or LE is utilizing the CMWS/DMD PS for Black Key Management, has the EKMS Manager, Alternate or Tier 3 personnel, as applicable completed CT3/DMD Sustainment Training? [EKMS 1 (Series), Annex AH 4.b]

SECTION 3 - EKMS CLERK

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed

Yes / No	I	47. Is the EKMS Clerk restricted from having knowledge of/or access to combinations of security containers storing COMSEC keying material and only allowed to maintain TPI requirements after the COMSEC container has been opened by Manager personnel? [EKMS-1 (Series), Article 470.c(1)] **NOTE: Pull/review corresponding SF-700's to see if the Clerk is reflected on any. If so, this constitutes a physical incident.**
Yes / No	I	48. Is the Clerk prohibited from having access to the LMD/KP as either an administrator or operator? [EKMS-1 (Series) Article 470.c.3, Annex X Paragraph 8]. **NOTE:** Have the Manager or Alternate logon to LCMS and verify the clerk is not either a sysadm or sysopr under Registration – Operators
Yes / No	A	49. Are all receipts, inventories, and destruction reports that are signed by the clerk, signed as a witness only? [EKMS-1 (Series), Article 470.b(4)]

SECTION 4 - LCMS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	50. Is the LMD monitor, KP, and STE arranged to allow the operator to view all displays without obstruction? [EKMS-1 (Series), Annex X, Paragraph 12.b]

Yes / No	P	51. Is LCMS being used to maintain records for all COMSEC material held by the account and is only COMSEC-accountable material reflected on the AIS? [EKMS-1 (Series), Articles 706, 718.b and 1005.a]
Yes / No	P	52. Does the account maintain a KP CIK ID and PIN log and is the log being retained for the prescribed time frame? [EKMS-1 (Series), Annex T, Paragraph 2.v and X Paragraph 12]
Yes / No	P	53. Are KP PINs changed every 6 months? [EKMS-1 (Series), Article 520.j(7)] **NOTE:** This can be verified through the LCMS activity data or the corresponding SF-700 (date changed).
Yes / No	P	54. **LMD Security Settings:** a. Is the LMD configured to lock out an account after 3 failed logon attempts? **and/or** b. Has the password expiration (180 **or 90** days) been altered? [EKMS-1 (Series), Article 515, 1005.b.3]
Yes / No	A	55. Does each EKMS Manager/Alternate have separate unique LCMS/KP Operator ID's/CIKs? [EKMS-1 (Series), Annex X, Paragraph 12.a]
Yes / No	P	56. Has the default root password been changed as required? {EKMS-1 (Series) Articles 515, Annex X Paragraph 12.Q
		NOTE: To determine this try to logon with the default generic root password. Also, 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. You will see if and when it was ever changed in the "Last Successful Change" entry.
Yes / No	A	57. Does the account have two LMD/KP System Administrators registered? [EKMS-1 (Series), Annex X, Paragraph 9]

Yes / No	A	58. Are PIN's/Passwords for all LMD/KP Administrators and Operators recorded and sealed in separate SF-700 envelopes for each respective person and protected as required? [EKMS-1 (Series), Articles 515.f (Note 2) and 520.j.(9)]
Yes / No	A	59. Has the Manager ensured the CAD data is current and is updated, as required? [EKMS-1 (Series) Articles 455.ad and 602]
Yes / No	I	60. Has the account performed a changeover every 3 months to update the Key Encryption Key Local (KEKL) used by the KP? [EKMS-1 (Series), Article 238.b.2, 945.c.8, Annex X, Paragraph 12.T] **NOTE:** Failure to perform changeover within the prescribed interval is a cryptographic incident. To determine, **do not look solely at CIK labeling**. Have the Manager or Alternate logon to LCMS and generate a User Defined Audit Report as follows: Utility – Activity Report – Generate Report "User Defined Audit Report", Dest EKMS ID = local account, "Generate Report". Next, enter the operator ID (or leave blank for all), Enter a start date (make it within the last 100 days), status (default = all), EKMS ID = Local Account, Ending Date: enter the current date, Alpha = KP Change Over – Generate Report. If performed within the 100 day period used, the changeover will be reflected in the report on the screen.

Yes / No	P	61. Has the account performed a KP rekey on an annual basis? [EKMS-1 (Series), Article 1005.a.11, Annex X, Paragraph 12.u] Follow the procedures in #60 above and change the alpha to KP Rekey, and the start date to 366 days earlier, i.e. if the inspection is conducted on 2 Feb 10, use 20090201 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 that the Firefly vector set has not expired**
Yes / No	I	62. Has the KP been re-certified in the last 3 years? [EKMS-1 (Series), Article 1185.e] **NOTE:** Prior to accessing as an incident, inquire to determine; (a) has the replacement one been received? (b) Was the corresponding Transit CIK received, (c) has the unit submitted a waiver for continued use of the existing KP possibly due to a hardware failure (LMD) or (d) does the account require a new FF Vector Set and/or MSK (if so did they order it?
Yes / No	P	63. Has the KP been returned to CMIO for re-certification within 30 days of the one currently held/in-use? [EKMS-1 (Series), Article 1005.B.4] **NOTE:** Failure to return a KP within the required timeframe is a reportable
		PDS unless the account is deployed and unable to enter it into DCS and the account has received a waiver (if so, ask to see the waiver).

Yes / No	I	64. Has the EKMS Manager ensured that the KP has not been used past the re-certification date? [EKMS-1 (Series), Article 945.c.1.d] **NOTE:** See #62 above for possible exceptions.
Yes / No	P	65. Has the account archived LCMS data on a semi-annual basis after each fixed cycle inventory and is archived media labeled, safeguarded and retained as required? [EKMS-1 (Series), Article 1005.a.12, Annex X, Paragraph 12.s]
Yes / No	A	66. Are the KP REINIT 1 and NAVREINIT 2 keys classified at the level of the accounts HCI and safeguarded appropriately? [EKMS-1 (Series), Article 1185.d(1)] **NOTE:** REINIT1 and NAVREINIT2 CIKS are not designated as "CRYPTO" and do not require TPI handling/storage.
Yes / No	A	67. Does the account maintain four copies of REINIT 1 and at least two copies of NAVREINIT 2? Are all reflected on the AIS, as required? [EKMS-1 (Series), Article 1185.d(3)] **NOTE:** If an account has additional copies but they are accounted for on the AIS do not cite as deficient.
Yes / No	A	68. Are REINIT 1 and NAVREINIT 2 CIKS properly registered in LCMS? [EKMS-1 (Series), Article 1185.d(3)(d)] To verify, in LCMS go to: Registration – COMSEC Material. a. Are REINIT 1 keys reflected on the AIS as "**AIDS**" and accounted for as **ALC-1?** b. Are NAVREINIT 2 keys reflected on the AIS as "**Equipment**" and accounted for as **ALC-4?**

Yes / No	A	69. Does the EKMS account wrap all reportable transactions (i.e. Receipts, Transfers, Destructions, Relief of Accountability, Possessions and Generation reports) to Tier 1 and the originator as applicable? [EKMS-1 (Series, Art 767.b]
Yes / No	P	70. Are backups being performed on the following as required? [EKMS-1(Series), Articles 718.d, 1005.a.12] 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	A	71. Is backup media labeled "Secret", and reflect proper downgrading instructions the date the backup was performed? [EKMS-1 (Series), Article 718.c Note 2]
Yes / No	A	72. Has the account generated, wrapped and submitted a COAL inventory on a monthly basis? [EKMS (Series) 766.b.4] **NOTE:** To verify in LCMS: 1. From the desktop 2. Accounting 3. Transaction 4. Display (Adjust to originated between and use a two month window example 20100201 (beginning) 20100228 (ending). 5. Look for a transaction type of "inventory" 6. Verify it is "processed" 7. Select the inventory and view the transaction to determine if
		the type is "Change Account Location" **NOTE:** Submarines are exempt from this when at-sea but will generate one within 30 days of departure or return, as applicable.

SECTION 5 -- <u>CHRONOLOGICAL FILE</u>

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	73. Does the CHRONOLOGICAL FILE contain the following required files: [EKMS-1 (Series), Article 706.a, Annex T] a. COMSEC material accounting reports (i.e., receipts, transfers, destruction, possession, generation, relief from accountability, conversion. b. Up-to-date EKMS Accountable Item Summary (AIS) or up-to-date printed COAL inventory (see EKMS-1B Art 706.a.2 and 763.c note). c. Inventory reports (including working copies and ALC 4 & 7 inventories) and reconciliation notices. (Note: working copies must reflect the signatures of the personnel who conducted/witnessed the inventory of the material reflected) d. Transaction Status Log. (Properly closed out and previous 2 years retained) (see EKMS-1B Art 724.b for close out procedures) e. USTRANSCOM IMT Form-10 f. CMS Form 1 (if required) g. COMSEC Responsibility Acknowledgement Forms h. Key Conversion Notices i. EKMS CF Generated Special Notices

SECTION 6 – ACCOUNTABLE ITEM SUMMARY (AIS)/TRANSACTION STATUS

LOG

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Item/Area Checked
Yes / No	P	74. Does the AIS reflect all COMSEC material held by the account? {EKMS-1 (Series) Article 763, 1005.a.4} **NOTE:** Randomly record the information off at least 3 items and do the following: Logon to LCMS – Accounting – Accountable Item Summary – (Change the display to Account) vice all. Is the item reflected on the Accountable Item Summary (AIS) and is it reflected as "On-Hand"?

SECTION 7 - <u>COMSEC MATERIAL RECEIPTS/TRANSFERS</u>

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	P	75. Are SF-153 COMSEC material Receipt Reports properly completed to include: TN number(s), date assigned, type of action, EKMS Manager and witness signatures? [EKMS-1 (Series), Article 1005.a, Annex U, Paragraph 9] **NOTE:** Accounting reports found to be missing required signatures constitutes an incomplete accounting report (non-reportable PDS).

Yes / No	A	76. Have Receipt, Transfer, Destruction, Generation, Possession and Relief of Accountability transactions been sent to Tier 1 via x.400? [EKMS-1 (Series), Chapter 7].
Yes / No	A	77. Have Receipt, Transfer, Destruction, Generation, Possession and Relief of Accountability transactions been sent to Tier 1 via x.400? [EKMS-1 (Series), Chapter 7].
Yes / No	P	78. Are receipts for COMSEC material submitted within 96 hours of receipt and submitted via X.400 to Tier 1? [EKMS-1 (Series), Article 742.b, 1005.a.15].
Yes / No	A	79. Has the receipt of Two Person Control (TPC) material been reported per CJCSI 3260.01? [EKMS-1 (Series), Article 255.d]
Yes / No	A	80. Has all AL1, AL2 and AL4 material received from NCMS (078000) or CMIO Norfolk (078002) been reported to the COR and originator of the shipment using EKMS transaction Transfer Receipt Report All (TRRA) and transmitted electronically via the X.400 message server? [EKMS-1 (Series), Article 742.a(1)]
Yes / No	A	81. Has all AL1, AL2, AL4 and AL6 material
		received from DIRNSA or USNDA been reported to the COR using TRRA, Transfer Receipt Report Exception (TRRE), or Transfer Receipt Report Individual (TRRI) via the message server? [EKMS-1 (Series), Article 742.a(2)]
Yes / No	A	82. Are pending tracers processed as required? {EKMS-1 Article 743} **NOTE:** Failure to respond to a third tracer is a Physical Incident.
Yes / No	P	83. Does the account report the receipt of corrupt Bulk Encrypted Transactions (BET's) within 96 hours of download? [EKMS-1 (Series) Article 742.d, 1005.a.15]

SECTION 8 - DESTRUCTION PROCEDURES/REPORTS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	84. Is routine destruction of COMSEC material performed IAW the methods prescribed in EKMS-1? [EKMS-1 (Series), Article 540, 790 and 945.e(10, 11)] **NOTE:** The use of an unapproved destruction device is considered a COMSEC Incident.
Yes / No	I	85. Is Non-Paper COMSEC Material (Key Tape destroyed by burning or disintegrating in a NSA-Evaluated/authorized destruction device? [EKMS-1 (Series), Article 540 j,(2)(a)] **NOTE:** Destruction of COMSEC material by other than authorized means is a Physical Incident.
Yes / No	I	86. Are destruction records being completed to document the destruction of all ALC 1, 2 and 6 COMSEC material regardless of its
		classification? [EKMS-1 (Series), Article 736.b(1)] **NOTE:** The absence of destruction reports for material charged to the account must be reported as a Physical Incident.
Yes / No	P	87. Is the destruction of key issued to a DTD, SKL or other electronic storage device being completed in accordance with EKMS-1? [EKMS-1 (Series), Article 540.c(3)(a), Annex Z, Paragraph 15.b and Annex AF paragraph 8.f.4] **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 (reflected on a CMS-25 or SF-153) and found to exist, report as a COMSEC Incident.

Yes / No	P	88. Do destruction records clearly identify the short title, edition(s), accounting number, ALC, and date of destruction? [EKMS-1 (Series), Article 736.a(3); Figures 7-1, 7-2, 7-3] **NOTE:** An incomplete accounting report or one missing required data is a non-reportable PDS.
Yes / No	P	89. Are destruction records properly signed and dated by the two individuals who conducted the destruction and are blocks 14 & 16 annotated to indicate the action the SF-153 was used for (destroyed/witness? [EKMS-1 (Series), Article 790.f(1)(2); and Figures 7-1-3 paragraph 4, 7-2-2 paragraph 2, 7-3-1 paragraph 2, Annex U] **NOTE:** Missing signatures constitutes an incomplete accounting report (Non-reportable PDS). Failure to complete blocks 14 & 16 would be an Administrative Discrepancy.
Yes / No	P	90. Is un-issued keying material that becomes superseded during the month destroyed no later than five working days after the end of the month in which it was superseded? [EKMS-1 (Series), Article 540.e(6)(a), e.(7)(a)] **NOTE;** This and # 86 would both constitute "late
		destruction" a non-reportable PDS.
Yes / No	P	91. Is superseded material, received in a ROB shipment, destroyed within 12 hours of opening the shipment and the SF-153 destruction document annotated "superseded upon receipt"? [EKMS-1 (Series), Article 620.d (Note)] **NOTE:** See comments for #86 above.

Yes / No	P	92. Have the following items been recorded as "Destroyed" or "Filled in End Equipment" NLT the 5th working day of the month following use/loading? [EKMS-1 (Series) Articles 238, 540, 1185 and Annex X paragraph 10] - FF Vector Set: USFAU 0000000333 - Message Signature Key(MSK): USFAU 4294967297 - Transit CIK: USKAU B7121 - KG Rules: USKAD BU71260 880091 **(current version should be retained and be listed as on-hand in LCMS; earlier versions should not be held by the account and on the AIS)** **NOTE:** Failure to record these items as either "Destroyed" or "Filled in End Equipment will result in them still being on the AIS (Late Destruction/PDS). The Edition of the transit CIK will match the serial number of the KP. National and Navy policy prohibit retention of the FF Vector Set or MSK following their use as such is not required. The FF Vector Set and MSK become REINIT1 and NAVREINIT2 CIKS created on KSD-64A's at the account.
Yes / No	I	93. Does the account end-of-month consolidated destruction reports that are filed in the Chronological File consist of both the Reportable and Local Destruction Reports (vice working copies)? [EKMS-1 (Series), Article 706.a(1)] **NOTE:** If a destruction report is required and missing, the material must be considered lost and such reported as a Physical Incident.
Yes / No	P	94. Have consolidated destruction records been signed by the CO/OIC/SCMSRO? [EKMS-1 (Series),
		Annex U, 7.a] **NOTE:** Missing signature(s) constitutes an incomplete accounting report (non-reportable PDS)
Yes / No	P	95. Are SAS/TPC destruction reports signed by two members of the SAS/TPC Team? [EKMS-1 (Series), Annex U, 7.b(1)]

Yes / No	A	96. For submarines and ships 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.(c).2]]

SECTION 9 – INVENTORY REPORTS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	97. Is all COMSEC material (including equipment and publications) assigned AL Code 1, 2, 4, 6, and 7 inventoried semiannually or as required and are inventories retained for the two years? [EKMS-1 (Series) Article 766.a; Annex T)] **NOTE:** Failure to complete inventories, including locally generated ones for ALC 4 and 7 material is a Physical Incident. Submarines deployed or on patrol will use a locally generated inventory as discussed in 766 (note).
Yes / No	P	98. Are inventory completions reported via message or online? [EKMS-1 (Series), Articles 766 (NOTE)Para 2, 766.2.A, 766.F.4(NOTE), 1005.A.16]. **Not applicable to inventories used solely for Change of Command**
Yes / No	I	99. Are SF-153 inventory reports being locally generated for AL Code 4 and 7 material? [EKMS-1 (Series), Article 766.d.(2)]

Yes / No	I	100. Are the results of the two semi-annual inventories (SAIR) of AL Code 4/7 material being retained locally at the command for two years? [EKMS-1 (Series), Article 766.a.2, ANNEX T] **NOTE:** If inventories are not on file, as required it cannot be ascertained that the account properly completed the inventory and must be documented as a Physical Incident.
Yes / No	A	101. Are "Request for Inventory Transaction" generated by the COR, being responded to within 30 days of the initial request of the inventory? (EKMS-1 (Series), Article 766.b.1.(c)] **NOTE:** Submarines deployed or on patrol will use a locally generated inventory.
Yes / No	I	102. Have discrepancies on the Inventory Reconciliation Status Report (IRST) resolved within 90 days or has an extension been granted by NCMS, in writing? [EKMS-1 (Series), Articles 766.b.(1)(e), 766.b(1)(f), 945.e.16] **Do not assess as an incident if an extension has been granted, in writing by NCMS.**
Yes / No	I	103. Has the Command submitted a Change of Custodian Inventory Report (CCIR) **or Consolidated Inventory, as applicable** for a Change of Command, Change of SCMSRO, or Change of EKMS Manager as required? [EKMS-1 (Series), Article 766.b(2), **766.b(3), and 766.b(5)**] **NOTE:** Failure to conduct, complete and retain required inventories is a Physical Incident.
Yes / No	P	104. Was the SAIR signed by the EKMS Manager, a properly cleared witness, and the Commanding Officer or SCMSRO? [EKMS-1 (Series), Annex U, Paragraph 7.A.1] **NOTE:** Three signatures are required. The absence of one of the three constitutes an incomplete accounting report (non-reportable PDS).
Yes / No	A	105. Was the CCIR or **Consolidated Inventory, as**

		applicable conducted for a change of command signed by the outgoing Commanding Officer? [EKMS-1 (Series), Article 766.a.(3)(a), 766.b(3) or 766.b(5)]
Yes / No	I	106. Are completed inventories retained for the current plus 2 years? [EKMS-1 (Series) Annex T.

SECTION 10 - CORRESPONDENCE, MESSAGE AND DIRECTIVES FILE

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	107. Does the Correspondence and Message File contain the following required files: [EKMS-1 (Series), Article 709]
		a. EKMS account establishment correspondence? **NOTE:** Mandatory for accounts established after 01 Jul 93; optional for previously established accounts.
		b. EKMS Manager, Alternate EKMS Manager, and Clerk appointment correspondence?
		c. COMSEC Incident and Practice Dangerous to Security reports (this includes documentation on non-reportable PDS's)?
		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.
		d. Correspondence relating to command allowance and authorization to store classified COMSEC material?
		e. CMS AA visit and inspection reports
		f. List of personnel authorized access to keying material and the LMD/KP?

Yes / No	A	108. 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	109. Does the Message File contain all effective general messages (i.e., ALCOMs, ALCOMPAC P, ALCOMLANT A) that pertain to account holdings or COMSEC policy and procedures? [EKMS-1 (Series), Article 709.b] **NOTE:** Pull the recap (ALCOM, ALCOMPAC P, ALCOMLANT A 01/"current year" to compare those on file with the Manager for completeness.
Yes / No	A	110. Is the command maintaining status messages promulgated by the various Controlling Authorities for material held by the account i.e. JCMO 2116XXXXZ, COGARD C4ITSC, etc…? [EKMS-1 (Series), Art 255.f, Article 760.a]

SECTION 11 - COMSEC LIBRARY

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	111. Does the account maintain a COMSEC library with all applicable instructions and manuals? [EKMS-1 (Series), Article 721] a. LMD/KP Operators Manual EKMS 704(series) b. EKMS Intelligent Computer Aided Trainer ICAT (embedded in the LCMS program) c. EKMS Managers JQR d. Local Element Issuing CBT e. COMLANTFLT/COMPACFLT/COMUSNAVEURINST C2282.1 (series) Basic Shipboard Allowance of COMSEC material

		f. EKMS-1 (series) Policy and Procedures g. EKMS-3 (series) EKMS Inspection Manual h. EKMS-5 (series) EKMS Cryptographic Equipment Manual i. COMDTINST 5510.23 (USCG only) j. NAG-53 (series) – Keying Standard for Non-Tactical KG-84/KIV-7 Point to Point Circuits (**Only required by shore-based accounts**) k. NAG 16 (series) Field Generation and Over-the-air distribution of tactical Electronic Key l. NSA Mandatory Modification Verification Guide (MMVG) m. OPNAVINST 2221.5 (series) Release of COMSEC material to U.S. Industrial Firms Under contract to USN.(Required when issuing to contractors) n. SECNAV M5510.30 (series) DON Personnel Security Program o. SECNAV M5510.36 (series) DON Information Security Program p. OPNAVINST 5530.14 (series) Physical Security and Loss Prevention q. SECNAVINST 5040.3 (series) Naval Command Inspection Program (if applicable) r. NAVICPINST 2300.4 (series) Utilization and disposal of Excess COMSEC Material s. NAVICPINST 5511.24 (series) Classified Electronic COMSEC Material in the Navy Supply System t. OPNAVINST 2221.3 (series) Qualifications of Maintenance Personnel u. CJCSI 3260.2 (series) Joint Policy Governing Positive Control Material Devices (**Only if SAS**

		material held) v. SDIP 293 NATO Cryptographic Instruction (**Required only if account holds NATO material**) w. AMSG-600 NATO Communications Security Information. (**Required only if the account holds NATO material**).

SECTION 12 - LOCAL CUSTODY FILE

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	112. Does the local custody file contain signed, effective, local custody documents for each item of COMSEC material charged to the account which has been issued to authorized LEs? [EKMS-1 (Series), Article 712] **NOTE: The absence or non-use of LCI documents is a Physical Incident.** **NOTE:** 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.

SECTION 13 - REPORT RETENTION/DISPOSITION

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	113. 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]
Yes / No	A	114. Are local custody documents being retained for the **minimum** 90 days after the material is destroyed or returned to the EKMS Manager? [EKMS-1 (Series), Annex T, Para 2.a]
Yes / No	A	115. Have the following been retained for the **minimum** retention period of one year: [EKMS-1 (Series), Annex T] a. Receipts for official messenger mail, DCS courier mail and registered mail
Yes / No		b. Terminated Letters of Agreement
Yes / No	A	116. Have the following been retained for the **minimum** retention period of two years: [EKMS-1 (Series), Annex T] a. Receipts b. Transfer reports c. Consolidated destruction reports? d. Generation Reports e. Possession Reports f. Relief of Accountability Reports g. LE CBT completion certificates h. Audit Trail Review Logs i. Key Conversion Notices (KCN) j. Training documentation
		NOTE: Failure to maintain and retain Audit Review Logs for 2 years is a Physical Incident. The absence of other documents; Destruction, Relief from Accountability or Transfer reports for material charged to the account will result in a Physical Incident (loss of material).

Yes / No	A	a. General correspondence and messages pertaining to COMSEC matters relating to account holdings?
Yes / No	I	b. Fixed Cycle/Combined inventories? **NOTE:** The absence of the inventories prevents verification the inventories were conducted.

SECTION 14 - RESEALING/STATUS MARKINGS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	117. Has all unsealed COMSEC material been sealed/resealed in accordance with EKMS-1 (Series) and local command instruction(s)? [EKMS-1 (Series), Article 772 a & b, 769.g.1 note, 1005.a.7, 945.e.13]
Yes / No	A	**NOTE:** If keying material is prematurely extracted, other than as indicated in article 769.g.1 note, it must be documented on the CMS-25 as a non-reportable PDS. If segmented material is found prematurely extracted and such is not documented on a CMS-25, report as a Physical Incident. 118. For accounts with less than 500 line items, are the effective and supersession dates annotated on all COMSEC keying material, COMSEC accountable manuals and publications? [EKMS-1 (Series), Article 760.a]
Yes / No	A/I	119. Are keytape canisters free of locally applied labels and stickers which may conceal attempted penetration or prevent inspection of protective packaging? [EKMS-1 (Series), Article 760.e(1)(a)(NOTE)] **NOTE:** If discovered, remove label, inspect the canister and train user. If the canister is damaged, report as a Physical Incident.

Yes / No	A	120. For accounts with 500 or more line items, are the effective and supersession dates annotated within LCMS's Effective Date Tool **and** on material prior to issue to Local Element personnel? [EKMS-1 (Series), Article 760.a] **NOTE:** To verify in LCMS, from the desktop – Distribution – Effective Date – Record a Hard Copy Effective Date

SECTION 15 – PAGE CHECKS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	121. Are required page/verification checks being accomplished by a manager and witness as follows: [EKMS-1 (Series), Articles 757, 775.e, and Annex V] a. Unsealed COMSEC keying material: upon initial receipt; during account inventories; during watch inventories; prior to transfer; and upon destruction?
		b. Unsealed maintenance and operating manuals: upon initial receipt; after entry of amendments which change pages (both person entering and person verifying entry); during inventories; prior to transfer; and upon destruction? **NOTE:** An oral yes is not sufficient for verification of page checks. 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 either Change of Command or Change of EKMS Manager.

Yes / No		c. Unsealed amendments: upon initial receipt; after entry of amendments which change pages (both person entering and person verifying entry); during inventories; during watch inventories; prior to transfer; and upon destruction?
Yes / No		d. Maintenance and repair kits: upon initial receipt; upon installation of modification; during inventories; prior to transfer of the Q(repair kits); and upon destruction? **NOTE:** An oral yes is not sufficient for verification of page checks. Randomly open 3 – 5 Q-kits and verify; (a) that an actual inventory is contained in the kit, (b) that the inventory document is signed/dated by the individuals who sight-inventoried the cards and (c) if any card has been removed, that the inventory reflects this and the appropriate documentation is in the kit in place of the removed card.
Yes / No		e. Equipment: upon receipt (i.e., uncrating); during EKMS account and watch inventories; prior to transfer; and upon destruction?
Yes / No		f. Resealed keying material: during account inventories; prior to transfer; and upon destruction?
Yes / No	A	122. Are page checks of Amendment residue recorded on the Record of Page checks (ROP) page? [EKMS-1 (Series), Article 757.d, 787.g(4)]
Yes / No	I	123. Are page check discrepancies being reported? [EKMS-1, Article 757.h; EKMS-1, Annex V] **NOTE:** Page check discrepancies must be reported as a Physical Incident.

SECTION 16 - CORRECTIONS AND AMENDMENTS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	124. Are corrections to a publication made with black or blue-black ink only? [EKMS-1 (Series), Article 787.g(1)(b)(1)]
Yes / No	A	125. Are pen and ink corrections identified by writing the amendment or correction number in the margin opposite the correction? [EKMS-1 (Series), Article 787.g(1)(b)(2)]
Yes / No	A	126. 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(2)(a)]
Yes / No	A	127. 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(5)(b)]
Yes / No	P	128. Is classified & unclassified amendment residue destroyed within five working days of amendment entry? [EKMS-1 (Series), Article 787.h(2) NOTE] **NOTE:** Failure to destroy amendment residue within the prescribed time frame constitutes "late destruction".

SECTION 17 – SECURE TERMINAL EQUIPMENT (STE)/IRIDIUM

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	129. Is the issuance of KSV-21 cards performed

		on a local custody basis using a SF-153 or local custody document? [EKMS-1 (Series), Article 712.a, Annex AD, paragraph 17] **NOTE:** Failure to use LCI documents or their equivalent is a Physical Incident.
Yes / No	I	130. Is access to Terminal Privilege Association (TPA) cards restricted to the EKMS Manager, Alternates or other properly designated personnel (LE Issuing) [EKMS-1 (Series), Annex AD, paragraph 4] **NOTE:** If discovered such would fall under a Physical Incident "Any other incident that may jeopardize the physical security of COMSEC material.
Yes / No	P	131. Are KSV-21 cards properly accounted for in LCMS? [EKMS-1 (Series), Article 763.a, Annex AD paragraph 16] **NOTE:** Material not reflected on the AIS when documentation exists that the material is charged to the account is a non-reportable PDS. The absence of documentation to indicate the material is being properly accounted for would be reported as a Physical Incident.
Yes / No	A	132. Are KSV-21 cards filled with operational key reflected on the accounts reportable destruction report following loading as "Filled in End Equipment"? [EKMS-1 (Series), Annex AD paragraphs 18 and 21.f] **NOTE:** If cards are unable to be zeroized prior to shipment, verify that the cards were shipped based on the classification of the key loaded on the card. If found to have been shipped via unapproved method, based on the classification, document as a Physical Incident.
Yes / No	A	133. Are SF-153 destruction reports submitted to the COR via X.400; (1) Upon destruction of STE keying material when the KSV-21 card is filled/loaded from the LMD/KP **or** (2) When an unused FD (filled by the CF) is loaded into a terminal for the express purpose (of zeroizing (destroying) it? [EKMS-1 (Series), Art 792 and Annex AD, paragraph 21]

Yes / No	P	134. Upon receipt of a Key Conversion Notice (KCN), were the following actions complete: - KCN processed in LCMS in accordance with the EKMS-704 (series) - Verify that the terminal serial number listed is the serial number of the terminal in which the key was loaded - Ensure that all keying material listed was, in fact, held and loaded/destroyed by the account as indicated on the report. Accounts must also prepare a "Filled in End Equipment" destruction report and send the report to the COR. [EKMS-1 (Series), Annex AD, paragraph 17.d] **NOTE: Not applicable to KSV-21 cards.** Only applicable to devices filled with SCIP Modern Key such as Iridium, Sectera, Omni, ViPR, etc…
Yes / No	P	135. If the account has an Iridium phone and sleeve (Short Title: FNBA 20) is the sleeve reflected on the AIS and accounted as an ALC 1 item? [EKMS-1 (Series) Tab 1 to Annex AD paragraph 3] **NOTE:** Material not reflected on the Accountable Item Summary (AIS) when documentation exists
Yes / No	P	that the material is charged to the account is a non-reportable PDS. Absence documentation to indicate the material is charged to the account, the matter would be reported as a Physical Incident (found material)
Yes / No	I	136. If an Iridium phone/sleeve (FNBA 20) is held and issued, were proper local custody procedures followed to ensure continuous accountability of the item? {EKMS-1 (Series) Article 712.a} **NOTE:** Failure to use LCI documents or their equivalent is a Physical Incident.
Yes / No	P	137. Is Iridium keying material which has been issued/loaded recorded as "Filled in End Equipment" in LCMS? {EKMS-1 (Series) Article 792, Tab 1 to Annex AD paragraph 12}

SECTION 18 - OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR TRANSFER (OTAT)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	138. Have the KVG(s) been certified by an authorized facility prior to initial use, following maintenance, whenever security control is lost (e.g., KVG found outside of proper storage and unattended) or at least every two years thereafter? [EKMS-1 (Series), Article 1145.b] **Note: If a KVG is not held, skip to #142**
Yes / No	I	139. Have NSA-furnished tamper detection labels been applied to certified/ re-certified KVG(s)? [EKMS-1 (Series), Article 1145.h and 1145.j] **NOTE:** Serial number discrepancies with applied
		Tamper Detection labels must be reported as a Physical Incident.
Yes / No	I	140. Does each certified KVG have a certification tag on the handle that displays the classification of the equipment, "CRYPTO" status, date of certification, command that performed certification, and name/rank of the certifying technician? [EKMS-1 (Series), Article 1145.i] **NOTE:** If the certification tag has been removed the device must be considered uncertified. If used and the certification date is not verified, or other prior official approval is obtained, access as a Cryptographic Incident.

Yes / No	P	141. Have fill devices containing electronic key been clearly labeled (tagged/marked) with the identity of the key it contains? [EKMS-1 (Series), Article 1175.b(2)and Article 1182] **NOTE:** This is only applicable to KYK-13/KYX-15's (legacy devices). If not labeled and they blink when checked there is no way to verify the contents are not superseded.
Yes / No	P	142. If the account generates, transmits, relays or receives electronic key, are local accounting records being maintained? [EKMS-1 (Series), Article 1175.b(2) and 1182.d] **NOTE:** N/A for recipients of key received via OTAR.
Yes / No	P	143. If the account generates electronic key for OTAR and/or OTAT, have accounting records been retained for a minimum of 60 days following the date of the last entry on the key generation log? [EKMS-1 (Series), Article 1182.d(1)]
Yes / No	A	144. Does the EKMS Manager conduct periodic reviews of OTAT/OTAR local accounting logs? [EKMS-1 (Series), Article 1115.c]

SECTION 19 - Data Transfer Device (DTD)/Simple Key Loader (SKL)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	145. Is a classification tag attached to the DTD via the lanyard ring to indicate handling requirements when the Crypto Ignition Key (CIK) is not inserted? [EKMS-1 (Series), Annex Z, Paragraph 8.f] **NOTE:** Only applicable to the AN/CYZ-10 (DTD).

Yes / No	A	146. Is a tag attached to the CIK (e.g., via chain) to identify the CIK's classification and serial number? [EKMS-1 (Series), Annex Z, Paragraph 9.d] **NOTE:** Only applicable to the AN/CYZ-10 (DTD).
Yes / No	I	147. For accounts with a Top Secret CIK, is the CIK removed from the DTD or SKL, as applicable and returned to TPI storage when authorized Users are not present? [EKMS-1 (Series), Annex Z, Paragraph 10.b, Annex AF, Paragraph 4] **NOTE:** If a DTD and or SKL are stored with the CIK, they must be safeguarded according to TPI rules if TS key is stored in the device.
Yes / No	I	148. Is unrestricted access to Supervisory CIKs or the SSO password for the DTD or SKL, as applicable limited to only those individuals who are authorized to perform all of the associated privileges? [EKMS-1 (Series), Annex Z, Paragraph 11.d, Annex AF paragraph 4.a] **NOTE:** Access to a supervisory CIK (DTD) or SSO password (SKL) allows the changing of the date and time as well as resetting the audit trail.
Yes / No	I	149. Have recipients of key issued to either a DTD or SKL signed a local custody document acknowledging receipt of the key? [EKMS-1 (Series), Article 769.h, Annex Z, Paragraph 13.d] **NOTE:** This is applicable whether issued from the LMD/KP or outside of LCMS and also includes fills provided DTD-to-DTD, DTD-to-SKL, or SKL-to-SKL). Non-use of LCI documents is a Physical Incident.
Yes / No	I/P	150. Does the EKMS Manager or Supervisory User locally account for all DTD CIKs by assigned serial number? [EKMS-1 (Series), Annex Z, Paragraph 7.b and 26] **NOTE:** Only applicable to the AN/CYZ-10 (DTD). Loss of a CIK is a Physical 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	151. For non-watch station environments, are the Supervisory and User CIKs for either the DTD or SKL, as applicable inventoried whenever the account conducts Fixed-Cycle or Change of EKMS Manager inventories? [EKMS-1 (Series), Annex Z, Paragraph 14.a(1), Annex AF paragraph 5.c}] **NOTE:** Loss or unauthorized copying of a CIK is a COMSEC Incident. Loss is considered such when the associated DTD has not been; stored properly, under the direct control of authorized personnel **or** failure to delete a lost/stolen CIK from its associated DTD.
Yes / No	P	152. For **watch station** environments, are the serial numbers of Supervisory CIKs, User CIKs, and DTDs visually verified whenever watch personnel change? Is the SKL and user CIK reflected and accounted for on the watch-to-watch inventory? [EKMS-1 (Series), Annex Z, Paragraph 14.b(1)(2), Annex AF paragraphs 4 and 5] **NOTE:** If the items are held but not reflected on the watch-to-watch inventory, it is a non-reportable PDS.
Yes / No	I	153. Is audit trail data reviewed by a Supervisory User or EKMS Manager at a minimum of monthly or when the Audit Trail icon illuminates, and are these reviews recorded in an Audit Review Log and the logs on file for 2 years? [EKMS-1 (Series), Annex Z, Paragraph 17.c.17.d, 17.f, Annex T] **NOTE:** Failure to perform and document Audit Trail reviews is a Physical Incident.
Yes / No	I	154. Are DTD's and/or SKL's which are initialized, storing key or issued reinitialized at a minimum of annually? [EKMS-1 (Series) Annex Z paragraphs 17.a, 26.a.6; Annex AF paragraphs 9.c, 15.a.12] **NOTE:** To determine, randomly select a DTD or SKL which is issued and have the audit data uploaded to the LMD for review. Both SKEK and LKEK/HDPK has a one-year crypto-period.

SECTION 20 - EMERGENCY PROTECTION OF COMSEC MATERIAL

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	155. Has the command prepared an Emergency Action Plan (EAP) for safeguarding COMSEC material in the event of an emergency? [EKMS-1, Annex M, Paragraph 2.a]
Yes / No	A	156. Are all authorized personnel at the command / facility made aware of the existence of the EAP? [EKMS-1 (Series), Annex M, Paragraph 6.d]
Yes / No	A	157 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 M, Paragraph 2.b]
Yes / No	A	158. Does the EKMS Manager maintain the COMSEC portion of the command EAP? [EKMS-1 (Series), Annex M, Paragraph 1]
Yes / No	A	159. 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 M, Paragraph 2.c]
Yes / No	A	160. When planning for natural disaster, does the EAP provide for: [EKMS-1 (Series), Annex M, Paragraph 4]
Yes / No		a. Fire reporting and initial fire fighting 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 emergency personnel 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 and Controlled Cryptographic Item (CCI) material and reporting any losses or unauthorized exposures to appropriate authorities?
Yes / No	A	161. Are EAP training exercises conducted yearly to ensure that everyone is familiar with their assigned duties? [EKMS-1 (Series), Annex M, Paragraph 6.d(3)]

SECTION 21 - EMERGENCY DESTRUCTION PLAN (EDP)

NOTE: Unless specified in Local, ISIC, or TYCOM directives, Section 21 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	162. Does the EKMS account have an EDP incorporated into their EAP? [EKMS-1 (Series), Annex M, Paragraph 2.c]
Yes / No	A	163. 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(5)(6); SECNAV-M 5510.36, exhibit 2B]
Yes / No	A	164. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [EKMS-1 (Series), Annex M, Paragraph 5.d, 6.c]

Yes / No	A	165. Are the sensitive pages of KAMs prepared for **ready** removal (i.e., upper left corner clipped) and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [EKMS-1 (series), Annex M, Paragraph 5.e(2)(a)]
Yes / No	A	166. Are the priorities of destruction indicated in the plan? [EKMS-1 (Series), Annex M, Paragraph 8]
Yes / No	A	167. Are EDP training exercises conducted on an annual basis to ensure that everyone is familiar with their duties? [EKMS-1 (Series), Annex M, Paragraph 6.d(3)]
Yes / No	A	168. Is the EDP divided into two parts: one for precautionary and one for complete destruction? [EKMS-1 (Series), Annex M, Paragraph 7]
Yes / No	A	169. Does the EDP provide for adequate identification and rapid reporting of the material destroyed, to include the method and extent of destruction and any classified COMSEC material items presumed compromised? [EKMS-1 (Series), Annex M, Paragraph 10.b]
Yes / No	A	170. 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 M, Paragraph 10.a]
Yes / No	A	171. Are document sinking bags available in sufficient quantity and in good condition to permit jettison of COMSEC material? (**NOTE:** Afloat units only) [EKMS-1 (Series), Annex M, Paragraph 9.d(2)(a)(b)]

SECTION 22 - COMMANDING OFFICER (CO, OIC, SCMSRO) RESPONSIBILITIES

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed

Yes / No	I	172. Has the Commanding Officer: a. appointed, in writing, qualified and responsible individuals as EKMS Manager and Alternate Manager(s), Local Elements (Issuing), and, if desired an EKMS Clerk. [EKMS-1 (Series) Article 450.b] **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, access as a Physical Incident (unauthorized access) b. established, in writing, a list of personnel authorized access to keying material. [EKMS-1 (Series) Article 450.c]
		NOTE: If the list has not been updated annually, access 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-25's, SF-153's, and SF-702's
Yes / No	A	c. ensured that training procedures are adequate to meet operational requirements. [EKMS-1 (Series) Article 450.d]
Yes / No	A	d. ensured that COMSEC incident reports are promptly submitted and action taken as required. [EKMS-1 (Series) Article 450.e]
Yes / No	A	e. extended crypto periods, if necessary, for up to two hours. [EKMS-1 (Series) Article 450.f] **NOTE:** If extended beyond 2 hours and such is not authorized by the Controlling Authority access 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]
Yes / No	P	g. ensured that unannounced spot checks are conducted where COMSEC material is used and stored. [EKMS-1 (Series) Article 450.i]
Yes / No	A	h. received debriefings from CMS A&A Training Teams and CMS/EKMS Inspectors. [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	I	j. ensured that an inventory of all COMSEC material held by an account was conducted in conjunction with a change of Commanding Officer, upon change of EKMS Manager, or semi-annually, as required. [EKMS-1 (Series) Article 450.n] **NOTE:** Failure to complete and submit required
		inventories is a Physical Incident.
Yes / No	A	k. ensured that the EKMS Manager position is a primary duty. When not possible, ensured that assignment of collateral duties to EKMS personnel did not interfere with COMSEC responsibilities. [EKMS-1 (Series) Article 450.o]
Yes / No	A	l. Has the CO, SCMSRO's or OIC, as applicable received the EKMS for CO's training facilitated by their local CMS A&A Team? [EKMS-1 (Series) Article 325.C.2, CMS for CO's Handbook figure 4, Para 3.B]

SECTION 23 - MATERIAL ACCOUNTABILITY TRACKING

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed

Yes / No	I	173. Randomly select 10 COMSEC short titles from the accounts Accountable Item Summary (AIS). Verify that these items are either in the EKMS VAULT or have been properly issued or transferred and that the corresponding SF-153 is on file. **(Login to LCMS – Accounting – Accountable Item Summary – (If desired you can 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" and have the EKMS Manager pull the corresponding SF-153 and verify for completeness.** **NOTE:** Failure to use LCI documents for material issued is a Physical Incident.
Yes / No	P	174. Randomly select 10 Short Titles held by the account that requires monthly destruction. Have the EKMS Manager produce the destruction report reflecting the Short Titles selected for the previous month. Verify that the working copies were signed by a minimum of two personnel and that the consolidated reports (for both the ALC 1, 2, 6 and ALC 4,7 material reflect three signatures and that the date of report and TN's match those in LCMS. **[EKMS-1 (series) Articles 1005.a.1, Annex T Para 2.n]**

COMMENTS:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

PURPOSE. The purpose of this inspection guide is to ensure all aspects of COMSEC management are covered by the EKMS inspector during the account inspection.

INITIAL REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

EKMS Account number: _____

Total Line items in EKMS account: _____

Immediate Superior in Command: _____

Date of Last EKMS Inspection: _____

Date of Last CMS A&A Periodic Training Visit: _____

Name/Grade/Rate and Command of EKMS Inspector:

_____

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: _____

Remarks: _____

_____

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

SECTION IDENTIFICATION

1 - Security

2 - Local Element (Issuing) Responsibilities

3 - Accountable Items Summary (AIS)

4 - Local Custody File

5 - Resealing/Status Markings

6 - Corrections and Amendments

7 - Destruction Procedures/Reports

8 - Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer (OTAT)

9 - Data Transfer Device (DTD)/Simple Key Loader (SKL)

10 - Emergency Action Plan (EAP)

11 - Emergency Destruction Plan (EDP)

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the EKMS Inspector conducting the inspection. Per Chapter 2 and Article 401.c, inspection reports shall include references and comments to substantiate the evaluation. As such, below each item reviewed space is provided to annotate comments to any question that receives a negative response. The inclusion of the inspection checklists should greatly aid both Inspectors and the inspected 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	1. 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 5510.30A, Article 11-1 paragraph 2,3; SECNAV-M 5510.36, Article 7-11; EKMS-1 (Series), Article 550.e]
Yes / No	A	2. Is a visitor's register maintained and retained for one year? (consecutive years in one book authorized) [EKMS-1 (Series), Article 550.e, Annex T]
Yes / No	I	3. Is **unescorted** access limited to individuals whose duties require such access and who meet access requirements? [EKMS-1 (Series), Article 505] **NOTE:** See #5 (Part B) for when such could result in/constitute a COMSEC Incident.

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	A	4. Are the names of individuals
		with regular duty assignments in
Yes / No	A	the COMSEC facility on a formal access list? [EKMS-1 (Series), Article 550.e(1)(b)]
Yes / No	I	5. PART 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]
Yes / No	A/I	PART 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(2)] **NOTE: If personnel have access to keying material and are not reflected on the list or individual designation letter, access as an incident (review watch-to-watch inventory, SF-153's, CMS-25's, SF-702 to determine (unauthorized access). If access list is outdated, access as admin discrepancy.**
Yes / No	I	6. Are users of COMSEC material properly cleared at least as high as the level of classified material handled? [EKMS-1 (Series), Article 505.a] **NOTE: Personnel uncleared or not cleared to the level of material they have access to must be reported as a Physical Incident.**
Yes / No	A	7. Is security clearance data of personnel whose duties require access to COMSEC material maintained by the Command Security Manager? [SECNAV-M 5510.30A, Article 9-5 paragraphs 2,3,4,5]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		NOTE: For Marine Corps, documented in the Management Manpower System MMS). For Coast Guard, documented
Yes / No	I	8. If the LE Issuing holds material for SCI/SI circuits, are the LE Issuing and Alternates SCI eligible and indoctrinated or has DON CAF granted temporary access? {EKMS-1 (Series), Article 414.d(3);SECNAV M5510.30 9-4.4]
Yes / No	A	9. 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	10. Are applicable security controls (e.g., guards and alarms) in place in accordance with SECNAV-M 5510.36, Chapter 10? [EKMS-1 (Series), Article 520.a(3)]
Yes / No	A	11. Is the COMSEC Facility outwardly identified only as a "RESTRICTED AREA"? [OPNAVINST 5530.14(series), Articles 210 and 218.a.4]
Yes / No	I	12. 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] **NOTE:** Effective 01 July 93 commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized to store any classified material. [EKMS-1 (Series), Article 520.f]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	A	13. Is a Maintenance Record for Security Containers and Vault Doors (Optional Form 89) maintained for each security container. EKMS-1 (Series), Article 520.b(3)]
Yes / No	A	14. Are all damages, repairs or alterations to the container or parts of the container (e.g., Group 1R locks, locking drawer, drawer head, etc.) properly documented on an Optional Form 89? [SECNAV-M 5510.36, Article 10-15, paragraph 3; EKMS-1 (Series), Article 520.f, NOTE]
Yes / No	I	15. Do storage containers conform to the two person integrity (TPI) requirements for the protection of Top Secret COMSEC keying material? [EKMS-1 (Series), Article 520.e] **NOTE:** Not applicable if only Secret and below material is held.
Yes / No	A	16. 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(1)]
Yes / No	A	17. 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(2)]
Yes / No	A	18. Are completed SF-702's retained for 30 days beyond the last date recorded {EKMS-1 (Series} Article 520.b.2 (**NOTE**), SECNAV-M5510.36 Article 7.11
Yes / No	I	19. Except in an emergency, are combinations to the LE Issuing

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		security containers restricted to the Primary LE Issuing and alternates only? [EKMS-1 (Series), Article 515.c(1)]
Yes / No	A	20. 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(3)(a)]
Yes / No	A	21. 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(3)(b); SECNAV-M 5510.36, Article 7-11]
Yes / No	A	22. Are completed SF-701's retained for 30 days beyond the last date recorded {EKMS-1 (Series} Article 550.d.3.c, SECNAV-M5510.36 Article 7.11
Yes / No	A	23. 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(3)(c)]
Yes / No	I	24. Are combinations & associated SF-700's for TPI containers completed, stored, and safeguarded to prevent a single person from having access to both combinations? EKMS-1 (Series), Article 510.c.2, 510.c.3]
Yes / No	I	25. Are sealed records of combinations to COMSEC storage containers maintained in an approved security container (other than the container where the COMSEC

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		material is stored), and available to duty personnel for emergency use? [EKMS-1 (Series), Article 515.e] **NOTE:** If not properly stored in a GSA approved container, access as a Physical Incident in accordance with EKMS-1 (Series), Article 945.e.18.
Yes / No	A/I	26. Combinations to COMSEC material security containers must be protected as follows: [EKMS-1 (Series), Article 515.f]
Yes / No		a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope? **NOTE: The sealing of the A & B combination to a TPI container could result in a single person having access to the container (A Physical Incident**)
Yes / No	A	b. Combination envelope sealed using transparent lamination or plastic tape?
Yes / No	A	c. Names of individuals authorized access to the combinations recorded on the front of the envelope?
Yes / No	A	d. Proper classification markings on envelope?
Yes / No	A	e. Are the envelopes inspected monthly to ensure they have not been tampered with?
Yes / No	A	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]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	A	27. Is COMSEC material stored separately from other classified material (e.g., separate container or drawer to facilitate emergency removal or destruction), and
		segregated by status, type and classification? [EKMS-1 (Series), Article 520.a(4) and Annex M, Paragraph 3]
Yes / No	I	28. When not being used and under the direct control of authorized personnel, is all COMSEC material properly stored? [EKMS-1 (Series), Article 520.a(2)]
Yes / No	A	29. Are classified COMSEC files, records and logs properly marked with the highest classification to the level of its contents and annotated with the following statement? [EKMS-1 (Series), Article 715.d(2)(c)] "Derived from: EKMS 1 (series) "Declassify on: 22 September 2028" **NOTE:** The use of X1 – X8 is prohibited for downgrading /declassifying classified information. Declassification /Downgrading instructions will be in accordance with the CNO Policy ltr Ser N09N2/8U223000 dated 7 Jan 2008 until incorporated into SECNAV M5510.36. For records marked on/after 22 Sep 03, the date shown above reflects 25 years from the last authorized use of X1 – X8.

SECTION 2 - LOCAL ELEMENT (ISSUING) RESPONSIBILITIES

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	A	30. Are the 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	A	31. 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	A	32. Does the (Issuing) LE hold written instructions issued by the parent or servicing EKMS account (or LE (Issuing)) governing the handling, accountability, and disposition of COMSEC material? [EKMS-1 (Series), Article 465.b]
Yes / No	A	33. Does the LE (Issuing) provide written guidance concerning handling, accountability, and disposition of COMSEC material to all LE (Using) personnel [EKMS-1 (Series), Article 465.c]
Yes / No	A	34. Have all USN military LE personnel completed the CMS User Personnel Qualification Standards (PQS) (NAVEDTRA 43462 series)? [EKMS-1 (Series), Articles; 312, 450.g] **NOTE:** Not applicable to MSC, USMC/USCG
Yes / No	A	35. Does the LE issuing conduct training with all personnel handling COMSEC material to ensure they are adhering to proper EKMS procedures and document training in accordance

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		with command directives? (EKMS-1 (Series), Article 465.c, Annex T paragraph 2.ae]
Yes / No	I	36. Has the (Issuing) LE ensured that all LE personnel are; a. Authorized access to keying material in writing
Yes / No	A	b. Completed a COMSEC Responsibility Acknowledgement for?
Yes / No	A	c. Are completed COMSEC Responsibility Acknowledgement forms retained on file for 90 days from the date the individual no longer requires access to COMSEC material (is reassigned, transfers, etc…)
Yes / No	P	d. Are Commanding Officers/OIC's of LE's conducting spot checks within their organization? [EKMS-1(Series) Article 450.i NOTE 1]
Yes / No	A	37. If the (Issuing) LE has LE's which are responsible to a CO other than the Primary (Issuing) LE's CO, has the Primary (Issuing) LE ensure that Letter's of Agreement were exchanged? [EKMS-1 (Series), Article 445, Annex L]
Yes / No	A	38. Does the Letter of Agreement address the minimum issues: [EKMS-1 (Series), Annex L] a. Compliance with locally prepared COMSEC instructions? b. COMSEC Incident and PDS documentation and reporting procedures? c. Responsibility for Certifying Clearance/Access?

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		d. The issuance of COMSEC material in Electronic Form?
		e. Notification of Local Element Appointments? f. Storage/Facility Clearance?
Yes / No	A	39. Is a copy of the completed, Letter of Agreement held by the Primary (Issuing) LE and retained as required? [EKMS-1 (Series), Article 709.c, Annex T]
Yes / No	I	40. For LE's (external) supported through a LOA, are inventories completed for either Change of Command (OIC) or Change of LE Issuing (as applicable?) [EKMS 1 (Series) Article 766.a.3.d and 766.a.4 (note)].
Yes / No	A	41. 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? [EKMS 5 (Series) Article 111]
Yes / No	A/I	42. Has a formal Letter of 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 J] **NOTE:** (1) The absence of an appointment letter (required) when the person has the combinations at the LE Issuing level would constitute "unauthorized access" for Managers, Alternates and LE Issuing and Alternates.

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		(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 Admin Hit.
Yes / No	A	43. 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	44. Has the LOA/MOA and LE CBT Certificate of Completion been forwarded to the parent account EKMS Manager and a copy retained on file for a minimum of two years following the relief of the Primary (Issuing) LE and/or Alternates? [EKMS-1 (Series), Article 418, Annexes J and T]
Yes / No	A	45. Does the (Issuing) LE maintain required files as directed by the parent account EKMS Manager? [EKMS-1 (Series), Article 703 NOTE 2]

SECTION 3 - ACCOUNTABLE ITEMS SUMMARY (AIS)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	46. Does the (Issuing) LE maintain an up to date Accountable Item (A/I) Summary which was provided by the parent account EKMS Manager? [EKMS-1 (Series), Article 763.c]

SECTION 4 - LOCAL CUSTODY FILE

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	I	47. Does the Local Custody File contain all effective signed local custody documents for material which is issued? [EKMS-1 (Series), Article 712, 945.e.6.c] **NOTE:** Failure to utilize and maintain local custody documents is a Physical Incident.
Yes / No	P	48. Do the local custody documents (i.e., SF 153, or locally prepared equivalent), contain the minimum required information? [EKMS-1 (Series), Article 769.c(1)]
Yes / No	A	49. Are local custody documents being maintained on file for 90 days after supersession? [EKMS-1 (Series), Annex T, paragraph 2.a]

SECTION 5 - RESEALING/STATUS MARKINGS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	50. Has all unsealed COMSEC material been sealed/resealed in accordance with EKMS-1 (Series) and local command instruction(s)? [EKMS-1 (Series), Article 772 a & b, 769.g.1 (Note), 1005.a.7, 945.e.13] **NOTE:** If keying material is prematurely extracted, other than as indicated in article 769.g.1 (Note), it must be documented on the CMS-25 as a non-reportable PDS. If

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		segmented material is found prematurely extracted and such is not documented on a CMS-25, report as a Physical Incident.
Yes / No	A	51. Are the effective and superseded dates annotated on all COMSEC keying material, COMSEC accountable manuals and publications in accordance with EKMS-1? [EKMS-1 (Series), Article 760.a, 775.g]
Yes / No	A/I	52. Are key tape canisters free of locally applied labels and stickers which may conceal attempted penetration or prevent inspection of protective packaging? [EKMS-1 (Series), Article 760.e, 760.f, 945.e.13.a] **NOTE:** If discovered, remove label, inspect the canister and train user. If the canister is damaged, report as a Physical Incident.
Yes / No	A	53. Are required page checks being accomplished as follows: [EKMS-1 (Series), Article 775.e, 778.d; Annex Z]
Yes / No		a. Unsealed COMSEC keying material. Upon initial receipt; during account and watch inventories; and prior to destruction?
Yes / No		b. Resealed keying material. During Fixed-Cycle and Change of EKMS Manager inventories; and upon destruction?
Yes / No		c. Unsealed maintenance and operating manuals. Upon initial receipt; after entry of an amendment which changes pages; during Fixed-Cycle and Change of EKMS Manager inventories; and

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No		upon destruction?
Yes / No		d. Equipment. Upon initial receipt (uncrating); during Fixed-Cycle and Change of EKMS Manager inventories; during watch inventories; and upon destruction?
Yes / No	I	54. Are page check discrepancies reported to the account EKMS Manager or an Alternate? [EKMS-1 (Series), Articles; 775.f, 778.d, 945.e.1, Annex V] **NOTE:** Missing pages or cards, as applicable to COMSEC accountable books and/or Q-kits is a Physical Incident.
Yes / No	P	55. Does the CONTINUOUSLY MANNED WATCH STATION maintain a watch-to-watch inventory that lists all COMSEC material held (including accountability for resealed segments and CIKS for DTD's and/or SKL's issued)? [EKMS-1 (Series), Article 775.d(1), Annex Z, paragraph 14.b; Annex AC paragraph 17.b (**NOTE**)] **NOTE:** Signatures are used to ensure compliance. Missing signatures on accounting reports constitutes a non-reportable PDS
Yes / No	P	56. Is the material recorded on the watch-to-watch inventory listed by short title, edition, accounting number (as applicable) and quantity? [EKMS-1 (Series), Article 775.d(2), 1005.a.1] **NOTE:** As the watch-to-watch inventory is an accounting report, if the required data is not reflected, such would

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		constitute an incomplete accounting report.
Yes / No	P	57. Has the inventory been properly signed and dated for each change of watch? [EKMS-1 (Series), Article 775.d(4), (5),(6), 1005.a.1]
Yes / No	A	58. Are watch-to-watch inventories being retained for 30 days beyond the last recorded date on the inventory? [EKMS-1 (Series), Annex T, paragraph j]
Yes / No	P	59. Have inventories for a NON-WATCH STATION ENVIRONMENT been conducted and recorded on the local custody issue document or a watch-to-watch inventory in accordance with EKMS-1 (Series)? [EKMS-1 (Series), Article 778.c, 1005.a.]
Yes / No	I	60. For NON-WATCH STATION ENVIRONMENTS, are DTD and SKL CIKs inventoried whenever the account conducts Fixed-Cycle or Combined inventories? [EKMS-1 (Series), Annex Z, paragraph 14.a(1) and Annex AF paragraph 5.c]

SECTION 6 - CORRECTIONS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	61. Are corrections to publications made with black or blue-black ink only? [EKMS-1 (Series), Article 787.g(1)(b)1]
Yes / No	A	62. Is each pen and ink correction identified by

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		writing the correction number in the margin opposite the correction? [EKMS-1 (Series), Article 787.g(1)(b)2]
Yes / No	A	63. Has the person entering the correction signed and dated the appropriate blanks on the publication's Record of Amendments page? [EKMS-1 (Series), Article 787.g(2)(a)]
Yes / No	A	64. 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(5)(b)]
Yes / No	A	65. Have both the person entering the correction and the person verifying the correction conducted a page check of the publication, and recorded this on the Record of Page checks page? [EKMS-1 (Series), Articles 787.g(4),(5)]

SECTION 7 - <u>DESTRUCTION PROCEDURES/REPORTS</u>

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	66. 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(2)(b),

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		(d) and Article 945.e] **NOTE:** The absence of a destruction report or LCI document indicating the material has been returned to the supporting EKMS Manager is a Physical Incident.
Yes / No	P	67. Do destruction records clearly identify the short title, editions, accounting number, ALC, and date of destruction? [EKMS-1 (Series), Article 736.a(3); Figures 7-1, 7-2, 7-3, Article 1005.a.1]
Yes / No	P	68. Are LE destruction records properly signed, or initialed, by the two individuals who conducted the destruction? [EKMS-1 (Series) , Article 790.f(1)(2); Figures 7-1, 7-2, and 7-3, Article 1005.a.1]
Yes / No	P	69. Do local destruction records for segmented COMSEC material contain the following: [EKMS-1 (Series), Chapter 7 fig 7-1, 7-2, 7-3, Article 1005.a.1]
Yes / No		a. Short title and complete accounting data?
Yes / No		b. Date of destruction?
Yes / No		c. Signatures of the two individuals conducting destruction?
Yes / No	A	d. Marked “CONFIDENTIAL (When filled in)”?
Yes / No	A	e. Classification/ Declassification markings? Derived from: EKMS-1 (Series) Declassify on: 22 September 2028
Yes / No	P	70. Is <u>only</u> one copy of a short title, edition, and accounting number recorded on the CMS 25 or locally prepared segmented

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		destruction document? [EKMS-1 (Series), Figure 7-1, paragraph 8, Article 1005.a.1] **NOTE:** Classified keying material is ALC 1 material requiring the accounting for each individual segment henceforth the policy that a CMS-25 can only be used for a single Short Title otherwise such would constitute and improperly completed accounting report.
Yes / No	P	71. Is routine destruction of COMSEC material performed in accordance with the methods prescribed in EKMS-1? [EKMS-1 (Series), Article 790, 792, Annex Z paragraph 15.b, Annex AF paragraph 8.f.4.]
Yes / No	P	72. Is destruction of key issued either physically or in electronic form (DTD, SKL, TKL) being completed within the prescribed timeframes (EKMS-1 (Series), Article 540]
Yes / No	A	73. Can Local Element personnel demonstrate the proper procedures for conducting routine destruction of COMSEC material? [EKMS-1 (Series), Article 540, 790, Annex Z paragraph 15.b, Annex AF paragraph 8.f.4.]
Yes / No	P/I	74. If keying material was unintentionally removed from its protective canister, is the following documentation recorded on its associated disposition record: [EKMS-1 (Series), Article 772.d, Article 1005.a.7, Article 945.e.13.b]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

	a. A statement that the keytape segment(s) were unintentionally removed? b. The date of the unintentional removal? c. Identity of the keytape segment(s) actually removed? d. Signatures of the individuals who removed the key? **NOTE:** Except as authorized in Article 769.g **NOTE** 1, premature extraction is a non-reportable PDS even when properly documented on the CMS-25 however; when not documented on the CMS-25, report such as a Physical Incident (Unexplained removal of key)

SECTION 8 - OVER-THE-AIR-REKEY/OVER-THE-AIR TRANSFER

NOTE: If a Key Variable Generator (KVG) (i.e., KG-83, KGX-93/93A) is not held, skip to question 77.

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	75. If held, does the certified KVG (KG-83/KGV-93) have a certification tag on the handle that displays the classification of the equipment, "CRYPTO" status, date of certification, command that performed certification, and name/rank of the certifying technician? [EKMS-1 (Series), Article 1145.i]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		NOTE: If the certification tag has been removed the device must be considered uncertified. If used and the certification date is not verified, or other prior official approval is obtained, access as a Cryptographic Incident.
Yes / No	I	76. Has NSA-furnished tamper detection labels been applied to certified/recertified KVG(s)? [EKMS-1 (Series), Article 1145.h, j] **NOTE:** If inspected and it is found that the NSA applied tamper detection tape has been removed or is damaged, the device is no longer considered certified and the matter must be reported as a Physical Incident
Yes / No	P	77. If the LE generates, receives, relays, or transmits electronic key for OTAD/OTAR/OTAT, are accounting records used and maintained for a minimum of 60 days following the date of the last entry? [EKMS-1 (Series), Article 1005.a.10, 1175.b(2), 1182.d.1] **NOTE:** Activities in which key received is strictly for updating the TEK (OTAR) purposes are not required to maintain logs as key is not being generated, transmitted, relayed or received and extracted.
Yes / No	A	78. Does the Primary (Issuing)

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

	LE (or Alternate) conduct a periodic review of OTAT/OTAR accounting logs? [EKMS-1 (Series), Article 455.K and 1115.c]

SECTION 9 - DATA TRANSFER DEVICE (DTD)/SIMPLE KEY LOADER (SKL)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	79. Is a classification tag attached to the DTD via the lanyard ring to indicate handling requirements when the Crypto Ignition Key (CIK) is not inserted? [EKMS-1 (Series), Annex Z, paragraph 8.f] **NOTE:** Only applicable to the DTD and not the SKL.
Yes / No	A	80. Is a tag attached to the CIK (e.g., via chain) to identify the CIK's classification and serial number? [EKMS-1 (Series), Annex Z, paragraph 9.d] **NOTE:** Only applicable to the DTD and not the SKL.
Yes / No	I	81. Are DTD's and/or SKL's which are initialized, storing key reinitialized at a minimum of annually? [EKMS-1 (Series) Annex Z paragraphs 17.a, 26.a.6, Annex AF paragraphs 9.c, 15.a.12] **NOTE:** To determine, randomly select a DTD or SKL which is

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		issued and have the audit data uploaded to the LMD for review. Failure to reinitialize a DTD and/or SKL annually is a cryptographic incident as the SKEK or LKEK/HDPK has a one-year crypto-period.
Yes / No	A	82. Are DTD's and/or SKL's inspected weekly to detect any breach in the casing? [EKMS-1 (Series) Annex Z paragraph 21, Annex AF paragraph 4.h] **NOTE:** If any cracks or breaches are detected in either a DTD and/or SKL it is not to be used for storing key and must be reported as a Physical Incident.
Yes / No	I	83. For LE's with a Top Secret CIK, is the CIK removed from the DTD and returned to TPI storage when authorized users are not present? [EKMS-1 (Series), Annex Z paragraph 10.b] **NOTE:** Otherwise, <u>both</u> CIK and DTD must be continually safeguarded according to TPI rules. A DTD found outside of proper storage with the CIK inserted would constitute a loss of TPI (Physical Incident). If only Secret and below key is in the device it will still be a Physical Incident, and should be reported and the audit data reviewed to determine when the device was last accessed and what it was used for (loading, passing, receiving key)

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	A	84. Is unrestricted access to Supervisory CIKs and/or the SSO password for the DTD and/or SKL, as applicable limited to only those who are authorized to perform all of the associated privileges? [EKMS-1 (Series), Annex Z, paragraph 11.d, Annex AF paragraph 4] **NOTE:** If discovered, this must be brought to the attention of the supporting EKMS Manager. User level access to a Supervisory CIK for the DTD or the CIK and password for the SSO account on the SKL prohibits effective auditing of the device as the user can; change the date and time of the device or delete the audit data itself!
Yes / No	I	85. Have recipients of key issued to a DTD or SKL, from a LMD/KP, signed a local custody document acknowledging receipt of the key? [EKMS-1 (Series), Annex Z, paragraph 13.d, Annex AF paragraph f.1] **NOTE:** Failure to utilize and maintain LCI documents is a Physical Incident.
Yes / No	I	86. Does the (Issuing) LE or Supervisory User locally account for all DTD CIKs by assigned serial number? [EKMS-1 (Series), Annex Z, paragraph 7.b]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	I	87. Does the (Issuing) LE or Supervisory User locally account for all DTD CIKs by assigned serial number? [EKMS-1 (Series), Annex Z, paragraph 7.b] **NOTE:** If the CIKS are not labeled properly and inventoried by serial number, a review of the audit trail data must be conducted to determine if a CIK is outside of proper accountability or lost. The loss of a CIK is a Physical Incident and for both the DTD and/or SKL they must have the association with the device deleted.
Yes / No	I	88. For **non-watch station** environments, are the Supervisory and User CIKs for DTD's inventoried whenever the parent account conducts semi-annual (Fixed-Cycle), Change of Command or Change of EKMS Manager inventories, as applicable? [EKMS-1 (Series), Annex Z, paragraph 14.a(1)] **NOTE:** By policy, failure to complete required inventories is a Physical Incident. Therefore, if these are not properly inventoried the inventory was not completed properly and this should be assessed as a Physical Incident.
Yes / No	P	89. For **watch station** environments, are the serial

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

		numbers of CIKs and the associated equipment (DTD or SKL) visually verified whenever watch personnel change? [EKMS-1 (Series), Annex Z, paragraph 14.b(1), Annex AF paragraph 8.f.3, Article 1005.a.4] **NOTE:** If both the devices and CIKS are not on the watch-to-watch inventory assess as a non-reportable PDS.
Yes / No	I	90. Is the DTD or SKL audit trail data reviewed by appropriate personnel at least once per month or when the Audit Trail icon illuminates, and are these reviews recorded in an Audit Review Log and retained for 2 years? [EKMS-1 (Series), Annex Z, paragraph 17.c, Annex AF paragraph 9.b] **NOTE:** Failure to conduct and document Audit Trail reviews or retain logs to support such is occurring is a Physical Incident.

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	91. Do all COMSEC users have access to the COMSEC portion of the command's EAP? [EKMS-1 (Series), Article 455.o, Annex M, paragraph 2,6]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	A	92. Are EAP training exercises conducted annually to ensure that everyone is familiar with their assigned duties? [EKMS-1 (Series), Annex M, paragraph 6.d(3)]
Yes / No	A	93. For commands located outside CONUS and deployable commands, does the EAP provide detailed guidance for both natural disasters and hostile actions and include Emergency Destruction Procedures (EDP)? [EKMS-1 (Series), Annex M,
		Paragraph 2.c,4 and 5]
Yes / No	A	94. When planning for natural disasters, does the EAP provide for: [EKMS-1 (Series), Annex M, Paragraph 4]
Yes / No		a. Fire reporting and initial fire fighting 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
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

SECTION 11 - EMERGENCY DESTRUCTION PLAN (EDP)

NOTE: Unless otherwise specified in Local, ISIC, or TYCOM directives, Section 11 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	95. Does the LE have an Emergency Destruction Plan (EDP) incorporated into its EAP? [EKMS-1 (Series), Annex M, Paragraph 2.c]
Yes / No	A	96. 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(6)]
Yes / No	A	97. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [EKMS-1 (Series), Annex M, Paragraph 5.d and 6.c]
Yes / No	A	98. Are the sensitive pages of KAMs prepared for **ready** removal (i.e., upper left corner clipped), and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [EKMS-1 (Series), Annex M, Paragraph 5.e(2)(a)]

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

Yes / No	A	99. Are the priorities of destruction indicated in the plan? [EKMS-1 (Series), Annex M, Paragraph 8]
Yes / No	A	100. Are the EDP divided into two parts: one for precautionary and one for complete destruction? [EKMS-1 (Series), Annex M, Paragraph 7]
Yes / No	A	101. 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 M, Paragraph 10]
Yes / No	A	102. Does the EDP stress that accurate information concerning the extent of emergency destruction is second in importance only to the destruction of the material itself? [EKMS-1 (Series), Annex M, Paragraph 10.a]
Yes / No	A	103. 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 M, Paragraph 9.d(2)(b)]
Yes / No	A	104. If LE deploys in aircraft, does the plan cover specific actions to be followed in aircraft? [EKMS-1 (Series), Annex M, paragraph 9.c]

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

PURPOSE. The purpose of this inspection guide is to ensure all aspects of COMSEC management are covered by the EKMS Inspector during the account inspection.

INITIAL REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

EKMS Account number: _____

Total Line items in EKMS account: _____

Immediate Superior in Command: _____

Date of Last EKMS Inspection: _____

Date of Last CMS A&A Periodic Training Visit: _____

Name/Grade/Rate and Command of EKMS Inspector:

_____

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:

_____

Remarks: _____

_____

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

SECTION IDENTIFICATION

1 - Security

2 - Local Element Responsibilities

3 - Local Custody File

4 - Watch Station Inventory/Page checks

5 - Resealing/Status Markings

6 - Corrections

7 - Routine Destruction

8 - Data Transfer Device (DTD)/Simple Key Loader (SKL)

9 - Over-the-Air-Rekey/Over-the-Air-Transfer

10 - Emergency Action Plan (EAP)

11 - Emergency Destruction Plan (EDP)

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the EKMS Inspector conducting the inspection. Per Chapter 2 and Article 401.c, inspection reports shall include references and comments to substantiate the evaluation. As such, below each item reviewed space is provided to annotate comments to any question that receives a negative response. The inclusion of the inspection checklists should greatly aid both Inspectors and the inspected activity in conducting the out-brief, as well as in preparation of the official report.

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

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 that access to classified information is given only to visitors who possess the proper identification, proper security clearance, and NEED TO KNOW? [SECNAV-M 5510.30A, Article 11-1 paragraph 2,3; SECNAV-M 5510.36, Article 7-11; EKMS-1 (Series), Article 550.e]
Yes / No	A	2. Is a visitor's register maintained and retained for one year? (consecutive years in one book authorized) [EKMS-1 (Series), Article 550.e, Annex T]
Yes / No	A	3. Is the COMSEC Facility or space outwardly identified only as a "RESTRICTED AREA"? [OPNAVINST 5530.14(series), Articles 210.g.4 and 218.a.4]
Yes / No	I	4. Is **unescorted** access limited to individuals whose duties require such access and who meet access requirements? [EKMS-1 (Series), Article 505] **NOTE:** See #5 (Part B) for when such could result in/constitute a COMSEC Incident.
Yes / No	A	5. Are the names of individuals with regular duty assignments in the COMSEC facility on a formal access list? [EKMS-1 (Series),

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		Article 550.e(1)(b)]
Yes / No	I	6. PART 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]
Yes / No	A/I	PART 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(2)] **NOTE: If personnel have access to keying material and are not reflected on the list or individual designation letter, access as an incident (review watch-to-watch inventory, SF-153's, CMS-25's, SF-702 to determine (unauthorized access). If access list is outdated, access as admin discrepancy.**
Yes / No	I	7. Are users of COMSEC material properly cleared at least as high as the level of classified material handled? [EKMS-1 (Series), Article 505.a] **NOTE: Personnel uncleared or not cleared to the level of material they have access to must be reported as a Physical Incident.**
Yes / No	A	8. Is security clearance data of personnel whose duties require access to COMSEC material maintained by the Command Security Manager? [SECNAV-M 5510.30A, Article 9-5 paragraphs 2,3,4,5] **NOTE:** For Marine Corps, clearance

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		data is documented in the Management Manpower System (MMS). For Coast Guard, clearance data is documented in the Personnel Management Information System (PMIS).
Yes / No	I	9. If material is held/used by LE personnel for SCI/SI circuits, are LE personnel with access to the container SCI eligible and indoctrinated or has DON CAF granted temporary access [EKMS-1 (Series), Article 414.d; SECNAV M5510.30 9-4.4].
Yes / No	A	10. 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	11. Are applicable security controls (e.g., guards and alarms) in place in accordance with SECNAV-M 5510.36, Chapter 10? [EKMS-1 (Series), Article 520.a(3)]
Yes / No	I	12. 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] **NOTE:** Effective 01 July 93 commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized to store any classified material. [EKMS-1

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		(Series), Article 520.f]
Yes / No	A	13. Is a Maintenance Record for Security Containers and Vault Doors (Optional Form 89) maintained for each security container and retained within the container? EKMS-1 (Series), Article 520.b(3)]
Yes / No	A	14. Are all damages, repairs or alterations to the container or parts of the container (e.g., Group 1R locks, locking drawer, drawer head, etc.) properly documented on an Optional Form 89? [SECNAV-M 5510.36, Article 10-15, paragraph 3; EKMS-1 (Series), Article 520.f, NOTE]
Yes / No	I	15. Do storage containers conform to the two person integrity (TPI) requirements for the protection of Top Secret COMSEC keying material? [EKMS-1 (Series), Article 520.e] **NOTE:** N/A if only Secret and below material is held
Yes / No	A	16. 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(1)]
Yes / No	A	17. 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(2)]
Yes / No	A	18. Are completed SF-702's retained for 30 days beyond the

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		last date recorded {EKMS-1 (Series} Article 520.b(2)(**NOTE**), Annex T paragraph 2.aa, and SECNAV-M5510.36 Article 7.11]
Yes / No	I	19. 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(1)] **NOTE:** If unauthorized or personnel without a clearance equal to/higher than the contents is discovered, report as a Physical Incident.
Yes / No	A	20. 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(3)(a)]
Yes / No	A	21. 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(3)(b); SECNAV-M 5510.36, Article 7-11]
Yes / No	A	22. Are completed SF-701's retained for 30 days beyond the last date recorded {EKMS-1 (Series} Article 550.d(3)(c), Annex T paragraph 2.a SECNAV-M5510.36 Article 7.11]
Yes / No	A	23. 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

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		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(3)(c)]
Yes / No	I	24. Are combinations & associated SF-700's for TPI containers completed, stored, and safeguarded to prevent a single person from having access to both combinations?? [EKMS-1 (Series), Article 510.c.2, 510.c.3]
Yes / No	I	25. Are sealed records of combinations to COMSEC storage 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] **NOTE:** If not properly stored in a GSA approved container, access as a Physical Incident in accordance with EKMS-1 (Series), Article 945.e.18.
Yes / No	A/I	26. Combinations to COMSEC material security containers must be protected as follows: [EKMS-1 (Series), Article 515.f]
Yes / No		a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope? **NOTE:** The sealing of the A & B combination to a TPI container **could result in a single person having access to the container (a Physical Incident**)
Yes / No	A	b. Combination envelope sealed using transparent lamination

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		paper or plastic tape?
Yes / No	A	c. Names of individuals authorized access to the combinations recorded on the front of the envelope?
Yes / No	A	d. Proper classification markings on envelope?
Yes / No	A	e. Are the envelopes inspected monthly to ensure they have not been tampered with?
Yes / No	A	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	27. Is COMSEC material stored separately from other classified material (e.g., separate container or drawer to facilitate emergency removal or destruction), and segregated by status, type and classification? [EKMS-1 (Series), Article 520.a(4) and Annex M, Paragraph 3]
Yes / No	I	28. When not being used and under the direct control of authorized personnel, is all COMSEC material properly stored? [EKMS-1 (Series), Article 520.a(2)]
Yes / No	A	29. Are classified COMSEC files, records and logs properly marked with the highest classification to the level of its contents and annotated with the following statement? [EKMS-1 (Series), Article 715.d(2)(c)]
		"Derived from: EKMS 1 (series) "Declassify on: 22 September

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

	2028” **NOTE:** The use of X1 – X8 is prohibited for downgrading /declassifying classified information. Declassification /Downgrading instructions will be in accordance with the CNO Policy ltr Ser N09N2/8U223000 dated 7 Jan 2008 until incorporated into SECNAV M5510.36. For records marked on/after 22 Sep 03, the date shown above reflects 25 years from the last authorized use of X1 – X8.

SECTION 2 - LOCAL ELEMENT RESPONSIBILITIES

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	30. For LE’s (external) supported through a LOA, are inventories completed for Change of Command or (OIC) (as applicable?) [EKMS 1 (Series) Article 766.a.3.d and 766.a.4 (note)]
Yes / No	A	31. Do all LE personnel have access to written guidance (provided by the account EKMS Manager) concerning the proper handling, accountability, and disposition of COMSEC material? [EKMS-1 (series), Articles 455.e]
Yes / No	A	32. Have all LE personnel completed a COMSEC Responsibility Acknowledgement

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		form? [EKMS-1 (Series) Article 465.n]
Yes / No	P	a. Are Commanding Officers/OIC's LE's conducting spot checks within their organization? [EKMS-1(B) Article 450.i NOTE 1]

SECTION 3 - LOCAL CUSTODY FILE

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I/A	33. Does the local custody file contain signed, effective, local custody documents for each item of COMSEC material charged to the account which has been issued to authorized LEs? [EKMS-1 (Series), Article 712, 945.e.6.c] **NOTE:** The absence or non-use of LCI documents is a Physical Incident however, **if the material is reflected on a watch-to-watch inventory and the EKMS Manager has the original LCI document, have a copy xeroxed for the LE, assess as an admin hit and train on the matter.**
Yes / No	A	34. Are local custody documents being maintained on file for 90 days after supersession? [EKMS-1 (Series), Annex T, paragraph 2.a]

SECTION 4 - WATCH STATION INVENTORY/PAGECHECKS

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	P	35. Does the CONTINUOUSLY MANNED WATCH STATION maintain a watch-to-watch inventory that lists all COMSEC material held (including accountability for resealed segments and CIKS for DTD's and/or SKL's issued)? [EKMS-1 (Series), Article 775.d(1), Annex Z, paragraph 14.b, Annex AD paragraph 17.b(3)] **NOTE:** Signatures are used to ensure compliance. Missing signatures or material not reflected on accounting reports constitutes a non-reportable PDS
Yes / No	P	36. Is the material recorded on the watch-to-watch inventory listed by short title, edition, accounting number (as applicable), and quantity? [EKMS-1 (Series), Article 775.d(2), 1005.a.1] **NOTE:** As the watch-to-watch inventory is an accounting report, if the required data is not reflected, such would constitute an incomplete accounting report.
Yes / No	P	37. Has the inventory been properly signed and dated for each change of watch? [EKMS-1 (Series), Article 775.d(4), (5),(6), 1005.a.1]

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Yes / No	A	38. Are watch-to-watch inventories being retained for 30 days beyond the last recorded date on the inventory? [EKMS-1 (Series), Annex T, paragraph j]
Yes / No	P	39. Have inventories for a NON-WATCH STATION ENVIRONMENT been conducted and recorded on the local custody issue document or a watch-to-watch inventory in accordance with EKMS-1 (Series)? [EKMS-1 (Series), Article 778.c, 1005.a.1] **NOTE:** Signatures are used to ensure compliance. Missing signatures or material not reflected on local accounting reports constitutes a non-reportable PDS.
Yes / No	A	40. Are required page checks being accomplished as follows: [EKMS-1 (Series), Article 775.e, 778.d; Annex Z]
Yes / No		a. Unsealed COMSEC keying material. Upon initial receipt; during account and watch inventories; and prior to destruction?
Yes / No		b. Resealed keying material. During Fixed-Cycle and Change of EKMS Manager inventories; and upon destruction?
Yes / No		c. Unsealed maintenance and operating manuals. Upon initial receipt; after entry of an amendment which changes pages; during Fixed-Cycle and Change of EKMS Manager inventories; and upon destruction?
Yes / No		d. Equipment. Upon initial receipt (uncrating); during

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Yes / No		Fixed-Cycle and Change of EKMS Manager inventories; during watch inventories; and upon destruction?
Yes / No	I	41. Are page check discrepancies reported to the account EKMS Manager or an Alternate? [EKMS-1 (Series), Articles; 775.f, 778.d, 945.e.1, Annex V] **NOTE:** Missing pages or cards, as applicable to COMSEC accountable books and/or Q-kits is a Physical Incident.

SECTION 5 - RESEALING/STATUS MARKINGS

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A/I	42. Are key tape canisters free of locally applied labels and stickers which may conceal attempted penetration or prevent inspection of protective packaging? [EKMS-1 (Series), Article 760.e, 760.f, 945.e.13.a] **NOTE: If discovered, remove label, inspect the canister and train user. If the canister is damaged, report as a Physical Incident.**

SECTION 6 - CORRECTIONS

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	43. Are corrections to publications made with black or blue-black ink only? [EKMS-1 (Series), Article 787.g(1)(b)1]
Yes / No	A	44. Is each pen and ink correction identified by writing the correction number in the margin opposite the correction? [EKMS-1 (Series), Article 787.g(1)(b)2]
Yes / No	A	45. 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(2)(a)]
Yes / No	A	46. 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(5)(b)]
Yes / No	A	47. Have both the person entering the correction and the person verifying the correction conducted a page check of the publication, and recorded this on the Record of Page checks page? [EKMS-1 (Series), Articles 787.g(4), (5)]

SECTION 7 - ROUTINE DESTRUCTION

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Yes / No	I	48. 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(2)(b), (d) and Article 945.e] **NOTE:** The absence of a destruction report or LCI document indicating the material has been returned to the supporting EKMS Manager is a Physical Incident.
Yes / No	P	49. Do destruction records clearly identify the short title, editions, accounting number, ALC, and date of destruction? [EKMS-1 (Series), Article 736.a(3); Figures 7-1, 7-2, 7-3, Article 1005.a.1]
Yes / No	P	50. Are LE destruction records properly signed, or initialed, by the two individuals who conducted the destruction? [EKMS-1 (Series) , Article 790.f(1)(2); Figures 7-1, 7-2, and 7-3, Article 1005.a.1]
Yes / No	P	51. Do local destruction records for segmented COMSEC material contain the following: [EKMS-1 (Series), Chapter 7 fig 7-1, 7-2, 7-3, Article 1005.a.1]
Yes / No		a. Short title and complete accounting data?
Yes / No		b. Date of destruction?
Yes / No		c. Signatures of the two individuals conducting destruction?
Yes / No	A	d. Marked "CONFIDENTIAL (When

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		filled in)”?
Yes / No	A	e. Classification/Declassification markings? Derived from: EKMS-1 (Series) Declassify on: 22 Sept 2028
Yes / No	P	52. 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.1] **NOTE:** Classified keying material is ALC 1 material requiring the accounting for each individual segment henceforth the policy that a CMS-25 can only be used for a single Short Title otherwise such would constitute and improperly completed accounting report.
Yes / No	I	53. Is routine destruction of COMSEC material performed in accordance with the methods prescribed in EKMS-1? [EKMS-1 (Series), Articles 540, 945.e.10
Yes / No	P	54. Is destruction of key issued either physically or in electronic form (DTD, SKL, TKL) being completed within the prescribed timeframes (EKMS-1 (Series), Article 540]
Yes / No	A	55. Can Local Element personnel demonstrate the proper procedures for conducting routine destruction of COMSEC material? [EKMS-1 (Series), Article 540, 790, Annex Z paragraph 15.b, Annex AF paragraph 8.f.4.]

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Yes / No	P/I	56. If keying material was unintentionally removed from its protective canister, is the following documentation recorded on its associated disposition record: [EKMS-1 (Series), Article 772.d, Article 1005.a.7, Article 945.e.13.b] **NOTE:** Except as authorized in Article 769.g **NOTE** 1, premature extraction is a non-reportable PDS even when properly documented on the CMS-25 however, when not documented on the CMS-25, report as a Physical Incident (Unexplained removal of key)
Yes / No		a. A statement that the keytape segment(s) were unintentionally removed?
Yes / No		b. The date of the unintentional removal?
Yes / No		c. Identity of the keytape segment(s) actually removed?
Yes / No		d. Signatures of the individuals who removed the key?

SECTION 8 - DATA TRANSFER DEVICE (DTD)/SIMPLE KEY LOADER (SKL)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	57. Is a classification tag attached to the DTD via the lanyard ring to indicate handling requirements when the Crypto Ignition Key (CIK) is not inserted? [EKMS-1 (Series),

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		Annex Z, paragraph 8.f] **NOTE:** Only applicable to the DTD and not the SKL.
Yes / No	A	58. Is a tag attached to the CIK (e.g., via chain) to identify the CIK's classification and serial number? [EKMS-1 (Series), Annex Z, paragraph 9.d] **NOTE:** Only applicable to the DTD and not the SKL.
Yes / No	A	59. Are DTD's and/or SKL's inspected weekly to detect any breach in the casing? [EKMS-1 (Series) Annex Z paragraph 21, Annex AF paragraph 4.h] **NOTE:** If any cracks or breaches are detected in either a DTD and/or SKL it is not to be used for storing key and must be reported as a Physical Incident.
Yes / No	I	60. For LE's with a Top Secret CIK, is the CIK removed from the DTD and returned to TPI storage when authorized users are not present? [EKMS-1 (Series), Annex Z paragraph 10.b] **NOTE:** Otherwise, both CIK and DTD must be continually safeguarded according to TPI rules. A DTD found outside of proper storage with the CIK inserted would constitute a loss of TPI (Physical Incident). If only Secret and below key is in the device it will still be a Physical Incident, and should be reported and the audit data reviewed to determine when the

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		device was last accessed and what it was used for (loading, passing, receiving key)
Yes / No	I	61. Is unrestricted access to Supervisory CIKs and/or the SSO password for the DTD and/or SKL, as applicable limited to only those who are authorized to perform all of the associated privileges? [EKMS-1 (Series), Annex Z, paragraph 11.d, Annex AF paragraph 4] **NOTE:** If discovered, this must be brought to the attention of the supporting LE Issuing or EKMS Manager, as applicable. User level access to a Supervisory CIK for the DTD or the CIK and SSO password for the SKL is prohibited and could prevent effective auditing of the device as the user can; change the date and time of the device or delete the audit data itself!
Yes / No	I	62. Have recipients of key issued to a DTD or SKL, from a LMD/KP, signed a local custody document acknowledging receipt of the key? [EKMS-1 (Series), Annex Z, paragraph 13.d, Annex AF paragraph f.1] **NOTE:** Failure to utilize and maintain LCI documents is a Physical Incident.
Yes / No	I	63. For **non-watch station** environments, are the Supervisory and User CIKs for DTD's inventoried whenever the parent account conducts semi-annual (Fixed-Cycle), Change of

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		Command or Change of EKMS Manager inventories, as applicable? [EKMS-1 (Series), Annex Z, paragraph 14.a(1)] **NOTE:** By policy, failure to complete required inventories is a Physical Incident. Therefore, if these are not properly inventoried the inventory was not completed properly and this should be assessed as a Physical Incident.
Yes / No	P	64. For **watch station** environments, are the serial numbers of CIKs and the associated equipment (DTD or SKL) visually verified whenever watch personnel change? [EKMS-1 (Series), Annex Z, paragraph 14.b(1), Annex AF paragraph 8.f.3, Article 1005.a.4] **NOTE:** If both the devices and CIKS are not on the watch-to-watch inventory assess as a non-reportable PDS.
As policy prohibits access to either the Supervisory CIK or SSO password for the DTD/SKL as applicable, questions 67 and 68 are only applicable when the LE is either located remotely from the LE Issuing or EKMS Manager and specifically designated personnel are authorized to conduct and document audit trail reviews.		
Yes / No	I	65. Is the DTD or SKL audit trail data reviewed by appropriate personnel at least once per month or when the Audit Trail icon illuminates, and are these reviews recorded in an Audit Review Log? [EKMS-1 (Series), Annex Z, paragraph 17.c, Annex AF paragraph 9.b] **NOTE:** Failure to conduct and

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		document Audit Trail reviews is a Physical Incident.
Yes / No	I	66. Is the Audit Review Log retained at least two years? [EKMS-1 (Series), Annex Z, paragraph 17.f] **NOTE:** Although a review of logs may indicate reviews are being conducted, by policy there is a mandated maximum period between reviews and the account MUST have two years worth of logs. If not, it cannot be ascertained the audits were conducted.

SECTION 9 - OVER-THE-AIR-REKEY/OVER-THE-AIR TRANSFER

NOTE: If a Key Variable Generator (KVG) (i.e., KG-83, KGX-93/93A) is not held, skip to question 69.

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	I	67. If held, does the certified KVG (KG-83/KGV-93) have a certification tag on the handle that displays the classification of the equipment, "CRYPTO" status, date of certification, command that performed certification, and name/rank of the certifying technician? [EKMS-1 (Series), Article 1145.i] **NOTE:** If the certification tag has been removed the device must be considered uncertified. If

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

		used and the certification date is not verified, or other prior official approval is obtained, access as a Cryptographic Incident.
Yes / No	I	68. Has NSA-furnished tamper detection labels been applied to certified/recertified KVG(s)? [EKMS-1 (Series), Article 1145.h, j] **NOTE:** If inspected and it is found that the NSA applied tamper detection tape has been removed or is damaged, the device is no longer considered certified and the matter report as a Physical Incident
Yes / No	P	69. If the LE generates, receives, relays, or transmits electronic key for OTAD/OTAR/OTAT, are accounting records used and maintained for a minimum of 60 days following the date of the last entry? [EKMS-1 (Series), Article 1175.b(2), 1182.d1 1005.a.10] **NOTE:** Activities in which key received is strictly for updating the TEK (OTAR) purposes are not required to maintain logs as key is not being generated, transmitted, relayed or received and extracted.

SECTION 10 - <u>EMERGENCY ACTION PLAN (EAP)</u>

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Answer	Non-Compliance Constitutes Indicate as appropriate (A = Admin, I = Incident, P = PDS)	Area/Item Reviewed
Yes / No	A	70. Do all COMSEC users have access to the COMSEC portion of the command's EAP? [EKMS-1 (Series), Article 455.o, Annex M, paragraph 2,6]
Yes / No	A	71. Are EAP training exercises conducted annually to ensure that everyone is familiar with their assigned duties? [EKMS-1 (Series), Annex M, paragraph 6.d(3)]
Yes / No	A	72. For commands located outside CONUS and deployable commands, does the EAP provide detailed guidance for both natural disasters and hostile actions and include Emergency Destruction Procedures (EDP)? [EKMS-1 (Series), Annex M, Paragraph 2.c,4 and 5]
Yes / No	A	73. When planning for natural disasters, does the EAP provide for: [EKMS-1 (Series), Annex M, Paragraph 4]
Yes / No		a. Fire reporting and initial fire fighting 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)?

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

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?

SECTION 11 - EMERGENCY DESTRUCTION PLAN (EDP)

NOTE: Unless otherwise specified in Local, ISIC, or TYCOM directives, Section 11 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	74. Does the LE have an Emergency Destruction Plan (EDP) incorporated into its EAP? [EKMS-1 (Series), Annex M, Paragraph 2.c]
Yes / No	A	75. 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(6)]
Yes / No	A	76. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [EKMS-1 (Series), Annex M, Paragraph 5.d and 6.c]

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Yes / No	A	77. Are the sensitive pages of KAMs prepared for **ready** removal (i.e., upper left corner clipped), and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [EKMS-1 (Series), Annex M, Paragraph 5.e(2)(a)]
Yes / No	A	78. Are the priorities of destruction indicated in the plan? [EKMS-1 (Series), Annex M, Paragraph 8]
Yes / No	A	79. Are the EDP divided into two parts: one for precautionary and one for complete destruction? [EKMS-1 (Series), Annex M, Paragraph 7]
Yes / No	A	80. 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 M, Paragraph 10]
Yes / No	A	81. Does the EDP stress that accurate information concerning the extent of emergency destruction is second in importance only to the destruction of the material itself? [EKMS-1 (Series), Annex M, Paragraph 10.a]
Yes / No	A	82. 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 M, Paragraph 9.d(2)(b)]

ANNEX C
EKMS INSPECTION GUIDE
LOCAL ELEMENT (USING)

Yes / No	A	83. If User deploys in aircraft, does the plan cover specific actions to be followed in aircraft? [EKMS-1 (Series), Annex M, paragraph 9.c]

ANNEX D
INSPECTION GUIDE VAULT

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the Inspector conducting the EKMS Inspection. The criterion set forth 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, Inspection Reports evaluated as unsatisfactory shall include references and comments to substantiate the evaluation. As such, below each item reviewed, space is provided to respond to any questions that receive a negative response. This inclusion in the inspection checklists will greatly aid EKMS Inspectors 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 D or E, as applicable may not translate to specific a 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 bi-annual inspections). 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 EKMS Inspection Report) should not be granted without consulting NCMS and requesting a waiver for any non-compliant items noted.

ANNEX D
INSPECTION GUIDE VAULT

VAULT CHECKLIST

Answer	Area/Item Reviewed
Yes / No	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 N , Paragraph 2] a. Floors and walls: Poured, reinforced concrete, minimum 8" thick reinforcing rods 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.
Yes / No	b. Roof: Single piece, reinforced-concrete slab of a thickness to be determined by structural requirements, but not less than the walls and floors.
Yes / No	c. Ceiling: 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. **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.
Yes / No	d. Vault Door and Frame Unit: 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.
Yes / No	e. Lock: A combination lock that conforms to the Underwriters' Laboratories, Inc. Standard No. 768, for Group 1R or Group 1. The specific lock model used shall bear a valid UL Group 1R or Group 1 label. **NOTE:** All vault doors procured after 14 April 1993 must be equipped with a GSA-approved

ANNEX D
INSPECTION GUIDE VAULT

	combination lock that meets the requirements of Federal Specifications FF-L-2740. [EKMS-1 (Series), Annex N , paragraph 2 NOTE]
Yes / No	2. Are shore based CMS storage vaults equipped with the following minimum safety requirements: [EKMS-1 (Series), Annex N , paragraph 5.a] a. A luminous type light switch? **NOTE:** May be painted with fluorescent paint.
Yes / No	b. Is emergency lighting installed?
Yes / No	c. An interior alarm switch or device? (e.g., telephone, intercom)
Yes / No	d. A decal containing emergency instructions on how to obtain release if locked inside the vault?
Yes / No	3. If an emergency escape device **is** considered necessary, have the following minimum requirements been met: [EKMS-1 (Series), Annex N, paragraph 5.b]
	a. Is it permanently attached to the **inside** of
	the door and cannot be activated by the exterior locking device, or otherwise accessible from the outside?
Yes / No	b. Is it designed and installed so that drilling and rapping the door from the outside will not give access to the vault by activating the escape device?
Yes / No	c. Has the device met the requirements of GSA Federal Specification AA-D-600 series (GSA-FSS) Ch. 4 paragraph 4.4.8, dated 15 May 2000, concerning an exterior attack on the door? **NOTE:** A copy of AA-D-600 titled "Federal Specification Door, Vault Security" and related amendments can be obtained by clicking on the URL in this note.
Yes / No	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 ~~O~~, paragraph 5.c] a. A UL Bank Vault Emergency Ventilator?
Yes / No	b. At least one UL approved fire extinguisher

ANNEX D
INSPECTION GUIDE VAULT

	situated in a position near the vault door? **NOTE:** These provisions are recommended even if an emergency escape device is provided.
Yes / No	5. Are emergency destruction tools readily available? [EKMS-1 (Series), Annex M, paragraph 5.d and 6.c]
Yes / No	6. Is the space/compartment or vault which contains COMSEC material outwardly identified as "RESTRICTED AREA/AUTHORIZED PERSONNEL ONLY"? [OPNAVINST 5530.14 (series), Articles 210 and 218.
Yes / No	7. 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	8. If the original security integrity of the vault has been degraded in any way, have approved repairs been made? [SECNAV-M 5510.36, Article 10-15]
	NOTE: Effective 01 July 93, commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized to store any classified material. [EKMS-1 (Series), Article 520.f]
Yes / No	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?

ANNEX E

INSPECTION GUIDE
FIXED COMSEC FACILITY

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.

INITIAL REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

EKMS Account number: _____

Total Line items in EKMS account: _____

Immediate Superior in Command: _____

Date of Last EKMS Inspection: _____

Name/Grade/Rate and Command of EKMS Inspector:

_____

Date of Last Facilities Approval: _____

EKMS Manager Name/Grade: _____

Alternate EKMS Manager Name/Grade/Date of Appointment:

_____

Identify Following, as Applicable/Assigned:

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

_____

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

_____

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

_____

Remarks: _____

ANNEX E

INSPECTION GUIDE
FIXED COMSEC FACILITY

ACTION. The following inspection checklist shall be used and completed in its entirety by the EKMS Inspector conducting the EKMS Inspection. Per Chapter 2 and Article 401.c., unsatisfactory Inspection Reports shall include references and comments to substantiate the evaluation. As such, below each item reviewed, space is provided to respond to any questions that receive a negative response. This inclusion in the inspection checklists will greatly aid EKMS Inspectors 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 D or E, as applicable may not translate to specific a 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 bi-annual inspections). 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 bi-annually thereafter for continued storage of classified COMSEC material. Initial facility approval or continued approval (in the form of the EKMS Inspection Report) should not be granted without consulting NCMS and requesting a waiver for any non-compliant items noted.

ANNEX E

INSPECTION GUIDE
FIXED COMSEC FACILITY

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 O, 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 O, paragraph 2]
Yes / No	3. Are walls constructed from **true** floor to **true** ceiling? [EKMS-1 (Series), Annex O, 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 O, paragraph 3.b]
Yes / No	5. If false 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 O, paragraph 3.c]
Yes / No	6. Is only one door used for regular entrance to the facility, though other doors may exist for emergency exit and entry or removal of bulky items? [EKMS-1 (Series), Annex O, 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 O, paragraph 4.b(1)(a) through (c)] 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

ANNEX E

INSPECTION GUIDE
FIXED COMSEC FACILITY

	reinforced, hollow metal industrial doors, **or** metal-clad or solid hardwood doors with a minimum thickness of 1-3/4"). **NOTE**: Unattended telecommunications facilities constructed after 1983 shall have only one door.
Yes / No	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?
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 not continuously manned, is the door equipped with a GSA-approved, electro-mechanical lock meeting Federal Specificat**ion FF**-L-2740? [EKMS-1 (Series), Annex O, paragraph 4.b(2)]
Yes / No	9. If the facility is continuously manned (a built-in lock is not required), is the door designed so that a GSA-approved **electro-mechanical** lock Meeting Federal Specification FF-L-2740 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 O, paragraph 4.b(2)(a)] **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 not afford the required degree of protection and may not 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

ANNEX E

INSPECTION GUIDE
FIXED COMSEC FACILITY

	only be opened from inside the facility? [EKMS-1 (Series), Annex O, paragraph 4.b(3)]
	NOTE: Approved panic hardware and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the interior 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 O, paragraph 4.b(4)]
Yes / No	12. Is a method employed to establish positive visual identification of a visitor before entrance is granted? [EKMS-1 (Series), Annex O, paragraph 4.b(4)(a)]
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 O, paragraph 4.b(4)(b)]
Yes / No	14. Where windows exist, are they secured in a permanent manner to prevent them from being opened? (COMSEC facilities normally should not normally contain windows.) [EKMS-1 (Series), Annex O, paragraph 5]
Yes / No	15. Are windows alarmed and/or barred to prevent their use as an access point? [EKMS-1 (Series), Annex O, 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 O, 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 O, paragraph 6]
Yes / No	19. Do openings which are less than 96 square inches, have approved baffles installed to prevent an audio or acoustical hazard? [EKMS-1

ANNEX E

INSPECTION GUIDE
FIXED COMSEC FACILITY

	(Series), Annex O, Paragraph 6.a]
Yes / No	20. 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 O, paragraph 6.b]

ANNEX F

EKMS INSPECTION REPORT
EXAMPLE

From: (EKMS Inspector)
To: (ISIC/IUC)

Subj: REPORT OF EKMS INSPECTION OF (COMMAND TITLE)

Ref: (a) EKMS 3C

1. Title of command inspected:_____
EKMS Manager: _____
Primary Alternate Manager: _____
EKMS ID number:_____
Date inspected:_____
Inspected by:_____
(Name, Rank/Rate/Grade)
EKMS Inspector Certification:_____
(Date Certified/Re-certified)
Certifying ISIC/IUC:_____
Certifying A&A Team:_____

2. Evaluation of the command or unit inspected, [GRADE: (SAT or UNSAT)] and comments as required to substantiate the evaluation.

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

ANNEX F

EKMS INSPECTION REPORT
EXAMPLE

source external to the Department of the Navy shall include the Subj: REPORT OF EKMS INSPECTION OF (COMMAND TITLE)

appropriate caveat included in EKMS 3C, either Article 410.a, 410.b or 410.c]

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 inspection.

R.U.UNDERWAY

Copy to:
(NCMS//N7// and ISIC/IUC)

ANNEX G

ISIC EKMS INSPECTION
SEMI-ANNUAL REPORT

ISIC/IUCS will use the following template to report EKMS Inspection-related information to NCMS/N7 via Naval message. Reports will be submitted at a minimum of semi-annually and formatted supplying the content as reflected below:

BEGIN TEMPLATE

DDHHMMZ MON YR
FM ISIC/IUC
TO NCMS WASHINGTON DC/N7//
INFO COMNAVCYBERFOR VIRGINIA BEACH VA
SERVICING CMS AA TEAM
BT
(C O N F I D E N T I A L WHEN FILLED IN)
MSGID/GENADMIN/COMSUBRON SEVENTEEN/-/MMM//
SUBJ/EKMS ISIC SEMI-ANNUAL INSPECTION REPORT (**1ST HALF CY 20XX, MODIFY AS APPLICABLE**)(U)//
REF/A/DOC/NCMS WASHINGTON DC/05APR2010//
AMPN/REF A IS EKMS-1B//
POC/DOE,JOHN/LT/CSR-17/N6/240-857-7808/TEL:DSN 857-7808/EMAIL:JOHN.DOE(AT)NAVY.SMIL.MIL//
RMKS/1. (C) PER REF (A), THE FOLLOWING INFORMATION IS PROVIDED FOR CY 20XX:

A. COMPLETE LISTING OF SUBORDINATE EKMS ACCOUNTS:

	NAME	ACCT#	(COR)	LAST INSP/LAST AA VISIT:
(1)	USS NAUTILUS	*******	NCMS	15JAN10 18 JUL 09
(2)	USS SKIPJACK	*******	NCMS	10FEB10 20 AUG 09
(3)	USS DOLPHIN	*******	NCMS	14MAR09 28 FEB 09

B. EKMS INSPECTIONS/RESULTS: (ART 315)

	NAME	RESULTS	INCIDENTS	PDS	ADMIN	INSPECTOR
(1)	USS BLUEBACK	SAT	NONE	NONE	12	CSR-17
(2)	USS HOUSTON	UNSAT	1	3	30	CSR-17
(3)	USS PORTSMOUTH	SAT	NONE	1	7	CSR-17

C. EKMS TOWN HALL ATTENDANCE: (ART 325)

	NAME	DATE	REASON FOR NON-ATTENDANCE
(1)	USS OHIO	20 FEB 10	
(2)	USS SEAWOLF	20 FEB 10	
(3)	USS THRESHER		ON PATROL

D. FIXED-CYCLE INVENTORY/SAIR (TWICE EACH CY) (ART 766, ANNEX AK)

NAME	LAST PHYSICAL INVENTORY	LAST RECONCILIATION

ANNEX G

ISIC EKMS INSPECTION
SEMI-ANNUAL REPORT

(1) USS VIRGINIA 15 OCT 11 15 NOV 11
(2) USS ANNAPOLIS 20 DEC 11 24 DEC 11
(3) USS SCORPION 30 JAN 12 07 FEB 12

2. (C) SPECIFICS ON INCIDENTS/PDS/ADMIN/NCI:

(A) INCIDENTS: NUMBER AND TYPE (I.E., MISSING MATERIAL, ETC.)

(B) PDS: NUMBER AND TYPES (I.E., LATE DESTRUCTION, ETC.)

(C) NON-COMPLIANT ITEMS (NCI): USE FOR ITEMS WHICH ARE NOT IDENTIFIED BY THE ANNEXES AND QUESTIONS BUT ARE DEVIATIONS FROM POLICY AND REQUIRE WAIVERS OR ARE OF A SIGNIFICANT NATURE BUT ARE NOT OTHERWISE DEFINED AS A PDS OR INCIDENT. FOR ALL DISCREPANCIES INCLUDE THE FOLLOWING:

(1) REGULATION/PUBLICATION(S) AND SECTION AND SUBSECTION NUMBER(S):

(2) REGULATION/PUBLICATION STANDARD HEADING/TOPIC AREA:

(D) CLEAR, DETAILED DESCRIPTION OF THE NON-COMPLIANCE INCLUDING, BUT NOT LIMITED TO:

(1) LOCATION OF THE DEFICIENCY, E.G., BUILDING, SHIP, RADIO, VAULT, ETC.

(2) COMPLETE DESCRIPTION OF WHAT IS NOT IN COMPLIANCE.

(3) CORRECTION DATE - "TO BE CORRECTED BY: (DATE)
NOTE: IF A NCI IS CORRECTED DURING THE INSPECTION, THE INSPECTOR MAY USE HIS/HER DISCRETION WHETHER OR NOT TO CITE THE NCI. IF CITED, PUT "CORRECTED DURING THE INSPECTION.

(E) TOTAL NUMBER OF ACCTS HAVING "OUTSTANDING" NCI IDENTIFIED DURING PREVIOUS INSPECTION: (REFERENCE ACCT NR OF COMMAND; IDENTIFY ITEM THAT REMAINS UNCORRECTED; REASON GIVEN FOR FAILURE TO CORRECT):

(F) TRENDS OBSERVED AMONG ACCTS INSPECTED (E.G., MORE THAN ONE INSTANCE OF MISAPPLICATION OR MISUNDERSTANDING OF EXISTING POLICY, FAILURE TO CORRECTLY APPLY TPI, USE OF INCORRECT TRANSPORTATION METHOD FOR CCI, ETC.):

(G) TOTAL NUMBER OF FEEDBACK REPORTS (AS DEFINED IN EKMS 3 (SERIES))SUBMITTED TO NCMS THUS FAR IN CYXX:

ANNEX H

EKMS FEEDBACK REPORT
EXAMPLE

FM (ISIC/IUC)//OFFICE CODE//
TO NCMS WASHINGTON DC//N7//
INFO CHAIN OF COMMAND
BT
UNCLAS //N02201//
MSGID/GENADMIN/(ORIG ISIC/IUC PLA)//
SUBJ/EKMS FEEDBACK REPORT//
REF/A/DOC/NCMS/05APR2010//
AMPN/EKMS-3(SERIES) EKMS INSPECTION MANUAL, ARTICLE 405//
POC/R.U. UNDERWAY/ITCS(SW)/-/-/DSN:321-7654//
RMKS/1. ISIC/IUC INSPECTOR'S RECOMMENDATION(S) FOR CHANGES TO EKMS INSPECTION POLICY AND/OR PROCEDURES. BE SURE TO PROVIDE APPLICABLE SUPPORTING DOCUMENTATION.//

BT

ANNEX I

EKMS ISIC/IUC INSPECTION ENDORSEMENT EXAMPLE

From: ISIC/IUC

To: Inspected Command

Subj: ENDORSEMENT ON (INSPECTED COMMAND) EKMS INSPECTION DATED DD MMM YY LTR (SERIAL NUMBER OF INSPECTION REPORT)

Ref: (a) EKMS-3(Series) Article 110.e
(b) Inspection 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 inspection report.

R.U. Underway
CTF 99, N61