



UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
PSC BOX 8003
CHERRY POINT, NC 28533-0003

AirStaO 2250.1F
TISD
12 FEB 2009

AIR STATION ORDER 2250.1F w/ch 1

From: Commanding Officer, Marine Corps Air Station, Cherry Point
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR DISTRIBUTION AND CONTROL
OF THE ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS)

Ref: (a) EKMS 1 (series)
(b) SECNAVINST 5510.36 (series)

1. Situation. Communications Security (COMSEC) material is that material used to protect U.S. Government transmissions, communications, and the processing of classified or sensitive unclassified information related to national security from unauthorized persons. The EKMS system has been established to distribute, control, and safeguard COMSEC material, and thus is the means for protection of vital and sensitive information moving over government communications systems.

2. Cancellation. AirStaO 2250.1E.

3. Mission. To fulfill the requirement set forth in reference (a) to provide detailed, supplemental instructions for the handling, accounting and disposition of Communications Security (COMSEC) material within this command.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. The procedures listed below are promulgated for the internal distribution and control of EKMS material and equipment within this Command. It is the responsibility of the Command EKMS Manager and all other individuals, whom, for any reason, assume custody, use or otherwise are charged with the safeguarding of EKMS material to fulfill the requirements set forth in this Order.

DISTRIBUTION STATEMENT A: Approved for public release;
distribution is unlimited.

12 FEB 2009

(2) Concept of Operations

(a) The Command will designate in writing an EKMS Manager, a primary alternate and at least one additional alternate manager who will be equally responsible for the proper administration of the Command's EKMS account. The Command EKMS Manager is responsible to the Commanding Officer for the proper management and security of all COMSEC material held at the Command. The EKMS Manager is the principal advisor to the Commanding Officer concerning EKMS matters.

(b) A copy of this Order will be maintained by each Local Element (LE) and a copy made readily available to each EKMS user that assumes custody and responsibility for EKMS material and equipment.

(c) A COMSEC Responsibility Acknowledgement Form will be executed by each individual user of EKMS material and returned to the Station EKMS Manager. An example is contained in ~~annex J~~ **ANNEX K** of reference (a).

(d) Reference (a) contains detailed requirements and guidelines pertaining to the administration and physical security of EKMS. Handling of Secure Terminal Equipment (STE) and associated ~~*KOV-14~~ cryptographic cards will be in accordance with reference (a) and Air Station Order ~~2200.1D~~ **2200.1E**.

b. Task

(1) MCAS TISD

(a) Will appoint an EKMS Manager per guidelines set forth in reference (a).

(b) Will appoint an EKMS Primary Alternate Manager and at least one additional Alternate Manager and any additional Alternate Managers that may be required.

(2) MCAS EKMS Manager and Alternate EKMS Managers. The EKMS Manager is responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of COMSEC material assigned to an EKMS account and also serves as the Commanding Officer's primary advisor on EKMS account management matters. In this capacity, the EKMS Manager must:

(a) Provide the Commanding Officer and other interested personnel with information about new or revised COMSEC policies and procedures and their impact on the command.

(b) Maintain the command COMSEC material allowance, including conducting annual re-validation of all COMSEC material holdings.

(c) Maintain proper storage and adequate physical security for the COMSEC material held by the account.

(d) Provide Local Elements written guidance necessary for the accurate and secure handling/accounting of COMSEC materials.

(e) Conduct training to ensure all personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures and keep Alternate Managers informed of the account status to ensure they are capable of assuming the duties of the EKMS Manager.

(f) Maintain records and files as required by reference (a) and ensure prompt and accurate preparation, signature, and submission of account correspondence, message, and accounting reports.

(g) Issue COMSEC material on local custody forms to properly cleared, authorized recipients who have executed a COMSEC Responsibility Acknowledgment Form.

(h) Ensure that procedures are established to reassign local custody responsibility for COMSEC material held by individuals permanently leaving the command, or are departing on leave or TAD in excess of 30 days.

(i) Maintain the account's portion of the command Emergency Protection Plan (EPP) per Annex ~~T~~ of reference (a).

(3) MCAS Local Elements. Local Element personnel are responsible to their Commanding Officer for the proper management and security of all COMSEC material in their custody and responsible to their servicing EKMS account for the proper accountability, security, control, and disposition of COMSEC material issued to them. Local Elements must also:

12 FEB 2009

(a) Provide their Commanding Officer, if different from their servicing EKMS account, with information about new or revised COMSEC policies and procedures and their impact on the command.

(b) Follow written instructions issued by their servicing EKMS account governing the handling, accountability, and disposition of COMSEC material. Conduct and document training to ensure that all Local Element personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures. Emphasis should be placed on accountability, security and identification of improper practices.

(c) Ensure proper inventory, storage and adequate physical security is maintained for all COMSEC material.

(d) Maintain required records.

1. Access roster for areas where COMSEC material or equipment is stored or in use signed by the Commanding Officer.

2. Copy of Commanding Officer Authorization to handle COMSEC letter or roster.

3. Copies of each COMSEC User Acknowledgement form for every individual authorized by the Commanding Officer to handle COMSEC material.

4. Copy of annual Physical Security Evaluations (PSE) conducted by the Provost Marshal Office (PMO).

5. Copies of semi-annual inventories and all effective SF-153 custody documents.

6. Daily SF-701 inventories of all COMSEC holdings by serial number.

7. Documented COMSEC training events.

8. Copies of past Local Element spot-check results.

c. Coordinating Instructions

(1) Control and Reporting. Control of COMSEC material is based on the following:

(a) A continuous chain of custody receipts using both transfer reports and local custody documents.

(b) Accounting records, such as periodic inventory reports, possession reports, generation reports, conversion reports, destruction records, transfer reports, and local custody records.

(c) Immediate reporting of COMSEC material incidents to ensure compromise decisions are made expeditiously by controlling/evaluating authorities.

(2) Definitions

(a) Electronic Key Management System (EKMS). Interoperable collection of systems designed by the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

(b) EKMS Account. An administrative entity, identified by a six-digit account number (same number as account's EKMS ID), responsible for maintaining accountability, custody and control of COMSEC material. Also identified as or referred to as COMSEC account and/or CMS account.

(c) EKMS Manager. Individual designated in writing to manage COMSEC material issued to an EKMS account. The EKMS Manager is the Commanding Officer's primary advisor on matters concerning the security and handling of COMSEC material and the associated records and reports. The Command EKMS Manager represents the Commanding Officer, MCAS, Cherry Point for COMSEC material held by the Command and, when applicable, reports routine matters to the Commanding Officer.

(d) Alternate EKMS Manager(s). Individual(s) designated in writing by the Commanding Officer, and is responsible for assisting the EKMS Manager in the performance of his/her duties and assuming the duties of the EKMS Manager in his/her absence. Alternate Manager(s) share equally with the EKMS Manager the responsibility for the proper management and administration of an EKMS account.

(e) Local Element. Local Elements are separate entities, units, or commands, internal or external to the parent EKMS account, that require COMSEC material. Local Element

12 FEB 2009

personnel are designated in writing by his/her Commanding Officer. Local Elements, irrespective of command relationships, must adhere to the procedures in reference (a) and written instructions issued by their servicing EKMS Manager.

(3) Access to COMSEC Material

(a) Security Clearance. Access to classified COMSEC material requires a security clearance equal to or higher than the classification of the COMSEC material involved. However, access to unclassified COMSEC material does not require a security clearance.

(b) Need-to-know. Access to classified COMSEC material must be restricted to properly cleared individuals whose official duties require access to COMSEC material.

(c) Briefing/Indoctrination. All personnel who have access to COMSEC material must complete a COMSEC Responsibility Acknowledgement Form per Annex J of reference (a) and be properly indoctrinated regarding the sensitivity of the material, the rules for safeguarding such material, the procedures for reporting COMSEC incidents, the laws pertaining to espionage, and the rules pertaining to foreign contacts, visits, and travel per SECNAVINST 5510.30 (series).

(d) Written Access to COMSEC Keying Material. All personnel having access to COMSEC keying material must be authorized in writing by the Commanding Officer. Either an individual letter or an access roster may be used. Foreign nationals will not be granted access to, or provided information about, COMSEC keying material without written permission from the material's controlling authority. Access to other COMSEC material must be approved by NSA//DP02//.

(e) Record all visits in the visitor register and retain the register for at least 1 year. The visitor register, at a minimum, will contain the following:

1. Date/time of arrival and departure.
2. Printed name and signature of visitor.
3. Purpose of visit.

12 FEB 2009

4. Signature of authorized individual admitting the visitor(s).

(4) Safe Combinations. Each lock must have a combination composed of randomly selected numbers based on constraints of the manufacturer. The combination must not deliberately duplicate a combination selected for another lock within the command and must not be composed of successive numbers, numbers in a systematic sequence, or predictable sequences (e.g., birth dates, social security numbers, phone numbers).

(a) Combinations must be changed as follows:

1. When the lock is initially placed in use. A manufacturer preset combination **may not** be used.

2. When any person having knowledge of the combination no longer requires access.

3. When the possibility exists that the combination has been subjected to compromise.

4. When the combination has been taken out of service.

5. When any repair work has been performed on the combination lock.

6. At least once every 2 years or sooner as dictated by the above events.

(b) Lock combinations shall be classified and safeguarded the same as the highest classification of the material being protected by the combination.

(c) To provide for emergency access, a central record of the lock combinations for all COMSEC material security containers must be maintained in a security container, other than the container where COMSEC material is stored, and approved for storage of the highest classification of the material protected by the combination locks.

(d) Combinations to COMSEC material security containers must be protected as follows:

12 FEB 2009

1. Each combination must be recorded and individually wrapped in aluminum foil and protectively packaged in a separate SF-700 combination envelope.

2. Laminate each envelope in plastic (like an identification card) or seal in plastic tape.

3. The name and address of the individual(s) authorized access to the combinations must be recorded on the front of the envelope.

4. Individual protectively wrapped envelopes may be stored in the same single-lock security container.

5. Inspect the envelopes monthly to ensure they have not been tampered with and document the inspection finding utilizing a locally generated log. Minimum data logged must be date of inspection, printed name of the individual conducting the inspection and the signature of that individual.

(5) COMSEC Storage Requirements

(a) Store COMSEC material separately from other classified material (e.g., in separate containers or in separate drawers).

(b) Store COMSEC material only in containers and spaces approved for their storage. Unless COMSEC material is under the direct control of authorized persons, keep the containers and spaces locked.

(c) Comply with applicable information on supplementary controls (e.g., guards and alarms) for safeguarding classified material in accordance with chapter 10 of reference (b).

(d) Unkeyed Controlled Cryptographic Items (CCI) and/or CCI keyed with unclassified key marked or designated CRYPTO, must be stored in a manner that affords protection against pilferage, theft, sabotage, or tampering, and ensures that access and accounting integrity are maintained.

(e) Store classified, unkeyed equipment in the same manner as classified material of the same classification.

12 FEB 2009

(f) Protect all keyed equipment based on the classification of the equipment or the keying material, whichever is higher. Additionally, ensure that procedures are in effect to prevent unauthorized use of the equipment or extraction of its key.

(g) Keyed COMSEC equipment used to terminate full-time nets/circuits may be left in unattended spaces only if such spaces meet Department of the Navy criteria for open storage of information classified at the same level of the Traffic Encryption Key (TEK) used.

(h) In a continuously manned facility, a security check utilizing an SF-701 checklist will be conducted once per shift, at least once every 24 hours, to ensure that all classified COMSEC information is properly safeguarded, and that physical security protection systems/devices (e.g., door lock and vent covers) are functioning properly.

(i) In a non-continuously manned facility, conduct a security check utilizing an SF-701 checklist prior to departure of the last person to ensure the facility entrance door is locked and where installed, Intrusion Detection Systems (IDS) are activated.

(j) Where a facility is unmanned for periods greater than 24 hours (e.g., during weekends and holidays), the facility is to be protected by an approved IDS. A check must be conducted at least once every 12 hours to ensure that all doors to the facility are locked, and that there have been no attempts to forced entry.

(6) Required Forms for Storage Containers

COMPUTER

IS REQUIRED

(a) A classified[^]container information form, SF-700, [^]for each lock combination, must be placed on the inside of each COMSEC storage container. [^]THE TOP COPY OF THE FORM

(b) A security container open/closure log, SF-702, must be maintained for each lock on a COMSEC storage container. Each opening and closure of the container must be annotated on the accompanying SF-702.

(c) A Maintenance Record for Security Containers/Vault Doors, Optional Form 89, must be used as a permanent record and retained for the service life of the security container/vault door.

12 FEB 2009

(d) Paragraph 7-10 of reference (b) requires that Commanding Officers establish procedures for end of the day security checks, utilizing the SF-701 Activity Security Checklist, to ensure that all areas which process classified information are properly secured.

(7) Emergency Access to Containers and Combinations. In an emergency, the Commanding Officer, Security Manager or designated authority may direct the opening of any COMSEC material security container.

(a) At least two individuals shall be present to conduct and witness the emergency opening.

(b) After an emergency opening, the official who opened the container will make an after-the-fact report to the person in charge of the container.

(c) The individual(s) responsible for a container opened in an emergency must immediately conduct a complete inventory of the COMSEC material, and change the combinations as soon as possible.

(8) Destruction of COMSEC Material

(a) Routine destruction of COMSEC material will be carried out by the MCAS, Cherry Point EKMS Manager **only**.

(b) Hostile emergency destruction of COMSEC material will be carried out in accordance with Annex ~~T~~_M of reference (a).

(c) In the event of a hurricane, fire, flood, or other natural disaster, COMSEC material will be safeguarded in accordance with Annex ~~T~~_M of reference (a) and Air Station Order 5510.18~~B~~_C.

(9) COMSEC Incidents and Reporting Requirements. COMSEC incidents could potentially result in serious damage to national security and must be reported to the NSA. Immediately notify the EKMS Manager to report any of the following occurrences:

(a) COMSEC incidents are divided into three categories:

1. Cryptographic

12 FEB 2009

2. Personnel

3. Physical

(b) Examples of Cryptographic Incidents.

1. Use of COMSEC keying material that is compromised, superseded, defective, previously used (and not authorized for reuse), or the incorrect application of keying material such as use of keying material that was produced without the authorization of National Security Agency (NSA).

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

3. Unauthorized extension of a crypto period.

4. Use or attempted use of a Key Processor beyond its mandatory re-certification date without prior approval.

5. Use of COMSEC equipment having defective cryptographic logic circuits, or use of an unapproved operating procedure.

6. Plain text transmission resulting from a COMSEC equipment failure or malfunction.

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

8. Operational use of equipment without completion of required alarm check test or after failure of required alarm check test.

9. Use of any COMSEC equipment or device that has not been approved by NSA.

10. Discussion via non secure telecommunications of the details of a COMSEC equipment failure or malfunction.

11. Detection of malicious codes (viruses) on the EKMS system.

12. Any other occurrence that may jeopardize the crypto security of a COMSEC system.

12 FEB 2009

13. Failure to return a Key Processor for Re-Certification when it is due.

(c) Examples of Personnel Incidents

1. Known or suspected defection.

2. Known or suspected espionage.

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

4. Unauthorized disclosure of Personal Identification Numbers (PIN) and/or passwords that are utilized on systems which allow access to COMSEC material/information.

5. Unauthorized disclosure of information concerning COMSEC material.

6. Attempts by unauthorized persons to effect disclosure of information concerning COMSEC material.

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

(d) Examples of Physical Incidents

1. The physical loss of COMSEC material.

2. The physical loss and/or compromise of KP Crypto Ignition Keys (CIKs), all KP related keys or CIKs which contain, or may contain, EKMS related information, and any floppy disk containing key or other EKMS information.

3. Unauthorized access to COMSEC material by un-cleared persons.

4. Unauthorized access to COMSEC material by persons inappropriately cleared.

5. COMSEC material discovered outside of required accountability or physical control. For example:

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

b. Material left unsecured and unattended where unauthorized persons could have had access.

c. Failure to maintain required TPI for Top Secret keying material, except where a waiver has been granted.

6. COMSEC material and/or EKMS components improperly packaged or shipped.

7. Receipt of classified equipment, CCI equipment, or keying material marked or designated CRYPTO with a damaged inner wrapper.

8. Destruction of COMSEC material by other than authorized means.

9. COMSEC material not completely destroyed and left unattended.

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

11. Tampering with, or penetration of, a cryptosystem. For example:

a. COMSEC material received in protective packaging which shows evidence of tampering.

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

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

d. Discovery of a clandestine electronic surveillance or recording device in or near a COMSEC facility.

e. Activation of the anti-tamper mechanism on, or unexplained zeroization of, COMSEC equipment when other indications of unauthorized access or penetration are present.

12 FEB 2009

12. Unauthorized copying, reproduction, or photographing of COMSEC material.

13. Deliberate falsification of COMSEC records.

14. Any other incident that may jeopardize the physical security of COMSEC material.

(10) Practices Dangerous to Security (PDS's). The PDS's listed below, while not reportable to the national level (NSA), are practices, which have the potential to jeopardize the security of COMSEC material, if allowed to perpetuate. Report all PDS's to the EKMS Manager immediately.

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

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

(c) Mailing of SF-153 forms with status dates annotated for material listed.

(d) Loss of a User or Master CIK.

(e) CIK failure.

(f) Failure of a STE terminal to re-key.

(g) Utilizing a STE terminal in the secure mode with a display failure.

(h) Failure to adequately secure or remove CIK from an unattended STE terminal. This is a COMSEC incident if the terminal is located in a space not approved for the open storage of material to the classification level of the installed key.

(i) COMSEC material not listed on account or local element local inventory documents.

(j) Late destruction of electronic COMSEC material.

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

12 FEB 2009

(l) Activation of the anti-tamper mechanism on, or unexplained zeroization of, COMSEC equipment, as long as no other indications of unauthorized access or penetration were present.

(m) Failure to maintain OTAR/OTAT logs.

(n) KP Specific non-reportable PDS's

1. Failure to perform a KP Changeover every 3 months.

2. Failure to perform a KP Rekey annually.

3. Failure to update KP CIK Pins every 6 months.

4. Failure to properly maintain KP CIK/PIN log.

(o) Loss or finding of unclassified material as defined in Article 1015 of reference (a).

(11) Reportable Practices Dangerous to Security (PDS's).
The following PDS's are reportable to the NSA and must be immediately reported to the EKMS Manager:

(a) Premature or out-of-sequence use of keying material before its effective date, as long as the material was not reused. If material prematurely used is reused without consent of the Controlling Authority it is a COMSEC incident.

(b) Inadvertent (i.e., early) destruction of COMSEC keying material, or destruction without authorization of the controlling authority (CA) as long as destruction was properly documented.

(c) Not completing and returning a Fixed Cycle (FC) inventory.

(d) Not completing a special or Combined Inventory when there is a change of Commanding Officer or change of EKMS Manager.

(e) Unauthorized adjustment of preconfigured default password parameters on the EKMS Local Management Device (LMD).

AirStaO 2250.1F
12 FEB 2009

(12) Entering Amendments and Corrections to COMSEC Publications. Amendments and corrections are permanent changes to COMSEC and COMSEC-related publications, which incorporate up-to-date information. All amendments to COMSEC publications will be referred to the EKMS Manager.

5. Administration and Logistics. The CG, 2d MAW and tenant organization Commanding Officers concur with the contents of this Order insofar as it pertains to members of their command.

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps Reserve.

b. Signal. This Order is effective the date signed.

A handwritten signature in black ink, appearing to read 'R. Clinton', with a large, sweeping flourish extending from the top left.

ROBERT D. CLINTON
By direction

DISTRIBUTION: A



UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
POSTAL SERVICE CENTER BOX 8003
CHERRY POINT, NORTH CAROLINA 28533-0003

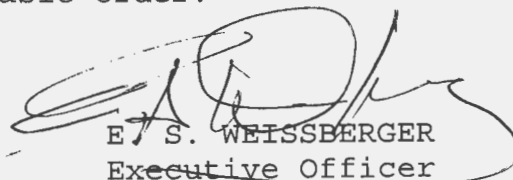
ASO 2250.1F Ch 1
TISD
11 MAY 2012

AIR STATION ORDER 2250.1F Ch 1

From: Commanding Officer, Marine Corps Air Station, Cherry Point
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR DISTRIBUTION AND CONTROL
OF THE ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS)

1. Situation. To direct pen changes to the basic Order.
2. Execution
 - a. On page 2, paragraph 4.a.(2)(c) change "annex J" to "Annex K".
 - b. On page 2, paragraph 4.a.(2)(d) change "KOV-14" to "KSV-21" and "Air Station Order 2280.1D." to "Air Station Order 2280.1E."
 - c. On page 3, paragraph 4.b.(2)(i) change "Annex L" to "Annex M".
 - d. On page 9, paragraph 4.c.(6)(a) replace the paragraph in its entirety with "A classified computer container information form, SF-700, is required for each lock combination. The top copy of the form must be placed on the inside of each COMSEC storage container."
 - e. On page 10, paragraph 4.c.(8)(b) change "Annex L" with "Annex M".
 - f. On page 10, paragraph 4.c.(8)(c) change "Annex L" with "Annex M" and "Air Station Order 5510.18B." with "Air Station Order 5510.18C."
3. Filing Instructions. File this Change page immediately behind the signature page of the basic Order.


E. S. WEISSBERGER
Executive Officer