



UNITED STATES MARINE CORPS
15TH MARINE EXPEDITIONARY UNIT
BOX 555365
CAMP PENDLETON, CALIFORNIA 92055-5365

MEUO 5500.1
SECMAN
17 AUG 2011

MARINE EXPEDITIONARY ORDER 5500.1

From: Commanding Officer
To: Distribution List

Subj: COMMAND SECURITY INSTRUCTION FOR THE 15TH MARINE EXPEDITIONARY
UNIT (MEU) INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)
STANDARD OPERATING PROCEDURE (SHORT TITLE: 15TH MEU IPSP SOP)

Ref: (a) SECNAV M5510.30
(b) SECNAV M5510.36
(c) MCO P5510.18A W/CH1
(d) IMEFO P5510.1D

Encl: (1) 15th MEU IPSP SOP

1. Situation. To provide policy and procedural guidance for the 15th MEU IPSP per the references. This Order supplements, but does not replicate the references.

2. Mission. This Order establishes the 15th MEU IPSP and provides guidance and procedures in order to ensure uniform implementation of the 15th MEU IPSP throughout the 15th MEU Command Element (CE) and Major Subordinate Elements (MSEs).

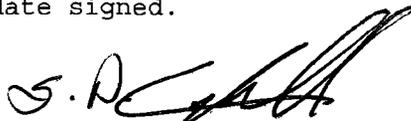
3. Execution. The 15th MEU CE and all MSEs shall comply with the policies and procedures outlined in enclosure (1). Any policies and procedures in conflict with this Order will be adjudicated by the 15th MEU Commanding Officer via the 15th MEU Security Manager.

4. Administration and Logistics. Requests for additional guidance and explanation, or recommendations concerning the contents of this Order, shall be addressed to the 15th MEU Security Manager or the Assistant Security Manager.

5. Command and Signal

a. This Order is applicable to all personnel assigned or attached to the 15th MEU. When the 15th MEU is formed as a Marine Air Ground Task Force (MAGTF), the 15th MEU Security Manager will exercise oversight of the MSEs' IPSPs. The actual administration for each MSE IPSP will be the responsibility of the given MSE Commander.

b. This Order is effective the date signed.


S. D. CAMPBELL

DISTRIBUTION: A

15TH MEU IPSP SOP

TABLE OF CONTENTS

| <u>IDENTIFICATION</u> | <u>TITLE</u> | <u>PAGE</u> |
|-----------------------|--|-------------|
| Chapter 1 | COMMAND SECURITY MANAGEMENT..... | 1-1 |
| 1. | Basic Policy..... | 1-1 |
| 2. | Security Manager..... | 1-1 |
| 3. | Assistant Security Manager..... | 1-2 |
| 4. | Section Security Representatives..... | 1-2 |
| 5. | Section Security Assistants..... | 1-3 |
| 6. | Security System Marines..... | 1-3 |
| 7. | Special Security Officer..... | 1-3 |
| 8. | Information Assurance Manager..... | 1-3 |
| 9. | Electronic Key Management System Manager..... | 1-3 |
| 10. | Classified Material Control Center Clerk..... | 1-4 |
| 11. | Top Secret Control Officer..... | 1-4 |
| | | |
| Chapter 2 | INFORMATION SECURITY PROGRAM..... | 2-1 |
| 1. | Basic Policy..... | 2-1 |
| 2. | Classification..... | 2-1 |
| 3. | Marking Classified..... | 2-1 |
| 4. | Challenging A Classification..... | 2-2 |
| 5. | Reproduction..... | 2-2 |
| 6. | Dissemination..... | 2-3 |
| 7. | Transmission and Transportation..... | 2-3 |
| 8. | Inventories..... | 2-3 |
| 9. | Storage and Destruction..... | 2-6 |
| 10. | Inspections..... | 2-7 |
| 11. | Loss or Compromise of Classified..... | 2-7 |
| 12. | Prohibited Digital Devices..... | 2-8 |
| 13. | Security Violations..... | 2-8 |
| 14. | Release to Foreign Nationals..... | 2-8 |
| 15. | Pre-Publication Review..... | 2-8 |
| 16. | Mail Procedures..... | 2-9 |
| | | |
| Figure 2-1 | Sample of Tamper Seal..... | 2-2 |
| | | |
| Chapter 3 | PERSONNEL SECURITY PROGRAM..... | 3-1 |
| 1. | Basic Policy..... | 3-1 |
| 2. | Access to Classified Information..... | 3-1 |
| 3. | Joint Personnel Adjudication System..... | 3-2 |
| 4. | Personnel Security Investigation (PSI) | 3-2 |
| 5. | Periodic Reinvestigation (PR) | 3-3 |
| 6. | Administrative Withdrawal of Access..... | 3-3 |
| 7. | Suspension of Access for Cause..... | 3-3 |
| 8. | Continuous Evaluation of Eligibility for Access..... | 3-4 |
| 9. | Reporting..... | 3-4 |
| 10. | Debriefing..... | 3-5 |

| <u>IDENTIFICATION</u> | <u>TITLE</u> | <u>PAGE</u> |
|-----------------------|--|-------------|
| Chapter 4 | SECURITY EDUCATION..... | 4-1 |
| 1. | Basic Policy..... | 4-1 |
| 2. | Briefings..... | 4-1 |
| 3. | On-The-Job Training (OJT)..... | 4-2 |
| 4. | Security Awareness Program..... | 4-2 |
| Chapter 5 | EMERGENCY ACTION PLAN..... | 5-1 |
| 1. | Basic Policy..... | 5-1 |
| 2. | Action..... | 5-1 |
| 3. | Concept..... | 5-1 |
| 4. | Escalation Measures..... | 5-1 |
| 5. | Authorization to Implement Plan..... | 5-2 |
| 6. | Execution of Emergency Destruction..... | 5-2 |
| 7. | 15th MEU Headquarters Aboard Camp Pendleton..... | 5-2 |
| 8. | Transfer of Classified Material..... | 5-3 |
| Chapter 6 | CLASSIFIED MATERIAL CONTROL CENTER (CMCC) SOP..... | 5-1 |
| 1. | General Guidance..... | 6-1 |
| 2. | Custodian Requirements..... | 6-2 |
| 3. | Physical Security Measures..... | 6-3 |
| 4. | Secondary Control Points..... | 6-5 |
| Figure 6-1 | Sample Format for Open Safe Instructions..... | 6-3 |
| Figure 6-2 | Sample of Open/Close Sign..... | 6-4 |
| Figure 6-3 | Sample of 15th MEU Inventory List..... | 6-6 |

Chapter 1

Command Security Management

1. Basic Policy

a. The IPSP management consists of the designation of officials responsible for ensuring compliance with and implementation of the IPSP for the 15th MEU CO. This program establishes a system of oversight and education to ensure effective control and security of classified information.

b. The 15th MEU CE and MSEs must have at a minimum the following:

(1) Security personnel designated in writing. At the very least, each element will have a command Security Manager, Assistant Security Manager, Section Security Representatives, System Security Marines, and Security System Computers.

(2) Written command security procedures and education plan.

(3) Prepared Emergency Action Plan (EAP) for the protection of classified material.

(4) Provisions for inspection and review of their IPSP within their command and subordinate elements.

2. Security Manager

a. The 15th MEU Executive Officer (XO) is the designated Security Manager for the 15th MEU. All MSEs are required to designate a Security Manager in writing for their commands. MSE Security Managers must be an officer who meets the requirements outlined in reference (d) and attend an authorized Security Manager Course. The CE and MSE Security Managers need to be designated by name and clearly identified to all members of the organization in organizational charts, telephone listings, and rosters.

b. The Command Security Manager will be responsible for the following:

(1) Serve as the principal advisor concerning information and personnel security matters to the Commanding Officer.

(2) The written development and oversight of the Command IPSP.

(3) Formulating and coordinating the command's annual security awareness and education program.

(4) The submission and receipt of visit certifications to and from other commands, agencies and organizations.

(5) Ensuring all personnel who possess access to classified or who wish to submit clearance packages have the appropriate need-to-know and qualifications.

(6) Maintaining liaison with the I MEF Special Security Office (SSO) concerning sensitive compartmented information (SCI) and procedures.

Enclosure (1)

(7) Executing the continuous evaluation of personnel eligibility for access to classified information and maintain record of all those who possess a clearance and level of clearance granted.

(8) Ensuring all personnel sign a SF-312, Non-Disclosure Agreement (NDA), prior to granting access and that a copy is retained on file for 2 years. This includes ensuring that all personnel departing the command re-read and sign the back of their original NDA.

(9) Retaining a record of all security appointments within the command.

(10) Performing site assist visits, inspections and reviews for subordinate commands/elements.

(11) All action concerning all security violation reports and compromises within the command.

(12) Coordinating with the information assurance manager on common security concerns.

3. Assistant Security Manager. The 15th MEU Intelligence Officer is the MEU Assistant Security Manager (ASM). The ASM acts in the absence of the Security Manager and conducts all the daily duties for the Security Manager. When the MEU is deployed, MSEs having elements located on separate vessels will designate ASMs with specific duties assigned. The MEU ASM will also be the 15th MEU Classified Material Control Center (CMCC) Officer.

4. Section Security Representatives (SSRs)

a. Each staff section will assign the section Alpha (or Primary if desired) as the primary SSR for their section. The section SNCOIC will be assigned as the Alternate SSR (ASSR). SSRs are responsible for their section's compliance to this policy in full.

b. The SSRs and ASSRs will at a minimum:

(1) Maintain communication with the Security Manager and ASM to keep up on security related matters that are relevant to the section and the command as a whole.

(2) Report all security related concerns and violations they identify both within their section and other sections to the Security Manager and ASM immediately.

(3) Maintain a system of accountability in accordance with MEU's policy for all classified material in the section's possession that has been identified as accountable. SSRs must be the final signature on all monthly Classified Material Control Center (CMCC) items inventory sheets.

5. Section Security Assistances. A section may designate Section Security Assistants (SSAs) if desired. These assignments do not relieve the responsibility of the Section's SSR or the Security Manager. For the purpose of this Order, the term "Section Security Assistants" refers to security clerks, acting in accordance with 15th MEU Security policies. Security clerks may be assigned as SSAs, regardless of rank, as long as they have a

Enclosure (1)

clearance commensurate with the highest classification of the material handled.

6. Security System Marines. Security System Marines (SSMs) are those Marines that are designated in writing that are authorized to move data to classified removable media. Each MEU section will identify no more than two Marines and two computers (that only those two Marines may access) to be authorized to move data to classified removable media. Those computers that are capable to move data to and from removable media are referred to as Security System Computers and must be inventoried and tracked by their serial numbers monthly.

7. Special Security Officer. All Special Security Officer (SSO) functions are provided by the I MEF SSO while in garrison. Similarly, when embarked aboard ship, the Amphibious Squadron (PHIBRON) provides the SSO. While deployed, the 15th MEU S-2 will coordinate with I MEF SSO and perform SSO-like actions.

8. Information Assurance Manager. The 15th MEU Information Assurance Manager (IAM) will be a Marine within the S-6, and will serve as the IAM for the CE and MSEs when they are formally attached to the MEU. The IAM is responsible for Information Systems Security and technical advice concerning protection of information produced on an automated system. The IAM is responsible for publishing Automated Data Processing (ADP) security procedures, guidance, and restrictions. The IAM also will serve as the 15th MEU Information Systems Security Officer and be responsible for the implementing network security requirements for 15th MEU's Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) systems. All 15th MEU elements will appoint an Information Assurance Manager in writing.

9. Electronic Key Management System Manager. The Commanding Officer shall appoint in writing an Electronic Key Management System (EKMS) Manager who shall serve as the principal advisor in all matters regarding EKMS. Each MSE will appoint in writing a Communication Security (COMSEC) custodian. The MEU EKMS Manager will be responsible for writing the MEU EKMS SOP (Local Handling Instructions).

10. Classified Material Control Center Clerk. The 15th MEU Classified Material Control Center (CMCC) will be run by the MEU S-2. The S-2 will assign a CMCC Clerk to assist in the operations of the CMCC. 15th MEU MSEs will be responsible for the administration of their own CMCC, but they must comply with this order and the inspection and review requirements the CMCC responsibilities for inventories and reviews are stated below.

11. Top Secret Control Officer. The 15th MEU Commanding Officer will appoint, in writing a Top Secret Control Officer (TSCO) to manage the command's Top Secret Control Program. Within this command the TSCO will ensure that all Top Secret materials are accounted for annually and perform all obligations of a TSCO as outlined in the I MEF IPSP Order. The 15th MEU TSCO will be a Marine within the S-2 Section.

Enclosure (1)

Chapter 2

Information Security Program

1. Basic Policy. The 15th MEU Information Security Program (ISP) establishes a system of oversight and monitoring to ensure effective control and security of classified information. The ISP for each section/unit/element shall, at a minimum, include the following:

a. An understanding of Classified Material Control Center (CMCC) procedures and responsibilities (see Chapter 6 for specific MEU CMCC SOP), including the inventory and review requirements;

b. An understanding of the how to handle and protect classified information;

c. Provisions for inspection and review of their IPSP within their command and subordinate elements; and

d. An understanding of visitor control procedures: When the MEU CE or MSEs host classified briefs, meetings, conferences, or visitors within their respective areas, the hosting section or element will take full responsibility to ensure that the location is being adequately safeguarded to prevent unauthorized personnel from entering, and that all attendee's possess the appropriate level of access.

2. Classification. The unnecessary classification of or higher than required classification of material should be avoided. If there is a reasonable doubt about the need to classify or the level of classification, safeguard it and consult the MEU Security Manager.

3. Marking Classified. All MEU classified documents require page markings, subject line markings, portion markings, document date, derived from line, and declassification instructions.

a. The use of stamps or the appropriate sticker labels (SFs 706, 707, 708, 709, 710, and 712) are required for the marking of information technology (IT) systems and storage which includes classified hard disk drives (HDDs). This is to ensure the equipment is not improperly handled or mistaken as classified. Unmarked items will be confiscated and returned after the item has been properly labeled.

b. Tamper Seals will be used to assist in the management of classified HDD's and are under the strict control of the MEU S-2. See Figure 2-1 for an example of the 15th MEU tamper seal (prior to tampering or compromise).

(1) Tamper seals are mandatory on all MEU external classified HDD's. The tamper seals are placed on external HDD's to assist in determining whether or not an external HDD has been inventoried.

(2) External HDD's intended for classified use shall be brought to the MEU CMCC Clerk prior to use for proper marking and accountability. Any classified external HDD's found without the tamper seal will be confiscated, and will be returned after the HDD has been inventoried and properly labeled.

c. MEU personnel will use coversheets to prevent inadvertent disclosure. Coversheets will at least be placed on the top of a classified document, in

Enclosure (1)

order to clearly display the classification of the paper product inside. Coversheets can also be stapled to folders or attached to binders.

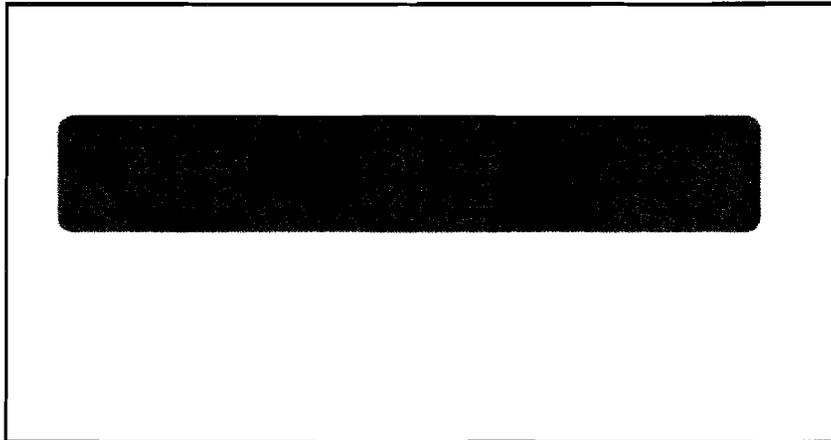


Figure 2-1.--Sample of Tamper Seal

4. Challenging a Classification

a. A challenge may request for a product to either be reclassified to a lower level or considered for full declassification.

b. All challenges will be submitted via the MEU Security Manager to ensure proper format and mailing. Every challenge must be submitted with sufficient justification for the material to be considered for either reclassification or declassification. All challenges must include a copy of the product that requires review.

c. Note that challenging a classification is not the same as simply requesting a tearline from an originator, or sanitizing a document by removing all classified information.

5. Reproduction

a. The MEU reproduction of all classified material shall be kept to a minimal and excess destroyed immediately. Classified material may only be reproduced on a device that has been accredited for that level of classification or higher.

b. Reproduction devices with imbedded hard drives that do not have volatile Random Access Memory (RAM) must reside in an open storage workspace.

c. Only 15th MEU printers with volatile RAM can be connected to classified networks or terminals in a closed storage facility or workspace, and must be turned off at the end of each working day, which must be captured as part of the Activity Security Checklist (SF-701).

d. Some documents and products have special controls placed on the information that either limit or prevent the reproduction of the document. Disregarding the special controls placed on such products is a security violation and must be reported immediately to the Security Manager for investigation.

6. Dissemination

a. In accordance with reference (b) the following dissemination requirements must be followed:

b. Top Secret information originated within the Department of Defense (DoD) shall not be disseminated outside the DoD without the consent of the originator or higher authority.

c. Unless specifically prohibited by the originator, Secret and Confidential information originated within the DoD may be disseminated to other DoD components and agencies within the executive branch of the U.S. Government.

d. In emergency situations, in which there is an imminent threat to life or in defense of the homeland, the Secretary of the Navy or a designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access.

7. Transmission and Transportation

a. When it is necessary to transmit or transport classified material there are specific procedures that must be followed to prevent the inadvertent disclosure, compromise or loss.

b. All MEU personnel will use the authorized DoD computerized network to send and receive classified information whenever possible.

c. Defense Courier Service (DCS) is a DoD funded program that is cleared to courier material as sensitive as Sensitive Compartmented Information (SCI) Material. Normally, it is only to be used for Top Secret and SCI material but may be utilized for transporting Secret material in situations where no other means is available or trusted.

d. Registered Mail is authorized only for material as high as Secret and can be utilized anywhere within the United States. Authorized outside the U.S. when the article is addressed to U.S. government agencies through U.S. Army, Navy, Air Force, and Marine Corps controlled USPS facilities.

e. Commercial Carrier - The Information Security Oversight Office (ISOO) has approved use of all the small package domestic express Blanket Purchase Agreements (BPA) carriers for overnight domestic express delivery of Secret classified shipments.

f. If there's a absolute need to hand carry classified information, an authorized MEU courier may be used. This method of transportation will only be approved when no other method is available. The MEU Security Manager and/or Assistant Security Manager (ASM) have the authority to issue courier cards and letters to personnel who have the need to physically transport classified material.

(1) All couriers must be approved, certified, and given a command courier brief prior to transporting classified material. This process includes signing a courier statement of understanding provided by the 15th MEU S-2.

Enclosure (1)

(2) Couriers are responsible when transporting classified material to ensure that upon arrival of their intended destination arrangements are in place to store classified material in an appropriate military, government, or government approved contractor facility. Under no circumstances is classified material to be stored unattended in a vehicle, hotel room, or hotel safe.

(3) Individuals found transporting classified materials or directing others to transport classified materials that have not been appropriately designated to do so will be found in violation of SECNAV M-5510.36 and will be reported and investigated. Temporary loss or full revocation of clearance may occur as a result of this security violation.

8. Inventories

a. All Top Secret information (including copies) originated or received by the MEU shall be continuously accounted for, individually serialized, and entered into the command Top Secret log, held by the MEU TSCO. The log will completely identify the information, and at a minimum include the date originated or received, individual serial numbers, copy number, title, originator, initial page count, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified, etc.) and date of each disposition action taken.

(1) Top Secret logs shall be retained for five (5) years.

(2) The MEU TSCO will obtain a record of receipt (typically a classified material receipt) from each recipient for Top Secret information distributed internally and externally.

(3) Top Secret information shall be physically sighted or accounted for at least annually or more frequently if circumstances warrant.

b. Inventories of the MEU and MSE CMCCs will be conducted at a minimum, at the following periodicity:

(1) Monthly. During the first seven (7) days of the month each MEU Section will conduct a by-line visual inspection of all CMCC items. The SSR will be ultimately responsible for ensuring their section conducted a proper inventory and review, and will be the final signature on all monthly CMCC inventory sheets.

(2) Quarterly. During the last week of every third month each MEU Section will conduct a by-line visual inspection of all CMCC items in the presence of the S-2 CMCC Clerk. The SSR and the CMCC Clerk will be responsible for ensuring a proper inventory and review is conducted, and both will sign the monthly CMCC inventory sheets.

(3) Anytime a compromise, suspected loss of classified material, or other potential lapse in security occurs, the Security Manager and Assistant Security Manager must be notified. The Security Manager will decide whether an immediate inventory is required.

(4) As directed by the 15th MEU Commander, the MEU Security Manager, MSE Commander, MSE Security Manager, or when directed by higher authority.

Enclosure (1)

c. Equipment in use or temporarily loaned will not be accepted as justification for not completing an audit within the month the audit is due. Sections/MSEs are directed to keep written record when classified equipment is temporarily loaned out of their custody for various reasons to include, but not limited to, training and repair. The written record may be used as proof of existence for one inventory period without the requirement to physically site the device. Beyond one inventory period, the classified gear needs to be physically sited at its temporary location until returned to the section.

d. If classified equipment transfers custody permanently between two sections or organizations then the Classified Material Transfer Custody (appendix C) shall be used, and a copy needs to be provided to the CMCC and retained by all parties.

e. All monthly and quarterly inventories and reviews will be done using the 15th MEU inventory sheets (appendix D). All inventory reports will be validated and signed by the SSR.

f. Extensions may be granted but must be submitted to and approved by the Security Manager. Extensions will not be approved beyond the month the audit is due.

g. Inventories of EKMS accounts will be in accordance with the MEU EKMS SOP (Local Handling Instructions). MSE Commanding Officers are reminded of their responsibilities for monthly reviews.

h. Inventory discrepancies. If it is discovered that there is a discrepancy with the report, it shall be reported immediately to the CMCC Clerk and ASM.

i. Sections that have new classified HDD's to report/inventory shall use appendix D and provide it to the CMCC Clerk and ASM before the equipment is put into use.

j. Secret and Confidential "working papers" such as classified notes from a training course or conference, research notes, rough drafts, and similar items that contain Secret or Confidential information are considered working papers.

(1) The following actions shall be taken with all working papers:

(a) Clearly mark the classification in the center location at the top and bottom of each page with the highest overall classification level of any information they contain along with the words "Working Paper" on the top left of the first page in letters larger than the text.

(b) Dated when created.

(c) Protected per the assigned classification level.

(d) Destroyed, by authorized means, when no longer needed.

(2) All working papers retained for more than 180 days from the date of creation, officially released outside the MEU, or transmitted over a classified IT system is considered a finished document and will need to be marked according to Chapter 3, Paragraph 3 of this Order.

Enclosure (1)

9. Storage and Destruction

a. All MEU classified information will be stored in an appropriate General Services Administration (GSA) approved security container, vault, or modular vault. Classified material that is no longer required shall be destroyed in order to minimize classified holdings and to protect the national security.

b. The S-2 GSA approved security containers will be the MEU CMCC.

c. Secondary Control Points (SCP) are an extension of the CMCC within each Staff Section and will be used by the SSRs to store their classified material. SSRs are responsible for the inventory, accounting, and management of their respective sections classified being held within their SCP.

d. All 15th MEU secure rooms, vaults, and safes require a Security Container Check Sheet (SF-702).

e. Under field conditions, during military operations, the MEU CO may require or impose security measures deemed adequate to meet the storage requirements commensurate to the level of classification used.

f. Combinations to GSA approved security locks in use will be changed whenever anyone who knows the combination leaves the command, no longer requires access, or whose clearance has been revoked or denied. Combinations also can and should be changed frequently, as a good security practice. Combinations shall be recorded and retained by the 15th MEU EKMS Manager using a SF-700, with a copy affixed inside each security container.

(1) The Principle or Staff Section utilizing the locks shall provide updated SF-700 forms to the EKMS Manager.

(2) Whenever a combination is changed, a new SF-700 must be created and secured in accordance with this Order and the old one destroyed.

g. Destruction. Some forms of classified cannot be destroyed within the command due to equipment limitations. In these instances the equipment will be sent outside of the MEU via the CMCC for destruction. Per reference (d), The Classified Material Transfer of Custody form shall be used to list the equipment to be relinquished. A copy of the form shall be placed in a section specific binder retained by the CMCC.

(1) Shredding Policy - All 15th MEU papers (CLASSIFIED and UNCLASSIFIED) will be shredded vice being thrown in trash cans. All classified must use approved cross-cut shredders.

(2) Top Secret: Records for the destruction of Top Secret material is required for no less than five (5) years, per reference (b).

(3) Secret: There is no requirement to record the destruction of Secret classified products in accordance with DoD regulations and reference (b).

(4) The MEU CMCC will keep record of all classified material mailed out for the purpose of destruction for a period of no less than two (2) years in accordance with reference (b).

Enclosure (1)

(5) Burning method of destruction will only be used under extreme or combat conditions, when there are no other methods available, and the retention of the excess classified material poses a threat to operations and the national security.

(6) Upon the return from each deployment the MEU will perform a review of all classified holdings to identify what classified material is no longer required and have it destroyed or considered for historical archiving.

(a) MEU wide reviews will be executed at the discretion of the MEU CO, and a Letter of Instruction for "clean-out" days will be provided by the MEU Security Manager (ref: SECNAV M-5510.36, 10-17).

(b) Any section within the command has the authority to perform a security review of their classified holdings as often as they see fit. Frequent reviews of classified holdings independent of required reviews are strongly encouraged.

10. Inspections

a. Each MSE Commanding Officer and Security Manager shall initiate inspection programs to ensure compliance with their respective IPSPs. A basic inspection checklist for a command security program can be obtained from the 15th MEU S-2.

b. The CE and each MSE will be inspected formally and unannounced by the 15th MEU Security Manager periodically to ensure compliance with this Order. Inspections will cover overall management, accounting and control of classified material, physical security of classified information, personnel security, and security education.

c. Vacated Command Post Inspections. Vacated Command Post Inspections (VCPI) are normally conducted by counterintelligence (CI) personnel (when attached and available). Additionally, inspections will be conducted in the field after exercises, on ship prior to turnover of spaces, and after any location where classified material was routinely used. When CI personnel are not available, these inspections are the responsibility of the senior Marine present of the unit vacating a position or ship space.

d. Daily inspections will be conducted by the 15th MEU Command Duty Officer (CDO) at the close of the business day. The CDO will ensure there is no left out classified material and check all security locks, and initial all SF-701 and SF-702 forms.

11. Loss or Compromise of Classified

a. If it becomes evident that classified information may have been lost or compromised it shall be reported to the MEU CO, Security Manager, and the ASM.

b. No more than 24 hours should pass from the moment it is believed that there has been a loss or compromise and the reporting of the event.

c. Preliminary. A Preliminary Inquiry (PI) must be completed within 72 hours of the incident being reported.

Enclosure (1)

b. Manual of the Judge Advocate General (JAGMAN) Investigation. When loss or compromise of information cannot be ruled out or determined remote as the result of a PI the MEU CO may decide to initiate a JAGMAN investigation.

c. A copy of all PI's and JAGMAN investigations will be provided to and retained by the MEU Security Manager. These investigation reports are a part of general inspections of the command security program and shall be used as a guide to determine common security problems that must be addressed through the command security education program and command security program.

12. Prohibited Digital Devices. Due to the threat that certain digital devices represent to national security the following devices are prohibited from MEU workspaces:

- a. Personal computers;
- b. All types of flash media (i.e. thumb-drives, and secure digital (SD) cards);
- c. Personal Cameras and video recorders;
- d. Audio recorders; and
- e. Cellular devices are prohibited from conferences, meetings, and training sessions where classified material will be discussed.

13. Security Violations

a. A security violation is any action that intentionally or unintentionally places classified material in a position to be lost or compromised, and should be reported immediately.

b. If it is discovered that someone was aware of a security violation, even though they may not have committed the violation, and did not report the incident, they too can be held responsible for their lack of judgment and failure to report the violation.

c. Security violations do not necessarily warrant the loss of clearance.

14. Release to Foreign Nationals. Only that material which has been approved for release to a specific foreign government may be released. The approval is evident in the classification marking //REL OR //REL TO followed by the tri-graph that represents the appropriate country.

15. Pre-Publication Review

a. A security and policy review will be performed on all 15th MEU information intended for public release including information intended for placement on publicly accessible websites or computer servers (i.e. Facebook, YouTube, etc.).

b. The MEU CO is authorized to release information to the public that is wholly within the command mission and scope. The CO is responsible for ensuring that a review of material proposed for public release is completed. This responsibility is normally delegated to the Public Affairs Officer. The security review is part of the overall public release process and needs to be

Enclosure (1)

coordinated with the MEU Security Manager in consultation with command subject matter experts.

c. If public release cannot be authorized within the Command, the material must be submitted for further review via the chain-of-command.

16. Mail Procedures. The 15th MEU have the following procedures to ensure items are properly cared for. The MEU mail clerk does not receive USPS First Class or Certified mail. All registered mail that has not been delivered to the appropriate section or person by the end of the work day will be returned to the Del Mar Post Office before close of business.

Chapter 3

Personnel Security Program

1. Basic Policy

a. The MEU Security Manager is responsible for developing and administering the MEU Personnel Security Program (PSP).

b. The MEU ASM however, will perform the daily duties and oversee the daily functioning of the PSP.

c. No 15th MEU person shall be given access to classified information or be assigned to sensitive duties unless a Personnel Security Investigation (PSI) is conducted.

2. Access to Classified Information

a. Access to classified information will be granted only if allowing access will promote the furtherance of the MEU's mission while preserving national security. No one has the right to access classified information solely because of rank, position, or security clearance. The CE and MSEs must show discretion before granting access and establish a need-to-know (defined as, sufficient need to access classified information to accomplish command mission and operational objectives).

b. Access eligibility for any level will be verified by the MEU S-2 using the Joint Personnel Adjudication System (JPAS). Access eligibility does not automatically mean there is a need-to-know, which is an absolute requirement before full access/disclosure.

c. Access rosters shall be placed on vaults and secure rooms to identify which MEU personnel have unlimited access to the space and have been entrusted with the combination and/or keys to the locks protecting the space.

(1) 15th MEU access rosters shall identify MEU personnel by rank, first name, last name, and the last four of the individual's social security number.

(2) MEU access rosters must be updated when an individual listed no longer requires access to that specific space.

d. Temporary access

(1) In the absence of adverse information, the MEU CO or XO may grant temporary access (also referred to as an interim clearance) to individuals pending completion of full investigative requirements and pending establishment of security clearance eligibility by the Department of Navy Central Adjudication Facility (DoNCAF).

(2) Personnel assigned to cryptographic duties must have the appropriate security clearance eligibility established prior to accessing U.S. cryptographic information. Interim security clearances are not valid for access to U.S. cryptographic information.

Enclosure (1)

e. Access to classified information will be formally terminated when it is no longer required in the performance of assigned duties and/or when the individual's security clearance eligibility is denied or revoked.

3. Joint Personnel Adjudication System

a. The Joint Personnel Adjudication System (JPAS) is the automated system of record for personnel security management within the Department of Defense, providing a means to record and document personnel security actions.

b. The day-to-day management of the MEU JPAS account will be conducted by the MEU S-2. A JPAS account is identified by a Security Management Office (SMO) code. The 15th MEU SMO code is 203106.

c. All visitors to the MEU that require access to classified information must first be checked in JPAS. Any 15th MEU personnel visiting other commands that need access to classified information must submit a visitor request via JPAS.

4. Personnel Security Investigations (PSI)

a. MSE Commanders and MEU Staff Sections' Officer-in-Charge (OIC) should carefully screen their personnel to determine eligibility and requirements prior to requesting a PSI.

b. The MEU Security Manager via the MEU S-2 will be the only office of the Command Element that is authorized to screen applicants and process security investigations.

c. Requesting and Screening Requirements. Staff Section leadership (OIC, Alpha, or Staff Non-Commissioned Officer In-Charge) or MSE Commanders or their Security Managers are the only officials authorized to request PSIs on individuals within their section/element. The following must be accomplished by all MEU permanent and temporarily assigned personnel when requesting a PSI/access.

(1) PSIs and Periodic Reinvestigations (PR) will not be requested for any MEU personnel who will be retired, resigned, or separated with less than 1 year service remaining.

(2) The scope of the PSI requested will be commensurate with the level of sensitivity of the access required or position occupied as part of the 15th MEU. Only the minimum investigation to satisfy a requirement will be requested.

(3) Request for Access Form: A local form provided by the MEU S-2 will be used to validate an individual's access requirement/need-to-know (appendix E). This form requires the signature of an Officer or Senior Staff Noncommissioned Officer in authority over the individual. Personnel that require Top Secret access or higher require the signature of the MEU CO or XO, or their MSE CO.

(4) All requests for access to SCI will be validated and approved by the I MEF SSO via the MEU S-2.

(5) Screening Questionnaire: Personnel shall fill out a screening questionnaire (appendix F) provided by the S-2. The questionnaire is used to

Enclosure (1)

assist the Security Manager to identify any derogatory information that may prevent the granting of temporary access, information reportable to the DoNCAF in accordance with reference (a) that has not previously been reported, and identify information that must be listed in a security investigation.

(6) Each individual approved for submission of a PSI will forward their completed SF-86, *Questionnaire for National Security Positions*, to the MEU S-2 via Electronic Questionnaires for Investigations Processing (e-QIP) for validation and processing.

5. Periodic Reinvestigation

a. Periodic Reinvestigations (PR) are submitted to update a previous investigation. The PR due date is based on the closed investigation date of the previous investigation.

b. Periodic Reinvestigations will not be initiated until 90 days from expiration date of previous investigation.

c. Periodic Reinvestigations are not required for personnel who intend to retire or end active service (EAS) within six (6) months of the expiration date of their current investigation.

d. MEU personnel that no longer need access or no longer need access to a certain level (i.e. a person cleared for SCI who now only needs a SECRET clearance) will not be put in for a PR.

e. Personnel whose clearance will expire during a deployment are exempt from submitting a new PR until returning from their deployment.

f. The MEU S-2 will make every attempt to routinely contact personnel who qualify for the submission of a PR and those that are past due. At a minimum the MEU S-2 will contact personnel needing a PR monthly. However, the individual is ultimately responsible for the submission of their PR. PR due dates can be obtained from the MEU S-2.

g. Failure to submit a PR in a timely fashion is grounds for suspension of access to classified information. Anything exceeding 6 months will be considered as excessive. If access is suspended the submission of a PR will be required before access can be reinstated.

6. Administrative Withdrawal of Access

a. Security access will be administratively withdrawn upon transfer from the 15th MEU or when access is no longer required.

b. The individual will be debriefed by the MEU S-2.

c. Access will be rescinded via JPAS due to Permanent Change of Station (PCS), EAS, and/or discharge of military service.

7. Suspension of Access for Cause. The MEU will suspend access for questionable or unfavorable information. This temporary measure cannot be changed once it is submitted in JPAS. The MEU will:

Enclosure (1)

a. Notify the individual in writing of suspension, to include a brief statement of reasons for action.

b. Report to DoNCAF no later than ten (10) working days from date of suspension. This will be done via JPAS/JCAVS - open "report incident" link and check box to "suspend" access, and will include specific reasons for suspension - any supporting documentation will be sent separately.

c. Remove individual's name from all access rosters and visit certifications.

d. Notify all coworkers of suspension.

e. Change combinations to which individual had access.

f. Cancel or hold in abeyance PCS orders.

8. Continuous Evaluation of Eligibility for Access. The following procedures are to be used to help conduct the continuous evaluation of eligibility of 15th MEU personnel:

a. The MEU Security Manager will review all legal, medical, or Substance Abuse Counseling Officer (SACO) reports as they pertain to MEU personnel with access or clearances. If warranted, access may be suspended and the adverse or derogatory information reported to DoNCAF via JPAS, with the 15th MEU Commanding Officer's recommended action.

b. Additionally, the command will periodically review the security access rosters for accuracy.

c. DoNCAF may report the discovery of adverse, derogatory, borderline, or questionable information to the MEU. The MEU will respond as follows:

(1) The information will be reviewed with the section head for facts relevant to the incident and the person's continuing eligibility for access.

(2) The Security Manager will then make a recommendation to the 15th MEU CO regarding the individual's eligibility for access.

(3) If required, the 15th MEU Security Manager will respond to DoNCAF, with the 15th MEU Commander's recommendation, for adjudication.

9. Reporting

a. All personnel have responsibility to report any information to the Security Manager that may have a bearing on a person's eligibility for access. In particular, the following requires reporting:

b. Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the U.S. by unconstitutional means.

c. Foreign influence concerns/close personal association with foreign nationals or nations.

d. Foreign citizenship (dual citizenship) or foreign monetary interests.

Enclosure (1)

e. Sexual behavior that is criminal or reflects a lack of judgment or discretion.

f. Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations or unwillingness to cooperate with security clearance processing.

g. Unexplained affluence or excessive indebtedness.

h. Alcohol abuse.

i. Illegal or improper drug use/involvement.

j. Apparent mental, emotional or personality disorder(s).

k. Criminal conduct.

l. Noncompliance with security requirements.

m. Engagement in outside activities, which could cause a conflict of interest.

n. Misuse of Information Technology Systems.

o. Suicide or attempted suicide.

p. Death or desertion.

10. Debriefing. All 15th MEU personnel who have had access to classified information and no longer need access for any reason will be debriefed by the MEU S-2. The MEU S-2 will coordinate debriefs by the MEF SSO for those personnel who have Top Secret/Sensitive Compartmented Information (TS/SCI) and Special Category (SPECAT) accesses. Once detached, the MEU S-2 will ensure these personnel are dropped from the command in JPAS.

Chapter 4

Security Education

1. Basic Policy. The Security Manager will establish and maintain an active security education program to instruct all personnel, regardless of rank or position, in security policies and procedures. The goal of the program is to develop fundamental habits of security to the point that proper discharge of duties and security of classified information becomes a natural element of every task.

2. Briefing. The 15th MEU and MSE security education programs will consist of training to accomplish at least the following requirements:

a. Orientation Security Briefings: All personnel joining the MEU will receive an Orientation Security Brief upon checking-in; CE personnel will receive the brief from the MEU S-2. Upon completion, they will sign a statement certifying that they have received the brief. The brief will cover at minimum:

- (1) Importance of security and need to safeguard information.
- (2) MEU security structure.
- (3) MEU security procedures for storage, transmission, destruction.
- (4) Access Requirements.
- (5) MEU classified information control procedures/measures.
- (6) Activities which could impact security clearance eligibility.
- (7) Reporting suspected security violations.

b. Annual Refresher Briefs: All MEU personnel with a clearance of any kind are required to attend an annual refresher brief. The brief at minimum will cover:

- (1) Importance of security and need to safeguard information.
- (2) Changes in security policies/situations.
- (3) MEU security structure.
- (4) MEU security procedures for storage, transmission, destruction.
- (5) Any recent security issues/incidents.

c. Counterintelligence (CI) Briefings: All MEU personnel who hold a Secret or higher security clearance are required to receive an annual CI Brief.

d. Specific Access Briefings: These briefs will only be given to those MEU personnel who need access to specific programs (e.g. North Atlantic Treaty Organization (NATO), SCI, etc.). The required access will determine who will be giving the brief (i.e. the MEU S-2 or the MEF SSO).

Enclosure (1)

e. Special Briefings: To familiarize personnel with security requirements of a specific assignment, such as CMCC Clerk, SSR duties, etc. These briefs are conditional upon assignment to specific duties, billets, and tasks. These briefs will be tailored to individual needs.

3. On-The-Job Training (OJT). It is the responsibility of each Supervisor to ensure all of their personnel get the appropriate OJT to accomplish all security tasks/duties being assigned. If any Supervisor needs help in training their personnel or wants to receive additional security training they need to contact the 15th MEU S-2 for assistance.

4. Security Awareness Program. The 15th MEU CE, and its MSEs, will initiate a Security Awareness Program. Security enhancement is a continuing program and personnel should be frequently exposed to current information. Programs will include, at a minimum:

- a. Signs and posters in or near areas where classified material is used.
- b. Posting advisories near reproduction machines that specify the classification level that each machine may be used for reproducing.
- c. Posting advisories emails, and command wide notices on security matters as a friendly reminder to bring security to the forefront.

Chapter 5

Emergency Action Plan

1. Basic Policy

a. The 15th MEU Emergency Action Plan (EAP) establishes the course of action to be taken in the event of an emergency situation where classified material may be at risk of loss or compromise.

b. This EAP will focus on natural disasters or manmade emergencies while stationed at Camp Pendleton (i.e. fire, flood, tornado, or earthquake, etc.).

c. When the MEU is deployed on Navy vessels, the CE and MSEs will need to integrate all EAPs with the Amphibious Ready Group (ARG) EAPs.

d. When the MEU is ashore, the Security Manager and EKMS Manager will need to reassess their plans to ensure they are updated as the situation dictates (ref: the EKMS SOP for further EKMS instructions).

2. Action. The 15th MEU Security Manager and MSE Security Managers are responsible for the effective execution of the EAP. They will be assisted in the execution of the EAP by the Assistant Security Manager, the CMCC Officer/Clerk, the 15th MEU CDO, and the section SSRs and ASSRs in order to prevent the loss or compromise of classified materials.

3. Concept

a. Safety of MEU personnel is paramount and security considerations secondary. Individuals tasked with carrying out this plan will not sacrifice their own safety or the safety of others in the execution of this plan.

b. Risk assessments will be conducted by each Security Manager to determine the types of emergencies that are likely to arise which would require the implementation of the EAP.

(1) All natural disaster emergency action plans are directed toward maintaining security and control over classified materials until the emergency has passed, or moving materials to a less vulnerable area.

(2) Hostile or terrorist action EAPs should be directed at keeping classified materials from unauthorized persons, and therefore focus on destroying rather than evacuated classified materials.

4. Escalation Measures. In the case of a natural disaster or a hostile action emergency, the MEU will use a logical progression of measures to be followed in order to prevent the compromise of classified material. The following steps will be taken:

- a. Augment existing security measures;
- b. Transfer non-essential material to a less vulnerable position;
- c. Destroy non-essential material;
- e. Destroy all material to prevent compromise.

Enclosure (1)

5. Authorization to Implement Plan

a. The 15th MEU Commanding Officer, upon the recommendation of the Security Manager, the Assistant Security Manager, or the 15th MEU CDO when they are the Senior MEU representative present, will authorize implementation of the EAP. Once authorized to conduct the EAP, the CMCC Officer, CMCC Clerk, and the section SSRs and ASSRs will be recalled to execute applicable portions of the EAP.

b. In the absence of the MEU CO, the Executive Officer/Security Manager is delegated authority to implement the EAP. As soon as possible, the Executive Officer will notify the Commanding Officer of the decision to implement the EAP.

c. Once the Commanding Officer or, in their absence, the Executive Officer directs the implementation of the EAP, the 15th MEU CDO or the 15th MEU CMCC Officer will notify the I MEF Senior Watch Officer (SWO), the I MEF Security Manager, and the Marine Corps Base (MCB) Camp Pendleton CDO of the decision to implement the EAP.

6. Execution of Emergency Destruction

a. The MEU will set the following priority for emergency destruction:

(1) Priority 1 - Top Secret material, Cryptographic equipment and keying material, with special emphasis on COMSEC, SCI, and any other SPECAT material;

(2) Priority 2 - Secret material;

(3) Priority 3 - Confidential Material.

b. All instances of emergency destruction being executed must be recorded and reported to the MEU Security Manager. These reports will have the reason for the destruction, the individual who authorized the destruction, items destroyed, time and date of destruction, and effectiveness of destruction. All reports will be kept by the MEU Security Manager for no less than 5 years. A copy of the report will be sent to HQMC (PP&O) via higher headquarters immediately.

7. 15th MEU Headquarters Aboard Camp Pendleton

a. In the event of an emergency such as a fire or other natural disaster during working hours in the 15th MEU Headquarters, Building 210821, personnel will immediately evacuate the building by the most expeditious route. All classified material need not be stored prior to the evacuation.

b. The MEU CDO will designate and post a sentry outside the central exits and ladder wells to ensure no unauthorized personnel enter the building. The sentry will not impede firefighters and other safety personnel from entering the building to accomplish their mission, however, the sentry will ensure that no emergency personnel depart with classified material.

c. If a fire occurs in the Headquarters Building after working hours, the 15th MEU CDO or Duty Noncommissioned Officer (DNCO) will immediately evacuate anyone still in the building. The CDO or DNCO will notify the fire department and the Area 21 Guard of the fire, and then notify the Executive

Enclosure (1)

Officer/Security Manager and the CMCC Officer/S-2. The DNCO will then muster at least four 15th MEU Marines to post one at each exit.

d. Once MEU personnel are allowed to re-enter the building, the CMCC Officer, CMCC Clerk, Section SSRs, and Section ASSRs will be recalled to conduct a complete inventory of all classified material. The CMCC Officer will report the results of the inventory to the MEU Security Manager.

8. Transfer Of Classified Material

a. In the event that the CO decides that the 15th MEU headquarters building is no longer secure to store classified material and directs implementation of the EAP, the MEU will transfer all classified material as required in coordination with the I MEF Security Manager and the Camp Pendleton Base Communication Center in order to store all MEU classified material in secure spaces.

b. All classified material will be placed in containers (seven cube embarkation boxes or pelican cases) for transfer.

c. The 15th MEU S-4 will obtain an adequate number of duty vans for the transfer.

d. The 15th MEU Headquarters Commandant will coordinate a working party to facilitate the move. Two person integrity is required for each vehicle that is used to transfer classified material.

e. Under the supervision of the 15th MEU CDO and DNCO, working parties from each staff section holding classified material will transfer the classified materials from the safes in their respective sections to their embarkation boxes where a detailed inventory will be taken (number of containers and contents). A copy of the inventory will be placed in each embarkation box with the classified material. Also, one copy of the inventory will be given to the Security Manager, one copy will be given to the CMCC Officer, and one copy will be retained by the SSR.

CHAPTER 6

Classified Material Control Center (CMCC) Standing Operating Procedures

1. General Guidance. This SOP sets forth procedures for the handling and controlling of classified material within the 15th MEU's CMCC and SSR's. Overall responsibility for classified material rest with the Commanding Officer. Responsibility for classified material stored within the CMCC rest with the S-2.

a. CMCC. The CMCC is tasked with controlling and accounting for all classified material other than Communications Material received or produced by the command.

b. SSRs. Classified materials held outside of the S-2/CMCC are the responsibility of the SSR.

(1) With the section, each person who handles classified material is responsible for its safekeeping. SSR's are established within sections of this Command to provide storage, control, and accountability of classified material routed to individual sections. SSR's are subordinate to the MEU CMCC.

(2) An SSR will be established within each of the following sections: S-2, S-3, S-4, and S-6. The SSR for each section is responsible for classified material being held by the section, regardless of who may have individually signed for the material. Each SSR shall be designated in writing by the Commanding Officer. The Alpha in each section will be the SSR and the Chief is the Alternate SSR. An inventory will of each respective section will be done when the SSR leaves the MEU. He will verify in writing that all classified material is accounted for in his section. The CMCC Clerk and the sections SSR replacement will verify.

c. 15th MEU Attachments. Some attachments, such as Counter Intelligence and Radio Battalion detachments, will hold classified material on their own cognizance and authority. This material is signed out from a parent unit's CMCC. The 15th MEU CMCC will render assistance as necessary in the storage of the material.

2. Custodian Requirements

a. CMCC Officer. The CMCC Officer is the S-2. The CMCC Officer must be a United States citizen who has been granted a final Secret clearance.

b. CMCC Clerk. The requirements for the CMCC Clerk are the same as for the CMCC Officer except that enlisted personnel in the grade of sergeant or above may be designated as CMCC Clerk.

c. SSR. Each Staff Section will assign the section Alpha as the primary Section Security Representative (SSR) for their section. SSR's must be a U.S. citizen, with a clearance commensurate with the highest level of classified material held by that SSR section.

d. ASSR. The section Staff Noncommissioned Officer in Charge will be assigned as the Alternate SSR (ASSR). ASSR must be a U.S. citizen, with a clearance commensurate with the highest level of classified material held by that ASSR section.

Enclosure (1)

e. SSA. A section may designate Section Security Assistants (SSAs) if desired. These assignments do not relieve the responsibility of the Section's SSR or the Security Manager. For the purpose of this Order, the term "Section Security Assistants" refers to security clerks, acting in accordance with MEU Security policies. Security clerks may be assigned as SSAs, regardless of rank, as long as they have a clearance commensurate with the highest classification of the material handled.

f. Security System Marine (SSM). SSMs are those Marines that are designated in writing that are authorized to move data to classified removable media. Each MEU section will identify no more than two Marines and two computers (that only those two Marines may access) to be authorized to move data to classified removable media. Those computers that are capable to move data to and from removable media are referred to as Security System Computers' and must be inventoried and tracked by their serial numbers monthly.

3. Physical Security Measures. This Command's CMCC meets the physical security requirements for the storage of moderate quantities of classified material, up to and including Secret. All Staff Sections will be the subject of a Physical Security Evaluation conducted by this Command's CMCC Officer prior to the storage of classified material in any staff section. All Classified Material will be kept in GSA approved security containers within the respected sections. No open storage of classified material is authorized within any area of this command. The MEU is not authorized to hold or store Top Secret material except in the SSES aboard ship.

a. During Working Hours

(1) Classified materials, which are removed from storage for working purposes, shall be kept under constant surveillance and never left unattended. They shall be turned face down or covered with the correct cover sheet or place in a folder when not in use.

(2) Classified information shall not be discussed over the telephone or when unauthorized personnel may overhear the conversation.

(3) Computer disks, carbon papers, plates, stencils, mats, preliminary drafts, and all similar items containing classified information shall be safeguarded according to their level of classification.

(4) STU III Key. Because the Crypto Ignition Key (CIK) permits the STU II to be used in the secure mode they must be protected against unauthorized access and use. CIKs may be retained by the individuals who sign for them on local custody. These individuals must protect the CIK as they would personal property. They must have physical control over the CIKs at all times. The CIK must be removed from its associated terminal whenever an authorized person is not present.

b. After Working Hours. Securing procedures will include a minimum of the following:

(1) A Security Container Check Sheet (SF 702-101) shall be posted on each safe or lock box where classified material is stored. This form may be destroyed after 30 days after last entry unless they are used to support an ongoing investigation.

Enclosure (1)

(2) Conduct security checks at the end of each working day utilizing the Activity Security Checklist (SF 700). This sheet will be posted on all outside doors of spaces containing classified material containers.

(3) Notice shall be conspicuously posted giving instructions to follow if any security container is found open. Figure 6-1 is a sample format for open safe instructions. It shall list only the names of individuals to be contacted in the event a security container is found open. The Command Duty Officer (CDO) shall maintain a recall roster of all personnel within the MEU.

(4) Combination locks will be turned a minimum of four complete turns after closing and a witness will be required to check containers to ensure they are locked. The witness will be different from the individual locking the container and will conduct his check within five minutes after the first individual.

(5) Security containers shall bear no outside markings which may indicate the classification level of the contents.

(6) Open/Closed or Open/Secured signs shall be used on all containers. Figure 6-2 provides an example of an open/closed sign.

(7) Sections that store or routinely use classified material will have a Classified Material Warning Sign conspicuously posted.

| <u>Open Safe Instruction</u> | | |
|---|--------------|--------------|
| Date combination Changed: _____ | | |
| <u>PROCEDURES TO FOLLOW IF THIS CONTAINER IS FOUND OPEN</u> | | |
| *1. Notify the Duty Officer immediately. | | |
| 2. Guard/Post a guard on the container until arrival of Duty Officer. | | |
| 3. Only the Duty Officer shall lock the container. | | |
| 4. Contact one of the below listed personnel in the order listed below. | | |
| GySgt Whitehead, Kevin | 760-725-4331 | See DNCO |
| GRADE/NAME | (Work Phone) | (Home Phone) |
| Sgt Vinopal, Dale | 760-725-4331 | See DNCO |
| GRADE/NAME | (Work Phone) | (Home Phone) |
| | | See DNCO |
| GRADE/NAME | (Work Phone) | (Home Phone) |
| | | See DNCO |
| GRADE/NAME | (Work Phone) | (Home Phone) |

Figure 6-1.--Sample Format for Open Safe Instructions

Enclosure (1)

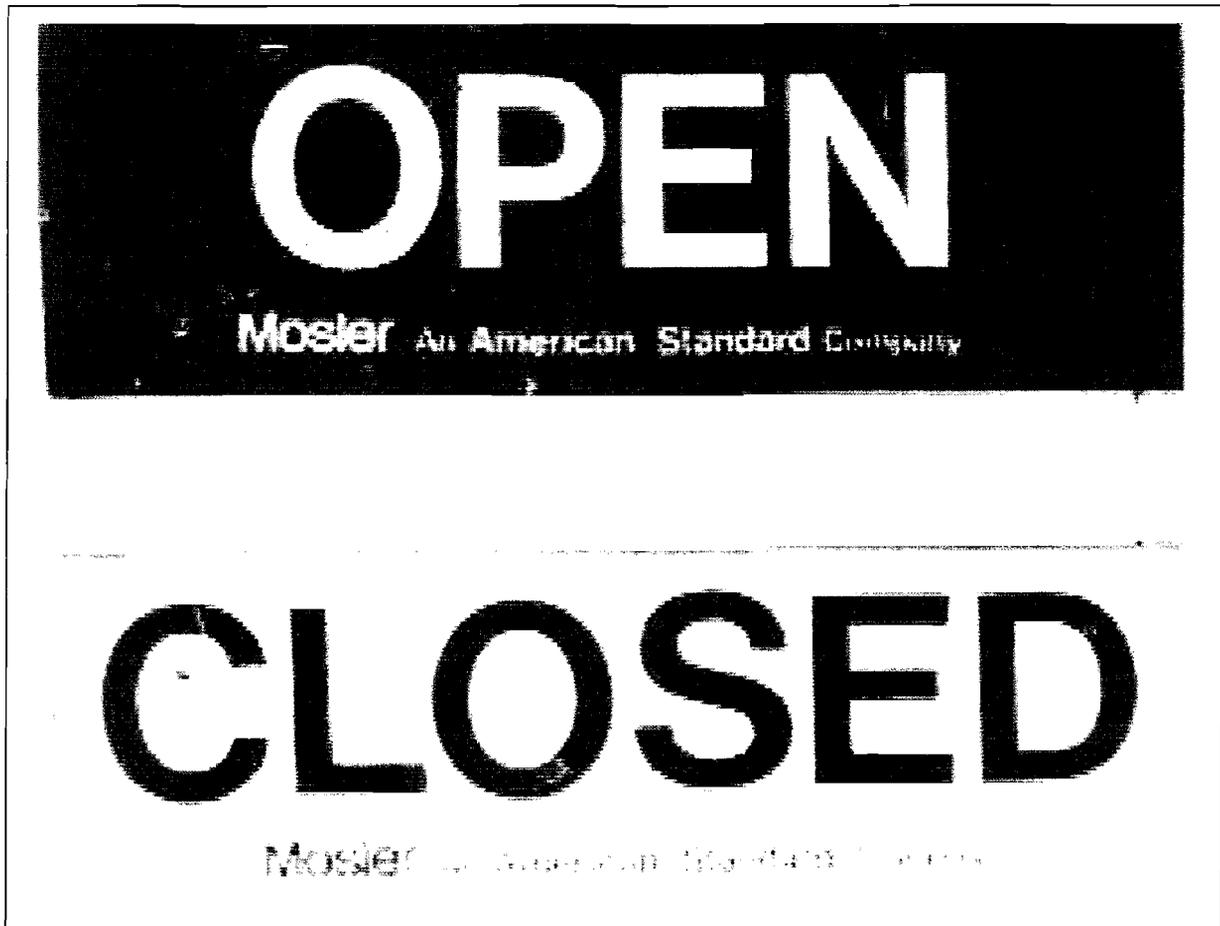


Figure 6-2.--Sample of Open/Close Sign

4. Secondary Control Points (SCPs). The S-1, S-3, S-4, and S-6 are authorized to hold classified materials. SCPs may not retain classified material above the level specified in their establishment authorization.

a. SSR's are responsible for the control and protection of all classified material brought into their respective sections.

b. The SSR will ensure that the following actions are accomplished:

(1) Verify the level of security clearance and access of each person assigned to the section served by that SSR and, when required, initiate action to upgrade or reduce individual clearance/access. Ensure only authorized personnel have access to classified materials.

(2) The SSR will ensure expeditious routing of classified documents to all cognizant personnel within the section. Return all controlled documents to the CMCC for additional routing to other staff sections, transfer or destruction as required.

(3) Each SSR is responsible for the establishment and maintenance of records for all controlled classified material checked out to the SSR under his control.

Enclosure (1)

(4) The SSR shall inventory all controlled classified material monthly or when any personnel in these sections changes and the results will be forwarded to CMCC for verification against CMCC records and filed for retention.

(5) Current security container information envelopes, with combinations to all SCP Security Containers are held by the EKMS manager. Figure A3-1 is the only form authorized to record security container combinations within this Unit. The outside cover of the form will be taped to the inside of the security container drawer which holds the combination dial. This form will list the home addresses and telephone numbers of personnel to contact in the event of an emergency.

(6) A listing of the priority of removal/destruction is located inside, at the front of the top drawer of each security container while in a hostile area.

(7) Controlled classified material is NOT transferred permanently between sections, but is delivered to the CMCC to ensure proper control/accounting.

(8) SSR's do not destroy controlled classified material. Controlled material will be delivered to the CMCC for destruction.

(9) SCP files will be maintained in an orderly fashion to avoid loss and/or accounting errors.

(10) Security personnel are to be thoroughly instructed on the nature of their duties.

(11) Unclassified material is not to be filed with classified material, unless it pertains to the classified subject matter.

(12) Combinations to all security containers are to be changed in accordance within the time frames established in the current edition of reference (d).

5. Inspection of Secondary Control Points. The Security Manager will conduct inspections of SCPs on a quarterly basis via the CMMC clerk to ensure the compliance of this Order and other related instructions utilizing Figure 6-3. The 15th MEU Security Manager may direct unscheduled/unannounced inspections of the CMCC or any SCP at any time.

Example HDD Inventory

Monday, May 16, 2011

| | | |
|---------------------------|----------------------------|---------------------|
| New Control Number | Old Control Number: | Print: _____ |
| Description: | HDD Type: | Sign: _____ |
| HDD Serial Number: | Capacity: | Date: _____ |
| Section: S-X | Manufacturer: | |
| New Control Number | Old Control Number: | Print: _____ |
| Description: | HDD Type: | Sign: _____ |
| HDD Serial Number: | Capacity: | Date: _____ |
| Section: S-X | Manufacturer: | |
| New Control Number | Old Control Number: | Print: _____ |
| Description: | HDD Type: | Sign: _____ |
| HDD Serial Number: | Capacity: | Date: _____ |
| Section: S-X | Manufacturer: | |
| New Control Number | Old Control Number: | Print: _____ |
| Description: | HDD Type: | Sign: _____ |
| HDD Serial Number: | Capacity: | Date: _____ |
| Section: S-X | Manufacturer: | |
| New Control Number | Old Control Number: | Print: _____ |
| Description: | HDD Type: | Sign: _____ |
| HDD Serial Number: | Capacity: | Date: _____ |
| Section: S-X | Manufacturer: | |

Figure 6-3.--Sample of 15th MEU Inventory List

6-6

Enclosure (1)

Rep Name: _____ Rep Sign: _____ Date: _____ Page 1 of 2

MEMO 5510.1
17 AUG 2011