UNITED STATES MARINE CORPS
COMMAND ELEMENT
II MARINE EXPEDITIONARY FORCE
PSC BOX 20080
CAMP LEJEUNE, NC 28542-0080

II MEFO 5510.1E
SECMAN
FEB 04 2019

II MARINE EXPEDITIONARY FORCE ORDER 5510.1E

From: Commanding General, II Marine Expeditionary Force
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR THE INFORMATION AND PERSONNEL SECURITY PROGRAM (SHORT TITLE: SOP FOR IPSP)

Ref: (a) DoD Manual 5200.01, Volumes 1-4, DoD Information Security Program
(b) SECNAV M-5510.30, Personnel Security Program
(c) SECNAV M-5510.36, Information Security Program
(d) MCO P5510.18A, Marine Corps Information and Security Program
(e) DoD 5220.22-M, National Industrial Security Program
(f) Homeland Security Presidential Directive 12 (HSPD-12)
(g) MCO 5530.14A, Physical Security Program
(h) MCO 3302.1E, Anti-Terrorism/Force Protection Program
(i) II MEFPOL 11-18, Building H-1 Access Control Policy
(j) II MEFPOL 5-17, North Atlantic Treaty Organization Program
(k) II MEFO P5511.1C, II MEF SOP for Classified Material Control Center

Encl: (1) II MEF Security Manual

1. Situation. To publish II Marine Expeditionary Force (MEF) command policy addressing responsibilities, and procedures for the management of Personnel, Information, Physical and Industrial Security. This Order is developed in accordance with references (a) through (k).

2. Cancellation. II MEFO 5510.1D.

3. Mission. To publish uniform and effective security procedures in the application of personnel, information, and physical security disciplines. Each chapter will address a security discipline or a part of a discipline. Familiarity with the contents of all the references is essential in developing an understanding of the supplemental instructions contained herein.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. Set forth policies and establish procedures in support of the II MEF Security Program and provide all levels of management with guidelines for adherence to regulations.

(2) Concept of Operations. The Command's Director of Security will administer the Personnel, Information, Physical and Industrial Security Programs as contained herein and conduct annual internal reviews and inspections of each security program, to include subordinate commands as a member of the Command Inspector's Inspection Team and independently as required. Self-inspections will be conducted semi-annually as directed in reference (d). Independent inspections and inventories are typically conducted annually, as circumstances may dictate, on all commands and organizations that hold classified information and equipment.

b. Subordinate Element Missions. Comply with the intent and content of this Order.

c. Coordinating Instruction. Recommended changes concerning this Security SOP are invited and may be submitted to the Commander via the appropriate chain of command.

5. Administration and Logistics. This Order incorporates all changes promulgated by the Secretary of Defense, Secretary of the Navy, and Commandant of the Marine Corps since publishing of the previous Order.

a. This Order contains modifications designed to clarify and provide a more comprehensive understanding of the Personnel, Information and Physical Security Programs as it pertains to the mission of II MEF and its activities.

b. This Order must be used in conjunction with references (a) through (k).

6. Command and Signal

a. Command. This Order applies to all active duty, reserve, and foreign military, civilian employees, contract support personnel within II MEF.

b. Signal. This Order is effective date signed.

B. N. WOLFORD
Chief of Staff

DISTRIBUTION: A,B

II MEF SECURITY MANUAL

TABLE OF CONTENTS

ENCLOSURE (1)

Chapter 1

RESPONSIBILITIES

1001. BASIC GUIDANCE

1. II Marine Expeditionary Force (II MEF) personnel will follow the guidelines and instructions set forth in the appropriate governing documents from the Department of Defense (DoD), Department of the Navy (DON) and U.S. Marine Corps (HQMC).

2. The Director of Security will adjust security policies and procedures as required when changes are made to the governing orders and directives.

3. Vigilance by all military/civilian personnel of II MEF is the ultimate security safeguard.

1002. DEFINITIONS

1. Access. The ability or opportunity to obtain knowledge of classified information.

2. Classified National Security Information. Information that has been determined pursuant to Executive Order 13526, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

3. Classified Material. Any matter, document, hard drive, magnetic tape, media, product, or substance on or in which classified information is recorded or embodied.

4. Continuous Evaluation. The process by which all military/civilian individuals who have established security clearance eligibility are monitored to assure they continue to meet the loyalty, reliability and trustworthiness standards expected of individuals who have access to classified information. This monitoring process relies on all personnel within a command to report questionable or unfavorable information that could place in question an individual's loyalty, reliability, or trustworthiness.

5. Custodian. A properly cleared individual with access to a specific category of classified material who has possession of, or is otherwise charged with, the responsibility for receiving,

safeguarding, destroying, transferring and accounting for classified information.

6. Derivative Classification. Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. The duplication or reproduction of existing classified information is not derivative classification.

7. Information Security. The system of policies, procedures, and requirements in place to protect classified information that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect Controlled Unclassified Information (CUI) that may be withheld from release to the public pursuant to Executive Order, statute, or regulation.

8. Joint Personnel Adjudication System (JPAS). JPAS tracks and contains all clearance related information for all DON personnel. This system will transition to Defense Information System for Security (DISS) by 2020.

9. Need-to-Know. Is a determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. It is the custodian's responsibility to determine the Need-to-Know before releasing classified information to any person.

10. Personnel Security Clearance. Is an administrative determination by the commander that an individual is eligible for access to classified information of a specific classification category. This is based upon the appropriate Personnel Security Investigation (PSI) and Department of Defense Consolidated Adjudication Facility (DoDCAF) adjudication.

11. CMCC Custodian. For the purpose of this Order, the Classified Material Control Center (CMCC) custodian is responsible for the control of classified material at this command. The CMCC Custodian must be coordinated with before receiving, reproducing, transmitting, or destroying collateral classified material in coordination with the governing orders and directives.

12. Security Incidents. There are two types of security incidents: violations and infractions. In either case, a security inquiry (SI) or investigation may be required to determine the circumstances of the incident and compliance with applicable directives and orders.

13. Spillage. Occurs whenever classified information or CUI is placed on an information system possessing insufficient information security controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information is subject to the requirements of this instruction.

14. Technical Data. Recorded information that is related to experimental or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts. Examples of technical data include: research and engineering data or drawings, associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information and computer software documentation.

15. Tentative Classification. Allows those individuals without original classification authority, who create information they believe to be classified or which they have significant doubt about the appropriate classification, to mark the information accordingly.

1003. COMMAND MANAGEMENT. In compliance with references (a), (b), (c) and (d), the Command Security Program has established a network of personnel with distinct responsibilities to supervise and ensure effective security, control, and utilization of classified material.

1. Control Officers. To ensure the proper handling and control of classified material, the following officers and their alternates, as appropriate, will be appointed in writing to manage the security program:

a. Director of Security

b. Top Secret Control Officer

c. North Atlantic Treaty Organization (NATO) Control Officer

d. Classified Material Control Center (CMCC) Custodians

Note: NATO CONTROL POINT OFFICER. HQMC is the Subregistry for all NATO Material held by the Command. Reference (j) denotes NATO responsibilities and program controls for this command.

2. Program Managers, Supervisors, and Special Staff Officers

a. Are responsible for security, and for the continual review of security procedures and practices within their respective units and areas of responsibility.

b. Will maintain adequate security for classified material, and ensure both military and civilian personnel have an eligibility to access classified information and have a demonstrative "Need-To-Know" before handling classified material in the performance of their duties.

c. Will ensure any adverse information that becomes known concerning any member of their activity is brought to the attention of the Director of Security.

d. Will recommend one security point of contact to coordinate security functions to the Director of Security. Alternate Security Coordinators may be recommended for appointment. The recommendation letter has to have the signature of senior management within the program or staff office.

e. Will ensure all of their military/civilian personnel attend/complete all of the courses per the II MEF annual training plan.

3. Safeguarding. Everyone is responsible for the security of classified information to which he or she has access. Each individual is responsible for reporting to the Office of the Director of Security any violation of security regulations, security weakness, or security incidents of which they may become aware. This can be accomplished in person, via email, or by phone to any security member.

4. Description of the security organization and identification of positions. Breakdown of the security organization within II MEF is as follows:

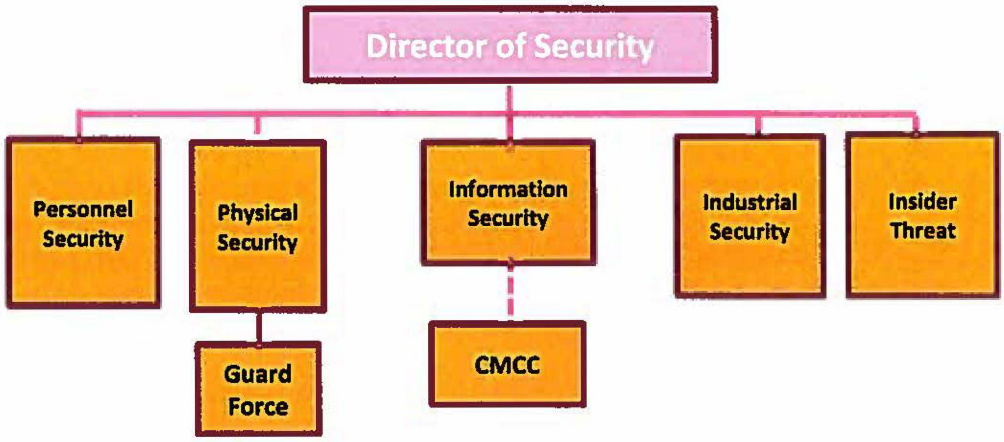

Figure 1-1. Security Organization

Chapter 2

PERSONNEL SECURITY INVESTIGATIONS, CLEARANCES, AND ACCESS

2001. GENERAL. This Order provides the requirements relating to personnel security investigations, access authorization, and the administrative withdrawal, denial or termination of security clearances or access for military and government civilian employees of this command.

2002. BASIC POLICY. No person shall be granted access to classified material or assigned to sensitive duties unless a favorable determination has been made by the Department of Defense Consolidated Adjudication Facility regarding loyalty, reliability, trustworthiness, and judgment. The initial determination will be based upon a Personnel Security Investigation (PSI) appropriate to the clearance level required for the position held and duties assigned.

2003. RESPONSIBILITIES

1. The Personnel Security Specialists are responsible for the administrative preparation and submission of a PSI for II MEF military and civilian personnel.

2. Program Managers, Supervisors and Special Staff Officers requesting security clearances or investigations of their personnel, should contact the Personnel Security Specialists for guidance in processing the requests. These requests must be aligned with the billet description for military person and position description for civilian personnel.

2004. POLICIES AND PROCEDURES

1. No person will be appointed or retained as a civilian employee in the DON and Marine Corps, granted access to classified information or assigned to other sensitive duties that are subject to investigation under the provisions of security regulations unless such appointment, acceptance, retention, clearance or assignment is clearly consistent with the interests of national security.

2. Appointment or retention in civilian employment and acceptance or retention in the Marine Corps shall be assumed to be clearly consistent with the interests of national security unless or until a determination has been made by competent

authority that there is a reasonable basis for doubting the person's loyalty to the Government of the United States.

3. Determinations of suitability or eligibility for civilian employment or service in the Marine Corps on any other basis are not personnel security determinations, and therefore, are not under the purview of this Order.

2005. INVESTIGATIONS. Verification of a valid security investigation will be completed as part of the check-in process.

1. Military personnel are required to have a National Agency Check with Local Records Check (NACLC) or T3 performed by the National Background Investigations Bureau (NBIB) and adjudicated by the DoDCAF for access to information and systems up to the Secret level.

2. Civilian personnel require an initial Access National Agency Check with Inquiries (ANACI) now known as a T1 or a follow-on NACLC now known as a T3R reinvestigation performed by NBIB and adjudicated by the DoDCAF for access to information and systems up to the Secret level.

3. Both military and civilian personnel are required to have an initial Single Scope Background Investigation (SSBI) now known as a T5 or a follow-on Phased Periodic Reinvestigation (PPR) now known as a T5R performed by NBIB and adjudicated by the DoDCAF for access to information and systems up to the Top Secret level. This includes all individuals requiring Sensitive Compartmented Information (SCI) access.

4. To remain in compliance with references, supporting contractors must have a favorably adjudicated NACLC/T3 (for Secret) or SSBI/T5 (for Top Secret) if classified access is required by their contract. Contractors requiring a Common Access Card (CAC) must have at least a National Agency Check with Inquiries (NACI/T1) opened. If the NACI/T1 returns unfavorably, the contractor CAC must be retrieved and revoked. Chapter 6 has more information on Industrial Security issues.

2006. INVESTIGATION PROCESS. PSIs take from three to twelve months on average to complete, depending on the type of investigation and the information provided by the individual. Investigations will not be performed on individuals with expected separation from federal service of 12 months or less.

1. Favorable. A favorable personnel security investigation determines whether the individual is of good character, is loyal to the U.S. government, reliable, trustworthy, and of good judgment. An individual who has been the subject of a favorable PSI is eligible to hold the type of clearance appropriate to the level of investigation performed. The DoDCAF-Navy is solely responsible for the adjudication of all PSIs for II MEF personnel.

2. Unfavorable/No Determination Made. An unfavorable PSI adjudication will result in the immediate loss of access to classified material. A "No Determination Made" can result from several scenarios, but generally means a prior investigation was not completed or sufficiently satisfied. Either of these will require interaction with the employee, Security and the DoDCAF-Navy.

2007. CLASSIFIED ACCESS

1. Top Secret. Top Secret access may be granted to those individuals who have been the subject of a favorably adjudicated SSBI/T5, SBPR/T5R or PPR/T5R investigation and their current position requires that level of Need-to-Know. Top Secret level investigations will be in compliance for five years after the closing date of the investigation. After the five-year period, individuals still requiring Top Secret access are required to submit a new investigation package. If Top Secret access is no longer required, Secret access eligibility remains for an additional five years.

2. Secret. Secret access may be granted to those individuals who have been the subject of a favorably adjudicated NACLC/T3, ANACI/T3, SSBI/T5, or PPR/T5R investigation and their current position requires that level of Need-to-Know. Secret level investigations will be in compliance for ten years after the closing date of the investigation. After the ten-year period, individuals are required to submit a new investigation package.

2008. INTERIM ACCESS. Individuals requiring Interim Access must have their investigation submitted to NBIB, and have their security-screening questionnaire screened by the Personnel Security Office for an eligibility determination and then approved by the Command Security Manager.

1. Individuals with adverse information (Driving under the Influence, Non-Judicial Punishment, criminal conduct, offenses

involving drugs or alcohol, etc.) are not eligible for Interim Access.

2. Individuals who have been the subject of a previously unfavorable PSI are not eligible to hold Interim Access. Interim Access can be granted and removed by the Director of Security.

2009. ADMINISTRATIVE WITHDRAWAL OF ACCESS

1. An individual's classified access will be administratively withdrawn if there is no foreseeable need for access to classified information. In consonance with a need to maintain the minimum number of cleared personnel consistent with mission requirements, Program Managers, Supervisors, or Special Staff Officers must notify the Director of Security of any person(s) who falls under one of the following situations:

a. Who should have their access downgraded or administratively withdrawn. Provide justification of this request.

b. When any person(s) are reassigned in the command to another job position. The new supervisor has to request access if required for that person's new position.

2. Administrative withdrawal of an individual's access will be effective upon change of the individual's duties, if they no longer require classified access.

3. When a classified access is administratively withdrawn, the appropriate entry will be made in both the individual's personnel security file and in JPAS. Administrative withdrawal of an individual's access has no negative bearing on the individual's clearance eligibility.

2010. CLEARANCE DENIAL OR REVOCATION FOR CAUSE

1. When a personnel security determination is made that an individual does not meet or no longer satisfies the requirements for a security clearance, the security clearance will be denied or revoked by the DoDCAF-Navy.

2. All due process provisions will be afforded to the individual.

3. The Personnel Security Office will be the primary point of contact for the individual and the DoDCAF-Navy, through the denial or revocation process.

4. The Commander may withdraw access to classified information when an employee has committed a security violation, a security incident, or disciplinary infractions, based on the severity of the incident.

2011. ACCESS

1. The Commander will grant access to classified information to an individual who has an official Need-to-Know, valid clearance eligibility and, for whom there is no disqualifying information.

2. Prior to granting access to classified material, all individuals, both military and civilian, must complete a Badge/Access Request Form, which can be obtained from the Security Management Office or on the Security Sharepoint Site.

3. The request should clearly articulate the classified access requirement and must be signed by the individual's supervisor. Once signed, send the Request Form to the Security Management Office for continued processing. Security is not the granting authority to classified material or areas, but simply facilitates enabling or disabling access, as requested or required by appropriate leadership personnel.

2012. VISIT REQUESTS. All incoming Visitor Requests must be submitted via JPAS to Security Management Office (SMO) Code 203611F14 for Non-TS/SCI and 203611F13 for TS/SCI.

2013. FOREIGN TRAVEL NOTIFICATION

1. All personnel, civilian and military, as directed by reference (n), will notify the Anti-Terrorism/Force Protection (AT/FP) Officer and Security Manager of their intent to either go on official government business or personal travel outside of the Continental United States (OCONUS) no less than 30-days prior to their departure date. This is accomplished by submitting the information on the II MEF Security SharePoint Page via the Foreign Travel link.

2014. REPORTING REQUIREMENTS

1. All command personnel are required to report unfavorable information to both their supervisor and the Personnel Security Office as soon as the information becomes available. Reportable personnel security issues are explained below in paragraph 4.

2. In addition to self-reporting, personnel have an obligation to report derogatory information about another employee once they are aware of the information. This includes information on co-workers, supervisors, subordinates, contractors or visitors.

3. The Security Manager is required to report all derogatory/unfavorable information to the DoDCAF-Navy without attempting to mitigate the information first.

a. The DoDCAF-Navy will then decide whether to favorably re-adjudicate the individuals eligibility or to begin the adverse determination process.

b. Security's jurisdiction over the matter ends once reported but Security will remain the primary point of contact between the individual and the DoDCAF-Navy as long as the person is assigned to II MEF.

c. If an individual resigns or retires prior to the DoDCAF-Navy making an adjudicative decision, the DoDCAF-Navy will enter a "Loss of Jurisdiction" entry into JPAS, which will end any adjudicative decision making process.

4. The following security issues must be reported to Security immediately:

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

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

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

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

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

f. Unexplained affluence or excessive indebtedness.

g. Alcohol abuse or alcohol related incidents.

h. Illegal or improper drug use/involvement.

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

j. Criminal conduct.

k. Noncompliance with security requirements.

l. Engagement in outside activities that could cause a conflict of interest.

m. Misuse of Information Technology Systems.

5. Further information on items above can be found in reference (b) Appendix G (Adjudication Guidelines).

2015. CONTINUOUS EVALUATION PROGRAM

1. All activities will report questionable or unfavorable information to the Director of Security for reporting to DoDCAF-Navy.

2. If the developed information is significant enough to require a suspension of the individual's access for cause, the suspension action will be accomplished in accordance with paragraph 9-7 of reference (b) using the proper administrative chain-of-command.

3. SCI access will be suspended by the SSO if required per reference (b) and applicable Intelligence Community directives and regulations. The SSO will coordinate these activities with the Director of Security so that command records can be updated to reflect status.

4. A command report of local access suspension for cause will automatically result in suspension of the individual's clearance eligibility by the DoDCAF-Navy. Once clearance eligibility is suspended (or the individual is debriefed from

access for cause), the individual may not be granted access or considered for re-indoctrination until clearance eligibility has been reestablished by the DoDCAF-Navy.

5. The Director of Security will act as the "go-between" in matters involving the DoDCAF-Navy, except in those instances under the purview of the SSO.

Chapter 3

ADMINISTRATIVE SANCTIONS

3001. REQUIREMENT. As directed by references (a) through (d) all II MEF personnel, civilian or military, are individually responsible for complying with the provisions of this Order and reporting any security incidents involving classified information.

3002. INCIDENTS SUBJECT TO SANCTIONS

1. Military and civilian personnel of the Department of the Navy are subject to administrative sanctions if they:

a. Knowingly, willfully, or negligently disclose classified information or CUI to any unauthorized person, organization, system, country or state.

b. Knowingly, willfully, or negligently violate any provision of the governing orders and directives established by the DoD, DON, and HQMC or this Order.

2. Sanctions include, but are not limited to: a warning notice, a reprimand, suspension without pay, forfeiture of pay, and removal or discharge. Sanctions will be imposed upon any person, regardless of grade or level of employment, responsible for a violation specified above, and as appropriate to the particular case, in accordance with applicable law and regulations.

3. Security violations and incidents reflect negatively on an individual's clearance eligibility and continued access to classified information. Security incidents can be cause for denial or revocation of the individual's clearance eligibility even when the violations are not separately punishable.

4. The unauthorized disclosure or spillage of CUI will be handled in accordance with reference (a) Volume 4 which also includes any amplifying protection and handling guidance for specific types of CUI required by law or federal regulation.

3003. CORRECTIVE ACTION. The DON has indicated that appropriate corrective action will be taken whenever: a violation occurs, or repeated administrative discrepancies, or repeated neglect, or disregard of requirements occurs.

1. The Director of Security will ensure a Security Inquiry (SI) is conducted, in accordance with the requirements outlined in DoD, DON and HQMC regulations and directives of the governing orders and directives for all security violations.

2. The Director of Security will ensure that NCIS is contacted when necessary and copies of all SIs are forwarded to the Commandant of the Marine Corps, PP&O (PS) if there is loss or compromise of classified material.

3004. ADMINISTRATIVE DISCREPANCIES

1. Repeated administrative discrepancies in the handling of classified material that are determined not to constitute an incident under paragraph 3002 may be grounds for adverse administrative action including: warning, admonition, or reprimand, as appropriate.

2. Administrative discrepancies include: failure to use appropriate cover sheets, incorrect classification markings and computation of dates for declassification, failure to properly mark working papers, failure to submit timely inventories, failure to initial the Security Container Check Sheet (SF-702), or other repeated neglect or disregard of requirements of this Order.

3005. SECURITY INCIDENTS/VIOLATIONS

1. There are three types of security incidents:

a. Willful violations are security incidents that indicate a person purposefully disregarded DoD, DON, and/or HQMC security or information safeguarding policies or requirements that resulted in, or could be expected to result in, the loss or compromise of classified information.

b. Negligent violations are security incidents that indicate a person acted unreasonably in causing the spillage or unauthorized disclosure (e.g., a careless lack of attention to detail, or reckless disregard for proper procedures).

c. Inadvertent violations are incidents where the person did not know, that the security violation or unauthorized disclosure was occurring (e.g., the person reasonable relied on improper markings).

2. There are infractions of security requirements involving failure to comply which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent.

a. While it does not constitute a security violation, if left uncorrected, infractions can lead to security violations or compromises.

b. An infraction requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

3. A security violation obviously presents the greater threat to national security as the unauthorized disclosure of classified information or CUI poses a significant threat to our Nation's security and to DoD, DON, HQMC, and II MEF operations and missions.

a. Security incidents of either type will be reported, and the problems causing the incident corrected rather than covered up.

b. If culpability is demonstrable, the offender(s) will be appropriately disciplined.

3006. DISCIPLINARY ACTION

1. The disciplinary action to be taken which resulted from a security violation by military personnel will be determined by appropriate authority.

2. There is no schedule of disciplinary actions for civilians, but rather a range of actions extending from informal admonishment to removal. This extensive range permits actions of varying degrees of severity.

3. Any person who violates the provisions of security regulations is subject to disciplinary action. The punishments for breaches of security for civilian personnel are:

FOR FAILURE TO SAFEGUARD CLASSIFIED MATERIAL RESULTING IN A SECURITY COMPROMISE:

First Offense	Second Offense	Third Offense
Reprimand	Temporary Access Suspension (TAS)	Local Access Suspension

FOR FAILURE TO SAFEGUARD CLASSIFIED MATERIAL NOT RESULTING IN A SECURITY COMPROMISE:

First Offense	Second Offense	Third Offense
Verbal Reprimand	Reprimand to TAS	Local Access Suspension

4. In addition to the possible disciplinary actions outlined above, 18 U.S.C., §798 informs all personnel that unauthorized disclosure of classified information may result in a fine of not more than $10,000 or imprisonment for not more than ten years, or both, per occurrence.

Chapter 4

SECURITY EDUCATION AND TRAINING

4001. REQUIREMENT. Implement, as directed by references (a) through (d), an active security education program to instruct all personnel in security policies and procedures. All civilian employees and military personnel are required to attend/complete the annual security training when scheduled. Waivers will not be granted.

4002. RESPONSIBILITIES

1. The Director of Security

a. Formulates and coordinates the security education program and is responsible for ensuring personnel receive the required security training.

b. Monitors the program, obtains training aids and program materials, and assists in presentations.

2. The security staff will assist the Director of Security with security training within the Command.

NOTE: Failure of individuals to complete the training requirements mentioned above could result in the loss of access until compliance is achieved.

4003. SECURITY BRIEFINGS AND TRAINING

1. At a minimum, the following required security briefs and training will be conducted for command personnel.

a. Local Orientation Briefing. A local orientation security briefing will be conducted for all newly joined personnel by the Director of Security or one of his/her representative. This briefing will be a part of the check-in process and will provide new personnel an awareness of basic requirements for the protection of classified information and Command security procedures.

b. Annual Refresher Briefing. A general security refresher-training brief will be conducted annually for all Command personnel by the Director of Security or his/her staff.

c. Counterintelligence Briefing (Reference DoD 5240.06). All civilian employee and military members must attend an annual Counterintelligence Brief provided by NCIS as required by reference (f). The Director of Security will schedule this mandatory briefing.

d. NATO Security Clearance Briefing

(1) All civilian employees and military members who have classified access will be required to receive a NATO awareness security brief. This briefing provides guidance concerning how to protect NATO classified material if the individual happens to be exposed to it inadvertently.

(2) All civilian employees and military members who are required to review and handle NATO material will be required to have read and acknowledged the NATO security brief.

e. Special Access Briefings. Any civilian employee and military member whose duties require access to special types of information (e.g., NATO, SCI, or other special access programs) must be briefed prior to access to the information. The Director of Security or his/her representative will conduct the NATO briefing. The SSO will conduct the SCI and SAP briefings.

f. Antiterrorism/Force Protection Training. Prior to personnel traveling outside CONUS (Temporary Additional Duty or leave), they must complete this training. This training is an annual requirement for all military/civilian personnel.

g. Debriefings. Personnel who have had access to classified and CUI shall be debriefed prior to transfer, termination of active military service or civilian employment, or temporary separation for a period of sixty days or more, including leave without pay.

h. One-Time Special Security Briefings. From time to time, as new information concerning security regulations and procedures is received from higher authority, the Director of Security will schedule special training sessions for the particular organizational groups, which are affected by the new security information.

i. Derivative Classification Training Requirements. Per references (a) through (d) all personnel who receives or generates classified information will be marking derivatively classified information. Individuals that derivatively classify

will receive annual training in the proper application of derivative classification principles, with an emphasis on avoiding over-classification. Due to the possible exposure to and requirement to take classified notes, everyone granted classified access is directed to complete this training. The training will be completed on the Center of Development Security Excellence (CDSE) website at the following link https://cdse.usalearning.gov/

j. Foreign Travel Briefs. Foreign travel briefings are normally provided by the resident NCIS agent located at Marine Corps Base, Camp Lejeune (MCI-East) prior to traveling overseas. NCIS personnel will determine if a foreign travel brief/debrief is necessary dependent upon the country. Personnel with TS/SCI or SAP access must coordinate their travel plans with the SSO.

2. Security Professionals. The Security Professional Education and Development (SPeD) Certification Program is part of the DoD initiative to professionalize the security workforce. This initiative is to ensure there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

3. On-The-Job Security Training. For all other personnel there is On-Line training and other resources that are available at the CDSE, which may be used at https://cdse.usalearning.gov/. A number of these training courses have acquisition points.

a. This training covers a wide range of areas that could apply to the individual job descriptions and can assist in understanding their duties.

b. There are individual courses that are Instructor-led, eLearning, Virtual Instructor-led, Curricula, Shorts, and Webinars.

Chapter 5

INFORMATION SECURITY POLICY AND PROCEDURES

5001. POLICY. The Information Security Program is established, as required by references (a), (c), and (d), to ensure information classified under the authority of Executive Order (E.O.) 13526 is protected from unauthorized disclosure. This program applies uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission, and destruction of classified information.

5002. AUTHORITY

1. The Commanding General, II MEF is responsible for establishing and maintaining an Information Security Program in compliance with references.

2. The responsibility for the security and proper handling of classified material extends directly to military and civilian personnel having knowledge or possession of such material and to Program Managers and supervisors within whose purview classified material is utilized.

3. Individual requests for guidance or interpretation of this publication should be addressed to the Commanding General, II MEF, Attn: Director of Security.

5003. APPLICABILITY

1. This chapter establishes coordinated policies for the security of classified information, by incorporating the policies of numerous DoD, DON, and HQMC directives. It is not expected that these directives will or can ensure absolute security at II MEF. Rather, they permit the accomplishment of essential tasks while affording selected items of information reasonable degrees of security with a minimum risk.

2. As this chapter establishes coordinated policies for maintenance of the program, it is applicable to all organizations and activities under the purview of the Commander. References (a), (c), (d), and this Order will provide the basis for managing the II MEF Information Security Program.

5004. RESPONSIBILITY FOR COMPLIANCE

1. The Director of Security is responsible for compliance with and implementation of this Order.

2. Program Managers, Commanding Officers, and supervisors are responsible for compliance with and implementation of this Order within their areas of responsibility.

3. Each individual, military/civilian, or contractor, employed through the Navy or Marine Corps, is responsible for compliance with this Order in all respects.

4. All activities that hold classified information are required to be registered as a Secondary Control Point (SCP's) with the CMCC and have on-hand hard copies of the appropriate references and this Order.

a. Upon determination of transferring, retiring, resigning or being reassigned, SCPs will immediately notify the CMCC in order to coordinate a timely and efficient inventory and turnover of sub-custody material.

b. Newly assigned SCPs must be approved, assigned, and briefed by the CMCC prior to receiving any sub-custody material.

5. SCPs are responsible for the actions of all personnel assigned to them and those who may be in use of the classified material in their care.

5005. CMCC CUSTODIAN RESPONSIBILITIES

1. The CMCC Custodian is responsible for controlling classified material entering, leaving, or being created at II MEF.

2. Any expected in-bound classified material will be reported to the CMCC Custodian as soon as the project POC is aware of it.

a. Receive. The CMCC Custodian and Alternate Custodian are the only authorized recipients of classified Federal Express (FedEx), United States Postal Service (USPS), and Courier packages.

(1) Only the CMCC Custodian or Alternate will open these packages. If a package is received and is incorrectly issued to an unauthorized recipient, that recipient will proceed directly to the CMCC with the package and all wrappings.

(2) The CMCC Custodian will then verify the contents of the package matches the transmittal receipt and return the receipt to the sender.

b. Control Numbers. The CMCC Custodian will mark the classified material with a control number, attach SF-707 Secret Classification Sticker, if required, and will annotate all required information from the item(s) into the CMCC Database.

c. Dissemination. The CMCC Custodian will issue the classified material to the appropriate sub-custodian to include colored cover sheets as required.

(1) The SCPs is responsible for that classified material and will handle, store and use the material in accordance with all current policies and regulations. Any changes in the location, SCPs, project, or status of the classified material will be reported to the CMCC immediately. Secondary control points do not satisfy the procedural requirement for inbound or outbound classified material.

(2) When a file, folder, or group of classified documents are removed from secure storage, it must be conspicuously marked with the highest classification of any classified document it contains and have an appropriate classified document cover sheet attached.

(3) The only document cover sheets authorized for use by activities at II MEF are as follows:

(a) Top Secret, SF 703 - NSN 7540-01-213-7901

(b) Secret, SF 704 - NSN 7540-01-213-7902

(c) Confidential, SF 705 - NSN 7540-01-213-7903

d. Inventory. The CMCC Custodian manages the entire classified material inventory and requires all SCPs to conduct monthly inventories internally.

e. Safeguarding

(1) Security Management Physical Security Officer will conduct a annual inventory of General Services Administration (GSA) security containers to ensure their structural integrity and proper use.

(2) The CMCC Custodian will ensure all SCPs are trained on proper safeguarding requirements and that all updated policies and procedures are located in a public location for all users to review.

3. All classified material that is no longer needed for any reason will be turned into the CMCC Custodian for "DESTRUCTION." The CMCC Custodian will either destroy the material on site using approved methods. As soon as the CMCC Custodian officially takes custody of the material from the SCPs, the SCPs responsibility is relieved and the material will be removed from that SCPs inventory.

4. All classified material generated (to include working papers) at this Command must be properly portion marked with all classification markings required and controlled immediately after creation.

5. Classified material will only be signed out to individuals during day-to-day operations that utilize the material and who can account for its safe handling, storage, and protection when not in use.

6. Cross-domain transfer of documents from the high side, MCEN-S, to the low side, Non-Secure Internet Protocol Router Network, is authorized by the Data Transfer Agents (DTA). The DTA is responsible for the transfer of SIPRNet unclassified material and ensures that the material has been reviewed and certified to be transferred.

5006. TRANSFER OR TRANSMISSION OF CLASSIFIED MATERIAL

1. All classified material mailed via USPS Registered Mail will be received by the CMCC Custodian. The CMCC Custodian will coordinate with Supply and/or Mail Room for delivery of classified material packages to ensure complete control of the material.

a. If Supply or Mail Room notifies a person that a package has arrived and that user suspects the package contains classified materials, that Supply Clerk, Mail Clerk, or person must immediately notify the CMCC Custodian.

(1) If the Mail Clerk delivers a package to a person and upon opening the package, its contains classified information,

that individual, will immediately deliver the package with all wrappings and registered mail receipt to the CMCC Custodian.

(2) Do not tamper with the interior wrapper that identifies the package as classified material.

b. All classified material for transfer will be turned into the CMCC, no later than 1400 Monday through Friday, and will be shipped after receipt at the CMCC.

c. When informing anyone outside the Command to mail classified material by USPS to II MEF, the address provided below is to be used.

(1) The correct mailing address for FedEx and USPS containing classified information should read as follows:

Outer Envelope:

COMMANDING GENERAL II MEF
ATTN CMCC
1 Julian C. Smith St
Camp Lejuene NC 28542-0080

Inner Envelope:

POC/Project (on interior label only)
1 Julian C. Smith St
Camp Lejuene NC 28542-0080

(2) Never have the classified information mailed directly to an individual.

2. Transmission of NATO Classified Material

a. Requests to send NATO classified material to personnel or activities outside the Command will be processed via the NATO control point officer in the CMCC.

b. NATO information must be stored separately. It cannot be commingled with U.S. classified information.

c. Authority to hand-carry any NATO classified material outside CONUS, its territories or Canada, on commercial aircraft must be approved by HQMC. NATO Classified material must be packaged separately from other classified material and the inner envelope marked "NATO" along with the classification marking.

Only the activity address of the courier will be shown on the outer envelope or wrapping.

d. Transmission of COSMIC Top Secret is handled by the Security Office, and shall not be hand carried internationally. COSMIC TOP SECRET, NATO SECRET, all ATOMAL documents, and documents warranting special access controls must be transferred through the registry system, which includes foreign travel.

e. A continuous chain of receipts is required to record the movement of all COSMIC and NATO Secret material. The COMSEC Custodian will maintain receipts on COMSEC material. The CMCC custodian will maintain receipts on NATO.

3. The Director of Security will provide written authorization to individuals required to escort or hand-carry classified information. This authorization may be the DD 2501, Courier Authorization Card, included on official travel orders, or a courier authorization letter and is prepared by the Security Management Office. Any of these three written authorizations may be used to identify appropriately cleared DoD military and civilian personnel approved to escort or hand-carry classified information (*Special Access Program (SAP) and SCI information are excluded*) between DoD commands subject to the following conditions:

a. The individual has a recurrent need to escort or hand-carry classified information.

b. The expiration date may not exceed 3 years from the issue date (*pertains only to DD 2501*).

c. The individual must return the hand-carry written authorization to the Security Management Office upon transfer, termination of employment, or when authorization is no longer required.

4. The written authorization is intended for use between DoD commands worldwide and provides sufficient authorization to hand-carry classified information aboard a U.S. military aircraft.

5. Every precaution must be taken to prevent unauthorized disclosure when individuals are hand-carrying classified material in an official travel status.

6. If the movement requires transportation, the CMCC Custodian shall double wrap the classified material. A locked carrying-case or bag may be considered as the outer double wrapping, except when hand carrying aboard commercial aircraft.

7. II MEF personnel requiring a Courier Card must meet with the Security Management Office at least two (2) weeks prior to date of departure to complete the Courier Advisory Acknowledgement prior to being issued a Courier Letter or Courier Card and to ensure the classified package will be ready for pickup on date of departure.

a. It is mandatory for the Courier to check in with the CMCC prior to departure and immediately after returning from couriering classified information.

b. The Courier Card or Courier Letter must be returned to the Security Management Office upon expiration, upon departure from the command or upon completion of the mission in which the Courier Card or Letter was required.

8. Any request for COMSEC equipment or information coming into the Command or leaving the Command must be requested from the COMSEC Local Element Custodian.

9. Any classified material brought into this Command after hours, or when the CMCC Custodian or Alternate are unavailable, will be checked in with the Command Duty Officer (CDO) and stored appropriately in a secured room or security container until the material can be processed through the CMCC. The CDO will contact the CMCC Custodians of the material so it can be retrieved for proper storage and assignment, as required.

10. Classified information will not be discussed via telephone except as authorized on approved secure communication devices (i.e., Secure Telephone Equipment (STE)) and will not be transmitted via unapproved unclassified facsimile equipment.

5007. INSPECTIONS AND INVENTORIES

1. The Director of Security, with assistance from other security personnel, will conduct unannounced and random inspections of Level I and II Restricted Areas.

2. To insure that there is no introduction of prohibited items or contraband into Secure Working Areas or the CMCC, and to

deter the unauthorized removal of classified material the following is provided:

a. Prohibited items include personal or government equipment including:

(1) Laptops, computers, Personal Digital Assistant (PDA), and media.

(2) Photographic, video, and audio recording equipment.

(3) Two-way Radios, pagers, cellular telephones, and Personal Wearable Fitness Devices.

b. Contraband items are commonly defined as goods prohibited by law from being imported or exported. There are many different kinds of contraband, including homemade weapons, gambling paraphernalia, excessively metered envelopes, weapons, drugs, and food.

3. Containers containing classified material are subject to random and unannounced inspections. CMCC Custodian may require inventories and conduct the inventory at any time.

5008. REPRODUCTION

1. All classified information will be printed on colored paper. All Secret information will be printed on pink paper. All TS/SCI information will be printed on yellow paper. This does not preclude the individual from properly marking all classified information.

2. Reproduction of classified information must be accounted for with the SCPs and CMCC within II MEF.

3. Classified information will only be reproduced to the extent required for operational necessity unless restricted by the originating agency or for compliance with applicable statutes or directives.

5009. CLASSIFIED MEETINGS AND BRIEFINGS

1. Classified meetings or briefings will be coordinated by the II MEF Host, as directed by reference (i), with II MEF Security Management Office.

2. Personnel inviting guests from other organizations are required to notify Security via the visitor processes (whichever applies) to ensure proper vetting can be completed prior to guests arrival.

3. Foreign visitors. A foreign visit is any contact by a foreign national or foreign representative that involves substantive or technical discussions or information. Avoid entering into these types of discussions with foreign persons or their representatives on initiatives that will result in the disclosure of classified information or CUI without first obtaining approval as explained in reference (i).

a. If an email, phone, or letter is received requesting information or visit to II MEF the only reply to make is that their request is passed to the II MEF Foreign Disclosure Officer (FDO) for action.

b. For all requests for foreign official visits will be submitted through the sponsoring government's Embassy as indicated in reference (i).

c. Foreign national visitors who are not sponsored by a foreign government or international organization are "unofficial visitors." Security and FDO will comply with reference (i). If the "unofficial visitor" is approved to visit, their access to information at II MEF facilities is limited to that which is in the public domain only.

4. All classified notes will be turned into the meeting host at the end of the meeting along with the person's name, phone number, and organization's mailing address. The meeting host at the end of the meeting will enclose all the classified notes within a carrying case and deliver to the CMCC Custodian prior to that person's departure and for mailing to his/her security office, if necessary.

5. Personal Electronic Device (PED)

a. It is the responsibility of II MEF personnel hosting/sponsoring an Classified Meetings to inform their visitors of the II MEF Personal Electronic Device (PED) Policy.

b. PEDs in restricted areas are not authorized and it is recommended that personnel leave their PEDs in their locked vehicles or, if available, locked within lockboxes located near the meeting room.

5010. PRINTING FROM MCEN-S COMPUTERS

1. Personnel utilizing their MCEN-S accounts within II MEF facilities have printing permissions and are required to coordinate with their SCP or CMCC to document holdings.

a. The MCEN-S user has to understand that they will apply all requirements listed in the Marking Classified National Security Information booklet and reference (a) Volume 2 prior to request to printing.

b. The marking booklet is available on the II MEF Security Management Office SharePoint page.

2. Marking is required on all information technology (IT) systems and electronic media, including removable components that contain classified information.

a. IT systems include any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.

b. Electronic media includes Universal Serial Bus drives; flash drives, pen drives, compact disks, and etc. are not authorized on MCEN-S equipment.

c. IT systems that process classified data, in forms other than traditional documents, such as weapons, navigation, and communication systems also require appropriate marking.

d. Every MCEN-S user is responsible for derivatively marking any classified or controlled unclassified document for printing to include clearly annotated classification markings on the top and bottom of each page and paragraph/portion marking. Use page numbers (example: page 1 of 5, 2 of 5, etc.) to ensure full document accountability.

e. All classified working papers will be controlled, logged in the Working Papers Logbook, maintained by the CMCC Custodian and only up to 180 days, and then turned into the CMCC for destruction or processed as a classified document. It is strongly encouraged that working papers be maintained for the minimum amount of time necessary.

5011. DISCOVERY OF SUSPECTED CLASSIFIED DATA FOUND ADRIFT. Any materials discovered by II MEF personnel that are unlabeled, unknown, or potentially classified will be turned into the CMCC Custodian for immediate investigation/destruction.

5012. SHREDDER REQUIREMENTS

1. All paper material will be shredded.

2. The National Security Agency (NSA) product list of approved crosscut shredders for destruction of classified information is located on the II MEF Security Management Office SharePoint website (for collateral). The CMCC Custodian, Alternate CMCC Custodian, or SSO will approve prior to classified shredding within II MEF.

3. CMCC Custodian and SSO will use a NSA approved crosscut shredder that will reduce the information to shreds no greater than five square millimeters.

4. Strip shredders are not authorized for the destruction of classified information.

5. Destruction of unclassified sensitive data and Controlled Unclassified Information documents will be destroyed by utilizing a strip or crosscut shredder.

5013. WORKING PAPERS. Classified (Secret, Confidential) Working Papers are documents and material accumulated or created in the preparation of a deliverable, i.e. meeting notes, draft documents, and draft PowerPoint presentations. Working papers are marked in the same manner as a finished document at all times. All working papers will be reviewed by the Security Management Office for proper markings before being released by the originator outside the originating command.

1. Working papers that contain Top Secret or SAP information must be generated and maintained inside the SCIF. These documents will be properly marked, centered top and bottom, with the highest overall classification along with the words "Working Paper" on each page. These documents will be properly accounted for within the SCIF by the SSO.

2. All Secret and Confidential material held by the Command will be logged into the CMCC and accounted for. The one

exception is the classified information maintained on the SIPR server.

3. Working papers will be maintained for less than 180 days or filed permanently.

Chapter 6

INDUSTRIAL SECURITY

6001. GENERAL. The National Industrial Security Program (NISP) was established to safeguard classified information that is released to industry to ensure the protection is maintained as required by E.O. 12829.

6002. RESPONSIBILITIES

1. As required by references (a) through (e), Program Managers and supervisors, identified as host activities in this chapter, will establish procedures as outlined in this chapter that includes appropriate guidance, consistent with reference (e) and this manual, to ensure that classified information released to industry is safeguarded.

2. The host activity, via the Director of Security, may deny access, to contract employees, to areas and information under their control for cause.

a. Suspension or revocation of contractor security clearances can only be affected through the Department of Defense Consolidated Adjudication Facility-Industry Division.

b. Any actions taken to deny a contractor access to areas and information will be reported to the Contracting Officer Representative (COR). If SCI access is of concern, a report will also be forwarded to the SSO.

3. Contractors are required to have either a final or interim security clearance, in order to have access to classified information at II MEF. In addition, contractors granted access to classified COMSEC or NATO material must hold a FINAL security clearance for the level of classification involved.

4. Responsibility for initiating and submitting the request for a security investigation to the NBIB in support of classified access, lies with the contractor's parent company/facility. This includes requests for initial security investigations and periodic reinvestigations.

6003. ACCESS. DoD Contractors will perform work within II MEF in one of the following ways:

1. When a contractor is determined as a short or long-term

visitor, the DoD Contractor must comply with II MEF security regulations and shall be included in the II MEF security education program.

2. When the contractor has a tenant seat within II MEF spaces, i.e., has sole occupancy of a space that is controlled and occupied by the contractor, the host activity shall assume responsibility for security oversight over classified work carried out by the cleared DoD contractor employees in their area. The host activity is responsible for all security aspects of the contractor's operations in the work area and within the Command's area of responsibility.

6004. CHECK-IN. Prior to any DoD contractor reporting aboard for a dedicated seat assignment, the Contracting Officer will coordinate with the II MEF Security Management Office with the appropriate documentation required.

6005. ESCORTING PRIVILEGES. Only DoD civilian and military personnel whose principal place of work is within II MEF are authorized to escort visitors and contractor personnel within II MEF areas.

1. Individuals must be thoroughly briefed in their responsibilities as an escort prior to performing the duty. Members of the Security Management Office conduct this training.

2. Escorts will announce that a visitor is in the area so that co-workers can turn over, cover, or store controlled unclassified material.

3. Escorts will walk with the individual under escort; and visually observe the individual under escort until the visitor leaves II MEF or another escort assumes the duty.

4. Waivers to escort policy and procedures may be granted by the Director of Security or designee on a case-by-case basis.

6006. CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD FORM 254). The host activity shall ensure that a DD Form 254 is incorporated into each contract that is handling classified information or material. The DD Form 254 is a legal document and part of the contract.

1. The DD Form 254, with its attachments, supplements, and incorporated references, is designed to provide a contractor with the security requirements and classification guidance

needed for performance of a classified contract.

2. An original DD Form 254 will be issued with each request for proposal, other solicitations, contract award, or follow-on contract to ensure that the prospective contractor is aware of the security requirements and can plan accordingly.

3. A Follow-On contract is a contract that is awarded to the same contractor for the same item or services as a preceding contract. A revised DD Form 254 will indicate the new contract number, this authorizes the contractor to transfer material received or generated under the preceding contract to the new contract.

4. A revised DD Form 254 will be issued as necessary during the life of the contract when security requirements change.

5. A final DD Form 254 will be issued only if the contractor requests, in writing, an extension for classified material retention for an extended period after the contract period of performance, i.e., 2 years.

6. The DD Form 254 shall be periodically reviewed during the performance stages of the contract and a revised DD Form 254 issued if needed.

6007. COMMON ACCESS CARD (CAC)

1. Per reference (i), contractors who require access to the Marine Corps Enterprise Network (MCEN) account must meet the minimum investigation requirement of NACI prior to CAC issuance.

2. When it has been determined that a contractor does not meet the minimum investigative requirements per HSPD-12, the host activities will ensure DoD Contractors submit a Public Trust Positions Security Questionnaire, Standard Form (SF-85) to the Personnel Security Office. The Personnel Security Office will coordinate the remaining aspects of the investigation submission and fingerprints.

3. A CAC will be issued when the investigation questionnaire has been submitted to NBIB for processing and fingerprint results have returned favorably. If the investigation does not return favorably, the CAC must be retrieved and revoked.

6008. CHECK-OUT/DEBRIEFINGS. All contractors assigned to II MEF, must checkout with the Security Office when leaving the Command.

1. Contractors who had access to classified information must be debriefed by their respective host activity.

2. Contractors will surrender all government issued property to the II MEF Security Office (i.e. DoD Badge, CAC, building access badge).

3. Contractors who have MCEN-S Tokens will surrender them directly to the II MEF/G-6.

Chapter 7

EMERGENCY ACTION PLANS FOR CLASSIFIED MATERIAL

7001. GENERAL. The provision of this section, as directed by reference (c), relates to the emergency action to be taken to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of compromise, and for the recovery of classified information, if necessary, following such events.

7002. BASIC POLICY. All activities of II MEF that handle and store classified information, equipment, or data will write and execute an Emergency Action Plan (EAP).

7003. RESPONSIBILITY. The Director of Security is responsible to ensure that all activities that are handling and storing classified information, equipment, or data execute an EAP and an approved copy is maintained within the CMCC.

1. CMCC Custodians. Will coordinate with each of the sub-custodians to ensure that each secondary control point and restricted area has: an EAP on file, that appropriate drills are conducted, reports maintained on file, and copies of all reports are provided to the Command Inspector.

2. Physical Security Officer. Will provide guidance to the CMCC Custodian and SCPs on what is contained within an EAP regarding physical security issues.

7004. DEVELOPMENT OF AN EAP

1. It is essential that the EAP developed be site specific with respect to emergency conditions evaluated, evacuation policies and procedures, emergency reporting mechanisms, and alarm systems.

2. After the EAP has been developed and approved, the Secondary Control Point Custodians will review it with their military, civilian and contractor personnel to ensure they know what to do before, during, and after an emergency.

3. Keep a copy of the EAP in a convenient location where it is readily accessible, or provide a copy to all personnel.

Chapter 8

PHYSICAL SECURITY

8001. GENERAL. As established in reference (g), II MEF is required to provide physical safeguards for all Command personnel, information, and assets to deter from various undesirable events such as attacks, theft, sabotage, and espionage. These safeguards will be provided through various active and passive barriers, supplemental controls, and operating procedures. In all cases, implementation of these safeguards will be taken to ensure they are complementary to the installation safeguards and provide a layered approach to achieve security-in-depth.

8002. BADGING AND BUILDING ACCESS ORDER. Reference (i) provides the policy, eligibility, and procedural requirements to obtain badge access and visitor authorization (classified and unclassified) for all government, military, contractor, and foreign personnel required or requesting to gain entry into Command areas protected by access control measures. Access control is driven by the requirement for accountability and control of government information and facilities. Access to command spaces are strictly controlled to protect our workforce, information, and assets.

8003. STORAGE REQUIREMENTS. References (c) and (g) provide the basic policy and requirements for the storage and physical protection of classified information. All classified information will be properly stored within a properly accredited restricted area or security container when not in use. Standard Form (SF) 701, Activity Security Checklist and SF 702, Security Container Check Sheet, will be used to record the activities and securing of restricted areas and security containers. The SF 700, Security Container Information, will be maintained by the organizational CMCC for all restricted areas and security containers. II MEF Command Element may maintain internal security container SF 700s following coordination with the CMCC. All units and sections will be randomly inspected for proper use of SF 700s, 701s, and 702s by the CMCC or security staff. The Camp Lejeune Physical Security Office will also conduct physical security surveys annually on all restricted areas.

II MEF SECURITY MANUAL

Chapter 9

NAVAL CRIMINAL INVESTIGATION SERVICE (NCIS)

9001. BASIC POLICY

1. Certain matters affecting National Security must be reported to the Resident Agent, NCIS (RA NCIS) Camp Lejeune. The Director of Security will coordinate security related reporting to the RA NCIS.

2. All II MEF military and civilian personnel, whether they have access to classified information or not, will report to the Director of Security, any activities described below involving themselves, their immediate relatives, co-workers or others:

a. Sabotage, Espionage, International Terrorism, or Deliberate Compromise of Classified Material.

b. Known individuals with, or without clearance eligibility seeking illegal access to classified materials.

c. Personnel who have access to classified information who commit or attempt to commit suicide.

d. Unauthorized absentees who have access to classified information.

e. The death or desertion of a DON person who has access to classified information.

3. The Director of Security will immediately notify the RA NCIS Lejeune.

9002. FOREIGN TRAVEL. Foreign Travel briefings are normally provided by a RA NCIS, MCB Lejeune prior to travel to certain overseas locations.

9003. COUNTERINTELLIGENCE BRIEFING. NCIS agent will conduct annual Counterintelligence briefings for all civilian employees and military members as required by reference (f).