



UNITED STATES MARINE CORPS

I MARINE EXPEDITIONARY FORCE, FMF
BOX 555300
CAMP PENDLETON, CALIFORNIA 92055-5300

I MEFO P5510.1D
SECMAN

NOV 18 2009

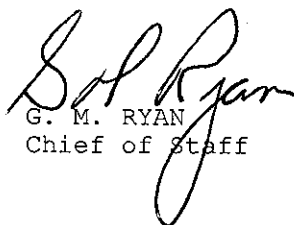
I MARINE EXPEDITIONARY FORCE ORDER P5510.1D

From: Commanding General
To: Distribution List

Subj: I MARINE EXPEDITIONARY FORCE INFORMATION AND PERSONNEL SECURITY
PROGRAM (SHORT TITLE: IMEF IPSP)

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCO P5510.18A

1. Situation. To issue procedures and guidance for the I Marine Expeditionary Force Information and Personnel Security Program (IPSP) to be in compliance with references (a) through (c) and to achieve uniform implementation of the IPSP throughout I MEF's Major Subordinate Commands (MSCs)
2. Cancellation. I MEFO P5510.1C and 5510.5C
3. Mission. This Order is effective upon receipt and all supervisory personnel will ensure strict compliance with its guidelines. Should any portions of this manual conflict with the directives of higher headquarters the latter will apply.
4. Execution. Recommendations concerning the contents of this manual are invited but shall be directed towards the Command Security Manager, I Marine Expeditionary Force.
5. Administration and Logistics. This manual has been rewritten to better address the unique security requirements of this command and ensure complete compliance with references (a) through (c). This order should be reviewed in its entirety.
6. Command and Signal. This order is applicable to the entire I MEF Total Force.


G. M. RYAN
Chief of Staff

Distribution List: I/II

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 1

INTRODUCTION

| | PARAGRAPH | PAGE |
|--------------------------------------|-----------|------|
| PURPOSE | 1000 | 1-2 |
| APPLICABILITY | 1001 | 1-2 |
| GUIDANCE | 1002 | 1-2 |
| OBJECTIVES | 1003 | 1-2 |
| COMBAT OPERATIONS | 1004 | 1-3 |
| WAIVERS AND EXCEPTIONS | 1005 | 1-3 |
| INSPECTIONS BY SENIOR COMMANDS | 1006 | 1-3 |
| PREPARATION FOR DEPLOYMENTS | 1007 | 1-3 |
| VIOLATIONS OF THIS ORDER | 1008 | 1-4 |

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 1

INTRODUCTION

1000. PURPOSE

1. This order provides information and instruction pertaining to the administration and implementation of the Department of the Navy (DoN) Information and Personnel Security Program (IPSP) within the I Marine Expeditionary Force (MEF) and guidance to subordinate commands.
2. It is paramount that all personnel engaged in administering the security of classified information preserve an objective point of view and opinion. The ideal result is the indoctrination and education of all personnel to the point that they automatically exercise discretion as it pertains to security in the discharge of their duties.
3. This order serves as a supplement to references (a), (b), and (c) and must be used in conjunction with those manuals to be effective.
4. This order is also intended to serve as an example for subordinate commands in establishing their Command Security Program.

1001. APPLICABILITY. This order applies to all Departments of the Navy Personnel, to include reserve and civilian personnel within the I MEF Command Element. All command personnel are individually responsible for compliance with this order.

1002. GUIDANCE. Command personnel are encouraged to contact the Command Security Manager to obtain guidance or interpretation of this order and the references.

1003. OBJECTIVES

1. Prevent and/or minimize the risk of unauthorized personnel from gaining access to Classified Military Information (CMI).
2. Provide sound management principles for the security of classified information.
3. Outline the I MEF Security Chain of Command.
4. Describe the security organization and identify positions.
5. Describe procedures for internal and subordinate security reviews and inspections.
6. Outline the internal procedures for reporting and investigating loss, compromise, and other security discrepancies.
7. Outline the I MEF IPSP Security Education Program.
8. Establish a Security Education Program to familiarize all I MEF

I MARINE EXPEDITIONARY FORCE IPSP

personnel with the regulations and procedures that have been established to safeguard classified information.

9. Establish command visitor control procedures to accommodate visits to the command involving access to or disclosure of classified information.

10. Establish procedures for the review of classified information prepared in the command to ensure correct classification and marking. Identify the sources of security classification guidance commonly used, and where they are located.

11. Establish destruction procedures for classified material held within the command.

12. Define the Emergency Action Plan for classified material.

13. Develop an Industrial Security Program for civilian contractors working within the command element.

1004. COMBAT OPERATIONS. Commanding Officers may modify the safeguarding requirements of this regulation and the listed references as necessary to meet local conditions during combat or combat-related operations. Even under these circumstances, the provisions of this order shall be followed as closely as possible. This exception does not apply to scheduled training or exercises.

1005. WAIVERS AND EXCEPTIONS

1. When fulfilling the requirements of this order result in an untenable sacrifice of operating efficiency, or when there are other good and sufficient reasons, a waiver of a specific requirement may be requested from the Chief of Naval Operations (N09N2) via CMC (ARS).

2. All waivers and exceptions shall be presented to the Command Security Manager with sufficient information and justification. Waivers must be endorsed by the Commanding General, Deputy Commanding General, or the Chief of Staff before they can be submitted to CMC (ARS).

1006. INSPECTIONS BY SENIOR COMMANDS

1. This command is inspected annually by the Commander, Marine Corps Forces, Pacific (COMMARFORPAC) Security Manager.

2. The Commandant of the Marine Corps (CMC), Administration and Resource Management Division, Headquarters Administrative Security Branch (ARS) will from time to time conduct an Inspection General review or an Assist Visit of this commands Information and Personnel Security Program.

1007. PREPARATION FOR DEPLOYMENTS.

1. This command, to include all subordinate commands, is required to ensure that forward and rear elements have sufficient staffing to manage the

I MARINE EXPEDITIONARY FORCE IPSP

Information and Personnel Security Programs. The commands security program is one of the essential parts for a unit's deployment. Failure to assign and train personnel to manage the commands security program will only lead to significant gaps in the units overall security posture.

1008. VIOLATIONS OF THIS ORDER

1. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice (UCMJ), or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this order.

3. Civilian employees are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this order.

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 2

COMMAND SECURITY MANAGEMENT

| | PARAGRAPH | PAGE |
|--|-----------|------|
| BASIC POLICY | 2000 | 2-2 |
| COMMANDING GENERAL | 2001 | 2-2 |
| SECURITY MANAGER | 2002 | 2-2 |
| DUTIES OF THE SECURITY MANAGER | 2003 | 2-3 |
| TOP SECRET CONTROL OFFICER | 2004 | 2-4 |
| SECURITY OFFICER | 2005 | 2-4 |
| ASSISTANT SECURITY PERSONNEL | 2006 | 2-4 |
| INFORMATION ASSURANCE MANAGER | 2007 | 2-5 |
| ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) MANAGER | 2008 | 2-5 |
| SPECIAL SECURITY OFFICER | 2009 | 2-5 |
| SECTION SECURITY REPRESENTATIVE | 2010 | 2-5 |
| SECURITY SERVICING AGREEMENT | 2011 | 2-6 |
| INSPECTIONS, ASSIST VISITS AND REVIEWS | 2012 | 2-6 |

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. BASIC POLICY. The effectiveness of the commands security program is dependent on the importance given it and the personnel appointed to fill the requirements outlined in this order.

2001. COMMANDING GENERAL

1. Program management consists of the designation of security officials working together to ensuring compliance with the command IPSP to fulfill the Commanding General's responsibilities.
2. Commanding General's responsibilities include:
 - a. Designating a Security Manager in writing.
 - b. Designating a Top Secret Control Officer (TSCO) in writing.
 - c. Designating a security officer in writing to manage physical security matters.
 - d. Designating an Information Assurance Manager in writing.
 - e. Ensure the command has an established Information and Personnel Security Program (IPSP), and that it is reviewed annually to ensure compliance with any new Department of Defense (DoD), Department of Navy (DoN), and Headquarters Marine Corps (ARS) security regulations, manuals and policies.
 - f. Designate a Special Security Officer (SSO) to administer the command Sensitive Compartmented Information (SCI) security program.
 - g. Ensuring that all security official appointment letters are kept on file.
 - h. Ensuring that the Security Manager and other command security officials are appropriately trained and understand their duties.
 - i. Ensuring the command has a robust security awareness program that is administered annually.
 - j. Establishing an emergency action plan for the protection and possible destruction of classified material.
 - k. Ensuring that the command Security Manager conducts inspections, program reviews, and assist visits of subordinate commands annually.
 - l. Establishing an industrial security program.

2002. SECURITY MANAGER.

1. The Commanding General shall appoint, in writing, a command Security Manager. This individual shall be identified to all members of the command and added to organizational charts, telephone listings, rosters, etc.

I MARINE EXPEDITIONARY FORCE IPSP

2. The I Marine Expeditionary Force Command Security Manager must be an officer or a GS-11 civilian employee or higher. This individual must meet all qualification requirements outlined in references (a), (b) and (c).
3. The Security Manager will be afforded direct access to the commanding officer as outlined in references (a), (b), and (c) to ensure effective management of the command IPSP.
4. The Security Manager shall be provided with sufficient personnel and office space to effectively run and manage the command IPSP.

2003. DUTIES OF THE SECURITY MANAGER.

1. The principal advisor concerning information and personnel security matters to the Commanding General.
2. Responsible for the written development and management of the Command IPSP.
3. Responsible for the written development of a desktop standard operating procedure manual for the Security Manager's office to address the internal administrative security responsibilities.
4. Formulates and coordinates the commands annual security awareness and education program to include scheduling a mobile security training team to Camp Pendleton in conjunction with the base Security Manager.
5. Development of the commands visitor control program concerning access to classified information and the submission of visit certifications to other commands, agencies and organizations.
6. Ensure all personnel who possess access to classified or who wish to submit clearance packages have the appropriate need to know and qualifications. This includes keeping records of all clearance packages submitted.
7. Execute continuous evaluation of personnel eligibility for access to classified information and maintain record of all those who possess a clearance and level of clearance they have been granted.
8. Maintain liaison with the Command Special Security Office concerning information and personnel security policies and procedures.
9. Ensure that all personnel that leave the command due to retirement, separation, or relieved for cause per reference (a) have completed a security termination statement.
10. Retain record of all security appointment records and review quarterly to identify any changes to the personnel that have been previously appointed.
11. Ensure all personnel execute a Non-disclosure Agreement (SF-312) prior to granting access and that all originals are forwarded to HQMC at the address listed in reference (a) and that a copy be retained on file.

I MARINE EXPEDITIONARY FORCE IPSP

12. Perform site assist visits, inspections and reviews for subordinate commands annually and that these inspections, assist visits and reviews are recorded and retained for official record for no less than two years.

13. Make certain that immediate action is taken concerning all security violation reports and possible compromises within the command and that adequate records are kept concerning all preliminary investigations and JAGMAN investigations.

14. Coordinate with the information assurance manager common security concerns and develop policies that address security vulnerabilities.

15. Ensure that only those with the appropriate "Need to Know" have sufficient access to classified military information.

16. Development of the command industrial security program.

2004. TOP SECRET CONTROL OFFICER (TSCO).

1. The Commanding General will appoint, in writing, a Top Secret Control Officer to manage the commands Top Secret Control Program.

2. The TSCO must be a military member, E-7 or above, or civilian employee, GS-7 or higher.

3. The TSCO must be a U.S. citizen and be the subject of a completed Single Scope Background Investigation (SSBI/SBPR) in the last 5 years.

4. All standard duties required of the TSCO are outlined in reference (b) chapter 2, and chapter 4 of this order.

5. Within this command the TSCO will ensure that all Top Secret Material accounted for annually and perform all obligation of a TSCO as outlined in reference (b).

6. The Security Manager may be appointed as the TSCO as the position does not conflict with his/her duties.

2005. SECURITY OFFICER

1. The Commanding General will appoint in writing a Security Officer to manage the commands physical security program.

2. The primary function of this billet is to work in conjunction with the Security Manager and the base Provost Marshalls Office, Physical Security Officer to ensure the command is adhering to reference (b).

3. If one is not appointed the duties will fall to the Security Manager.

2006. ASSISTANT SECURITY PERSONNEL. The Chief of Staff may elect to appoint additional assistant security personnel to properly staff the command Security Manager's office as necessary.

1. Assistant Security Manager (ASM). The Assistant Security Manager, if assigned, must be a U.S. citizen, either a Staff Sergeant (E-6) or above, or a federal civilian employee of equal level. The designation of the

I MARINE EXPEDITIONARY FORCE IPSP

individual will be in writing. The Assistant Security Manager must be subject of a favorably adjudicated Single Scope Background Investigation (SSBI). The Assistant Security Manager will provide guidance to the Security Manager and perform the duties of the Security Manager in his absence.

2. Security Assistant. The security assistant, if assigned, must be a U.S. citizen, military or federal civilian employee and subject of a favorably adjudicated National Agency Check with Local Agency Checks and Credit Check (NACLC). Rank is not of importance to the billet. Security assistants will perform routine administrative duties of the office.

2007. INFORMATION ASSURANCE MANAGER (IAM). The IAM is responsible for the development, and implementation of a security program to protect, safeguard, and track all command information assurance (IA) matters.

2008. ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) MANAGER. The Commanding General shall point in writing an EKMS manager who shall serve as the principal advisor in all matters regarding the Communication Material System (CMS).

2009. SPECIAL SECURITY OFFICER (SSO)

1. The Senior Intelligence office (SIO) will appoint in writing a Special Security Officer (SSO) to manage the commands Sensitive Compartmented Information (SCI) facilities (SCIF) and program.

2. The SSO must be a U.S. citizen and either a commissioned officer or a civilian employee GS-9 or above, and possess a clearance of TS/SCI.

2010. SECTION SECURITY REPRESENTATIVE (SSR)

1. Section Security Representative (SSR): Each section that retains and accesses classified material shall appoint in writing a SNCO or Officer as a Section Security Representative. An Assistant Section Security Representative (ASSR) may also be assigned as needed.

2. The SSR shall at a minimum:

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

b. Report all security related concerns and violations they identify both within their section and other sections to the Command Security Manager immediately.

c. Maintain a system of accountability for all classified material, in the sections possession, that has been identified as accountable products.

d. Manage all GSA approved security containers, vaults, and secure rooms utilized by their respective section. This includes changing combinations as required per reference (b) and the keeping a listing of all safes and their specific location.

I MARINE EXPEDITIONARY FORCE IPSP

2011. SECURITY SEVICING AGREEMENT (SSA)

1. This command may establish Security Service Agreement (SSA) with other commands in accordance with references (c). Such agreements may be appropriate in situations where security, economy, and efficiency are considerations.

2. The SSA shall be specific and clearly define the security responsibilities being relinquished and absorbed.

2012. INSPECTIONS, ASSIST VISITS, AND REVIEWS

1. The Security Manager will perform inspections, assist visits and reviews of subordinate commands annually in accordance with reference (a), (b) and (c).

2. The Security Manager will also participate and support the commands IGMC upon request.

4. The Security Manager will execute internal security inspections of command Principle and Special Staff sections.

3. Chapter 5 of this manual outlines all aspects of this commands subordinate command inspection program.

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 3

PERSONNEL SECURITY

| | PARAGRAPH | PAGE |
|---|-----------|------|
| BASIC POLICY | 3000 | 3-3 |
| DIRECTOR, DEPARTMENT OF THE NAVY CENTRAL ADJUDICATION FACILITY | 3001 | 3-3 |
| OFFICE OF PERSONNEL MANAGEMENT | 3002 | 3-3 |
| ACCESS TO CLASSIFIED INFORMATION | 3003 | 3-3 |
| DEFINITION OF NEED TO KNOW | 3004 | 3-4 |
| JOINT PERSONNEL ADJUDICATION SYSTEM | 3005 | 3-4 |
| PERSONNEL SECURITY INVESTIGATIONS (PSI) | 3006 | 3-4 |
| PERIODIC REINVESTIGATIONS (PR) | 3007 | 3-5 |
| PSI REQUEST REQUIREMENTS | 3008 | 3-5 |
| APPLICANT SCREENING | 3009 | 3-6 |
| SUBMISSION OF PSI'S | 3010 | 3-6 |
| TEMPORARY ACCESS (INTERIM CLEARANCE) | 3011 | 3-6 |
| INDOCTRINATION | 3012 | 3-7 |
| AUTHORIZED SECURITY ACCESS BADGES | 3013 | 3-8 |
| PERSONNEL SECURITY FILES (PSF) | 3014 | 3-8 |
| DEBRIEFING | 3015 | 3-8 |
| UNFAVORABLE SECURITY DETERMINATIONS | 3016 | 3-9 |
| NO DETERMINATION MADE | 3017 | 3-9 |
| LETTER OF INTENT (LOI) | 3018 | 3-10 |
| LETTER OF DENIAL (LOD) | 3019 | 3-10 |
| APPEALING A DENIED OR REVOKED SECURITY CLEARANCE ... | 3020 | 3-11 |
| DUAL CITIZENSHIP | 3021 | 3-12 |
| VISITOR CONTROL | 3022 | 3-12 |
| SECURITY EDUCATION | 3023 | 3-13 |
| COUNTER INTELLIGENCE MATTERS | 3024 | 3-13 |

I MARINE EXPEDITIONARY FORCE IPSP

| | | |
|--|------|------|
| REPORTING DEROGATORY INFORMATION | 3025 | 3-14 |
| ACCESS SUSPENSION | 3026 | 3-14 |

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 3

PERSONNEL SECURITY

3000. BASIC POLICY

1. The Commanding Officer is ultimately responsible for the commands Personnel Security Program (PSP).
2. The Command Security Manager is responsible for developing and administering the personnel security program.
3. No individual will be given access to classified information or assigned to sensitive duties unless a favorable personnel security determination has been made regarding their loyalty, reliability, and trustworthiness. In the absence of adverse information, commanding officers may grant temporary access (also referred to as interim clearance) to individuals pending completion of full investigative requirements and pending establishment of security clearance eligibility by the DONCAF.
4. U.S. citizenship is a basic condition for access to classified information and assignment to a sensitive national security position.
5. Access to classified information will be formally terminated when it is no longer required in the performance of assigned DON duties and/or when the individual's security clearance eligibility is denied or revoked.

3001. DIRECTOR, DEPARTMENT OF NAVY CENTRAL ADJUDICATION FACILITY. The Department of Navy Central Adjudication Facility (DoNCAF) is the personnel security adjudicative determination authority for all individuals affiliated with the DON.

3002. OFFICE OF PERSONNEL MANAGEMENT. The Office of personnel Management (OPM) is responsible for oversight and implementation of EO 10450, which prescribes security requirements (including investigations) for federal government employment. Additionally, OPM is the single provider of personnel security investigative products for the Department of Defense.

3003. ACCESS TO CLASSIFIED INFORMATION.

1. The Commanding Officer retains the authority to grant or deny access to classified military information.
2. No one has the right to access classified military information solely because of rank, position, or security clearance. Commands must show discretion before granting access and establish a need to know.
3. Access to classified information will be granted only if allowing access will promote the furtherance of the commands mission while preserving the interests of national security.

I MARINE EXPEDITIONARY FORCE IPSP

3004. DEFINITION OF "NEED-TO-KNOW"

1. Access to classified information is not authorized by the favorable conclusion of a clearance eligibility determination. Access is only permitted to eligible individuals after determining that the individual has sufficient need to access classified information to accomplish command mission and operational objectives.
2. Need-to-know is a determination that an individual requires access to specific classified information in the performance of (or assist in the performance of) lawful and authorized government functions and duties.
3. Need-to-know is one of two information points that must be determined by every authorized holder of classified information prior to relinquishing classified information to a prospective recipient. Clearance eligibility is the second.

3005. JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

1. The Joint Personnel Adjudication System (JPAS) is the automated system of record for personnel security management within the DoD, providing a means to record and document personnel security actions. JPAS facilitates personnel security program (PSP) management for the DoD Central Adjudication Facilities (CAF's), for DoD security managers, and SCI program managers. JPAS interfaces with the Defense Security Service (DSS) and the OPM to provide Personnel Security Information (PSI) data, and the various DoD personnel systems to include the Defense Enrollment Eligibility Reporting System (DEERS) and Defense Civilian Personnel Data System (DCPDS) to provide personnel identifying data.
2. The Command Security Manager is ultimately responsible for the management of the commands JPAS account.
3. The JPAS account is identified by a Security Management Office (SMO) code. The SMO code is 201464.
4. JPAS is the system that controls the initiation and electronic submission of all security investigations.
5. Use of JPAS is absolutely mandatory for all DoD services. Further guidance concerning JPAS can be found in reference (a), appendix E and at www.navysecurity.navy.mil.

3006. PERSONNEL SECURITY INVESTIGATIONS (PSI)

1. National Agency Check with Local Agency and Credit Check (NACLC) is the investigation used to determine SECRET eligibility. This investigation requires 7 years of information for initial and periodic reinvestigation (PR) submissions. This investigation is good for 10 years from the date of investigation, also referred to as the closed date of the investigation.
2. Single Scope Background Investigation (SSBI) is the investigation used to determine TOP SECRET and SCI eligibility. This investigation requires 10 years of information for initial submissions and 7 years for PR submissions.

I MARINE EXPEDITIONARY FORCE IPSP

This investigation is good for 5 years from the date of investigation, also referred to as the closed date of the investigation.

3. A new investigation is required upon reentry of officers and enlisted personnel if there has been a break in active service greater than 24 months.

4. Further information concerning security investigations can be found in reference (a), chapter 6.

3007. PERIODIC REINVESTIGATION (PR).

1. Periodic Reinvestigations (PR) are submitted to update a previous investigation. There are two scopes for Periodic Reinvestigations, the SSBI-PR for Top Secret/SCI, and the NACLIC for Secret. The PR due date is based on the closed/investigation date of previous investigation.

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

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

4. 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 by this command. If access is suspended the submission of a PR will be required before access can be reinstated.

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

6. The Command Security Manager must 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 Command Security manager will contact personnel monthly.

7. The individual is ultimately responsible for the submission of their periodic reinvestigation. The PR due date can be obtained from the command security manager.

3008. PSI REQUEST REQUIREMENTS

1. In accordance with references (a) and (c) personnel who require access to classified military information must be thoroughly screened to ensure they qualify for a U.S. security clearance.

2. Need-to-know must be established to ensure that security clearances are only being processed for personnel who have a valid need to access classified military information.

2. The Command Security Manager's office and the SSO are the only two offices of this command element that are authorized to screen applicants and process security investigations.

I MARINE EXPEDITIONARY FORCE IPSP

3009. APPLICANT SCREENING

1. The following must be accomplished by all command permanent and temporarily assigned personnel.

a. Request for Access Form: A local form provided by the command security manager's office used to validate individuals access requirement/need-to-know. This form lists required personal information on the applicant such as Social Security Number, full name, date of birth, place of birth, billet description and the level of access required for the billet. This form requires the signature of an officer or staff noncommissioned officer in authority over the individual. Personnel that require Top Secret access require the signature of an LtCol/O5 or higher. Only command indoctrinated personnel can sign off on the request for access form.

b. Screening Questionnaire: Personnel shall fill out a screening questionnaire provided by the security manager's office. The questionnaire is used to 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.

c. Citizenship of all applicants must be verified. Only U.S. citizens qualify for a security clearance.

3010. SUBMISSION OF PSI

1. Personnel who have been found eligible for the submission of a security investigation, both initial and PR's, shall do so via the Electronic Questionnaires for Investigations Processing (e-QIP) program.

2. e-QIP is a web-based program that permits applicants to access their e-QIP accounts, once initiated, from a government computer or a personal computer without downloading any software.

3. All investigations are initiated and submitted via JPAS. Only JPAS users with the appropriate accesses can initiate and release investigations.

4. Fingerprint cards are required for all initial investigations. This includes initial SSBI's for personnel who already have an adjudicated NACLIC. Fingerprint cards are still submitted via the United States Postal Service.

3011. TEMPORARY ACCESS (INTERIM CLEARANCE)

1. Temporary access (also referred to as interim clearance) is a stopgap measure taken to minimize operational impact. In the absence of adverse information, commanding officers may grant temporary access to individuals pending completion of full investigative requirements. Listings of adverse information are identified in reference (a), appendix G, paragraph 4.

2. Temporary Top Secret access requirements.

I MARINE EXPEDITIONARY FORCE IPSP

a. Established secret or confidential security clearance eligibility or a current National Agency Check (NAC) favorably adjudicated by DON CAF.

b. A favorable review of the completed Personnel Security Questionnaire (PSQ) revealing no eligibility issues as outlined in reference (a), exhibit 10A.

c. The submission of the SSBI request to OPM.

3. Temporary secret or confidential access requirements.

a. A favorable review of the PSQ revealing no eligibility issues as outlined in reference (a), chapter 10, exhibit 10A.

b. The submission of an appropriate investigative request to OPM via the command security manager's office.

4. In accordance with reference (a), exhibit 8B, individuals with dual citizenship **cannot** be granted temporary access.

3012. INDOCTRINATION. All personnel entering employment with DON need to have a basic understanding of what "classified information" is, and the reasons(s) for its protection, as well as how to protect it. Personnel that qualify for temporary access or who have an adjudicated security clearance must complete the following forms to establish access within the I MEF Command Element;

1. Non-Disclosure Agreement (SF-312): All command personnel will, regardless if previously executed at another command, execute a Classified Information Nondisclosure Agreement (NdA), Standard Form (SF) 312, as a condition of access to classified. Further guidance concerning NdA's can be found in reference (a), chapter 9. NDA's are mailed to HQMC (MMSB-22)

2. Command Local Orientation: The Command Local Orientation is used to outline the unique security requirements and conditions of the command, and duties and responsibilities of command personnel who have been granted access to classified military information. This form also outlines specific obligations for reporting derogatory information on oneself and their co-workers.

3. Verbal Attestation: Required per MARADMIN 163/99. A verbal attestation will be completed for all personnel with Top Secret and Sensitive Compartmented Information (SCI) security clearances and those with access to Special Access Programs (SAP). Must be posted in JPAS when executed.

4. NATO Briefing: Required by MARADMIN 136/04. A NATO briefing is required by all USMC personnel (military, civilian, and contractors) that require access to SIPRNET. A written acknowledgement of the individual's receipt of the NATO briefing and responsibilities for safeguarding NATO classified information shall be maintained. Must be updated in JPAS when executed.

5. Access Approval/Badge Agreement Form: All command personnel will have a form filled out by the Security Manager outlining the level of access the

I MARINE EXPEDITIONARY FORCE IPSP

command has granted the applicant based on the guidelines listed in reference (a). This letter also serves as a waiver letter for temporary access and as a badge agreement to those command personnel that are issued a security access badge.

3013. AUTHORIZED SECURITY ACCESS BADGES

1. All I MEF command personnel that have been approved for access to classified military information will be issued a security badge for a period of no more than 365 days or until their PR due date, whichever comes first.

a. For actual badge formats, color codes, and details concerning security badges contact the Command Security Manager. Command security access badges are subject to change.

2. Expired badges must be turned in immediately and a new badge issued. Upon the issuing of a new security badge by the security manager's office a new local orientation form and badge agreement will be filled out. This supports the command continued security education process.

3. Local commands that produce their own unique security badge(s), as proof of clearance, may request, in writing, that the I MEF Security Manager reciprocate their commands security access badges.

4. This command retains the right to accept or decline badges issued by other units, organizations and commands.

3014. PERSONNEL SECURITY FILES (PSF).

1. The PSF retains all clearance and indoctrination related forms. This file is scanned and saved as a digital file.

2. The PSF retains a contact sheet that records all actions taken with command personnel concerning access and clearance related matters.

3. This file is destroyed either upon checkout or when it has been determined that the individual is no longer attached to the command or access is no longer required.

3015. DEBRIEFING

1. A debriefing will be given to individuals who no longer require access to classified information as a result of one of the following:

- a. Transfer from one command to another.
- b. Suspension of clearance by Commanding Officer.
- c. Revocation of security clearance.
- d. End of Active Service.
- e. Retirement.

I MARINE EXPEDITIONARY FORCE IPSP

2. A command debriefing form shall be executed and will include;
 - a. All classified material in individuals' possession must be returned;
 - b. Individuals are no longer eligible for access to classified information;
 - c. Reminder of the provision of the Classified Nondisclosure Agreement (SF-312) (exhibit 4a) to never divulge classified information, verbally, to any unauthorized person without written permission from CNO.
 - d. There are severe penalties for disclosure;
 - e. The individual must report to NCIS (or to the FBI or nearest DoD component if no longer affiliated with the DON), without delay, any attempt by an unauthorized person to solicit classified information.
3. Security Termination Statement (OPNAV 5511/14): This form is executed at the time of debriefing, unless the debriefing is done simply because the individual is transferring from one command to another and will continue to require access to classified material. This form is mailed to HQMC (MMSB-22) for file retention.
4. Administrative Debriefs: Administrative debriefs are normally performed when the individual has already left the command and no other command is currently servicing or owning the individual in JPAS. The debrief form will be labeled "Administrative Debrief" where the individuals signature would have gone, signed by the security rep accordingly and mailed to HQMC (MMSB-22).

3016. UNFAVORABLE SECURITY DETERMINATIONS. Not all investigations submitted for adjudication to the DoNCAF will come back with a favorable security determination. In most cases when an unfavorable security determination has been made access will be lost. When a negative ruling has been decided the command will receive notice via the JPAS immediately. This chapter further explains unfavorable security determinations.

3017. NO DETERMINATION MADE

1. "No Determination Made" is a ruling applied when there is insufficient information for the DoNCAF to adjudicate an investigation. Cases that result in a "No Determination Made" are due to derogatory information such as but not limited to financial irresponsibility, criminal records, and citizenship concerns. An individual that has a "No Determination Made" ruling cannot be granted temporary access. It must be understood that this ruling is not as severe as a Letter of Intent or a Letter of Denial.
2. A Request to Research/Upgrade (RRU) must be submitted via JPAS in order to determine why DoNCAF applied the "No Determination Made" ruling. Once the information is received from DoNCAF, normally via JPAS, the applicant must provide whatever supporting information and documentation that is requested. This entire process can take anywhere from 1 to 6 months to resolve. The time frame to resolve varies from case to case. There is no higher authority

I MARINE EXPEDITIONARY FORCE IPSP

or process that can overrule or expedite this matter.

3018. LETTER OF INTENT (LOI). A LOI is released by the DoNCAF when an unfavorable eligibility determination **is being contemplated**.

1. A LOI will outline the disqualifying information and provide additional guidance for the command and the applicant.
2. Commands must immediately reply to the LOI with a letter of receipt provided in the LOI package.
3. All recipients have the choice to submit a rebuttal, via the Command Security Manager, in order to mitigate all disqualifying information. DoNCAF will review the rebuttal and make a security determination.
4. When a LOI is received all temporary access must be withdrawn by the command. This requires the execution of an OPNAV 5511/14.
5. If a LOI is received as a result for a periodic reinvestigation or a clearance upgrade, the command may allow continued access at the level previously adjudicated if the applicant submits a rebuttal.
6. LOI's are also released when a command has reported to DoNCAF that an individual's continued access should be suspended as a result of actions by the individual that place is loyalty, trustworthiness, and/or judgment into question.
7. Personnel who choose not to submit a rebuttal will be debriefed immediately and forfeit their right to appeal. DoNCAF will be notified, via the Security Manager, of the applicant's decision not to submit a rebuttal. DoNCAF will make a final security determination and a letter of denial (LOD) will be released. The final determination will be posted in JPAS as DENIED. Applicants must wait a period of 365 days before attempting to reinstate there security clearance. A rebuttal to this particular LOD will not be permitted due to the applicant's decision not to submit a rebuttal to the LOI.
8. If a rebuttal is insufficient at mitigating the disqualifying information listed in the LOI, DoNCAF will issue a LOD within 60 to 90 days and all access will be terminated and the applicant must be debriefed.
9. LOI's released for individuals with Sensitive Compartmented Information (SCI) clearances will be processed through the SSO.
10. Additional guidance concerning LOI's can be found in reference (a), chapter 8, section 8-4.

3019. LETTER OF DENIAL. A LOD (previously referred to as letter of notification) is released by the DoNCAF when an unfavorable eligibility determination **has been made**.

I MARINE EXPEDITIONARY FORCE IPSP

1. All access must be terminated upon the notification of a LOD. Applicants must be debriefed in accordance with reference (a).
2. Rebuttals for a LOD are submitted to the Personnel Security Appeals Board (PSAB). The PSAB decision is final and concludes the administrative appeals process.
3. The command will receive a final security determination letter in the mail and JPAS will be updated by DoNCAF to reflect the PSAB decision.
4. If the rebuttal to a LOD is insufficient the applicant must wait 365 days from the date of decision listed in JPAS before appealing for a security clearance.
5. The LOD will list all the information from the LOI that wasn't sufficiently mitigated.
6. The SSO handles all SCI related cases.
7. Additional guidance concerning LOD's can be found in reference (a), chapter 8, section 8-4

3020. APPEALING A DENIED OR REVOKED SECURITY CLEARANCE

1. In order to appeal a revoked or denied security clearance an applicant must wait no less than 365 days, from the date the decision was decided, before submitting an appeal. The decision date can be verified via JPAS. A new investigation is not required for the appeal process.
2. An applicant cannot, with out command endorsement, submit an appeal directly to DoNCAF.
3. The initial phase of the appeal process is for the Security Manager to request a copy of the LOI or LOD that outlines all the relevant disqualifying information. This is done to ensure all issues are addressed before submitting an appeal.
4. The appeal is simply a new rebuttal outlining how the individual has resolved all previous disqualifying matters. The appeal is submitted via the Security Manager.
5. The overall process is similar to the LOI process in that a new rebuttal concerning the previous LOD's information must be addressed. Any relevant supporting documentation must be included with the new rebuttal and command endorsement letters from peers and senior leadership and the Commanding Officer.
6. If the command does not have a copy of the LOD one can be requested from DoNCAF and it will be mailed to the command.
7. Applicants whose clearances have been denied or revoked are not eligible for temporary access.

I MARINE EXPEDITIONARY FORCE IPSP

8. It must be understood that the process, from start to finish, can take as long as 6 months.

3021. DUAL CITIZENSHIP. In accordance with reference (a), exhibit 8b, an individual who is either a dual citizen or is in possession of a foreign issued passport, current or expired, is not eligible for temporary access.

1. Individuals who possess dual citizenship must be prepared to renounce dual citizenship in writing and either return any foreign issued passport to the appropriate country embassy or consulate and obtain a return receipt to demonstrate that the passport has been surrendered or surrender it to a security official (Security Manager, Assistant Security Manager, or anyone assigned to execute personnel security issues for the command) for destruction. If the passport is destroyed it must be recorded in writing and witnessed by the security official.

2. Additional guidance and clarity for dual citizenship matters is clearly outlined in reference (a), chapter 8, exhibit 8b.

3022. VISITOR CONTROL.

1. Positive control of visitors both cleared and uncleared is a challenge for commands. Throughout the Department of Defense it is essential that all visiting personnel being granted access to classified information have the appropriate security eligibility and access.

2. Military personnel and civil servants visiting this command must be owned or serviced by the command or organization they are currently assigned to or employed with, have current security eligibility, or have submitted a PR that can be verified via JPAS, and have been granted U.S. Access in JPAS in accordance with reference (a).

a. If a visitor is not being owned by the command that they are presently assigned to, access will be denied regardless if all other entries in JPAS are correct.

b. PR's or initial investigations that have been submitted over 30 days ago and do not reflect as received or opened or that have been deemed unacceptable will not be recognized as proof of clearance at this command. A new investigation will have to be submitted and the PSQ sent date on JPAS updated.

3. Contractors must meet the same requirements of military personnel and will also be required to have a visit certificate submitted via JPAS by their organization prior to access being granted.

4. Verification of clearance for visitors shall be obtained through the Security Manager or those personnel within the command that have been granted the authority to do so.

5. Permitting access to restricted areas to personnel without the proper clearance unescorted is a security violation and will be investigated. Such

I MARINE EXPEDITIONARY FORCE IPSP

actions are punishable under the Uniformed Code of Military Justice.

3023. SECURITY EDUCATION. The Security Manager is responsible to ensure that personnel within the command are kept abreast of changes that impact the command and its personnel directly.

1. Annually the Security Manager will coordinate with NCIS to provide a Counterintelligence (CI) brief that is required for all personnel who hold a Secret or higher security clearance.

- a. The Security Manager will also use these scheduled training opportunities to provide a security awareness briefing and should consider including the Information Assurance Manager, Operational Security Officer and the SSO.

- b. Annual training sessions should be held repeatedly throughout the year until a healthy majority of the command has attended the training. It is understood that command obligations, deployments and operations make it impractical for all command personnel to attend such training events.

3. The Command Security Manager will also provide education through various other methods such as posters, emails, and command wide notices.

4. It is critical that the command security program stay current and not become stagnant.

5. The Security Manager shall be expected to provide classroom instructional periods upon request.

6. Security Managers shall ensure they are part of pre-deployment and post deployment briefings. Command personnel are most likely to commit a security violation in a rush to deploy or shortly upon returning from deployment. These are critical windows for education.

7. Reference (a), chapter 4 lists all the annual minimum requirements for a security briefing. The list can and should be expanded upon with poor security trends that plague or concern the command.

3024. COUNTER INTELLIGENCE MATTERS. All command personnel, military and civilian, will report, whether they have a security clearance or not, any activities listed below to the Command Security Manager or their supervisor immediately.

1. Sabotage, Espionage, Terrorism, Subversion, or Deliberate Compromise: Individuals becoming aware of sabotage, espionage, terrorism, deliberate compromise or other subversive activities will report all available information concerning such activities immediately to the Commanding Officer or Security Manager or at the readily available command.

2. The Command notified will immediately notify the local NCIS office.

3. Further guidance concerning such matters is located in reference (a), chapter 3.

I MARINE EXPEDITIONARY FORCE IPSP

3025. REPORTING DEROGATORY INFORMATION. Personnel who possess a security clearance must report any of the following activities on themselves or their co-workers to their Commanding Officer or Security Manager immediately. Many of these actions such as suicide will also be reported to the local NCIS office.

1. Suicide or attempted Suicide.
2. Contact with individuals attempting to access classified material by an unauthorized or illegal manner.
3. Death, Unauthorized Absentee or Desertion.
4. Emotional, Mental and Personality Disorders.
5. Criminal Conduct.
6. Foreign Connections, Influence or Preference.
7. Financial Irresponsibility.
8. Personal Conduct.
9. Misuse of Information Technology.
10. Substance Abuse (alcohol or narcotic).
11. Allegiance to the United States (when in question).
12. Security Violations.
13. Outside Activities.
14. Sexual Behavior.

3026. ACCESS SUSPENSION.

1. The commanding officer has the authority to suspend access to military members and civilian employees. In such instances DoNCAF must be notified of the suspension via JPAS through the incident report link.
2. When access is suspended it is required that the individual be notified in writing, by the command, within 10 days with an explanation for the justification for access suspension.
3. The commanding officer may also reassign an individual to a non sensitive duty until the matter in question is formally adjudicated by DoNCAF.
4. All forms of access to classified spaces, vaults, and security containers must be terminated and combinations to said spaces changed.
5. If after suspension of access, the DoNCAF adjudicates the reported information favorably, that information will no longer be the basis for

I MARINE EXPEDITIONARY FORCE IPSP

continued suspension of access.

a. If the commanding officer continues to believe the individual is a risk then the commanding officer may reassign the individual to a non-sensitive position and elect to submit additional documentation that supports their concerns regarding the individual's disqualification.

b. See reference (a), chapter 9, paragraph 9-7 for additional and amplifying guidance.

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 4

INFORMATION SECURITY

| | PARAGRAPH | PAGE |
|---|-----------|------|
| BASIC POLICY | 4000 | 4-3 |
| CLASSIFICATION MANAGEMENT | 4001 | 4-3 |
| ORIGINAL CLASSIFICATION AUTHORITY (OCA) | 4002 | 4-3 |
| CHALLENGING A CLASSIFICATION | 4003 | 4-3 |
| DERIVATIVE CLASSIFICATION | 4004 | 4-4 |
| SECURITY CLASSIFICATION GUIDES (SCG) | 4005 | 4-4 |
| MARKING CLASSIFIED | 4006 | 4-4 |
| MARKING CLASSIFIED REMOVABLE IT STORAGE AND IT SYSTEMS | 4007 | 4-4 |
| MARKING CLASSIFIED DOCUMENTS PRODUCED BY IT SYSTEMS | 4008 | 4-5 |
| SANITIZING A DOCUMENT | 4009 | 4-5 |
| SAFEGUARDING | 4010 | 4-6 |
| COVERSHEETS | 4011 | 4-6 |
| TOP SECRET CONTROL MEASURES | 4012 | 4-6 |
| SECRET CONTROL MEASURES | 4013 | 4-6 |
| WORKING PAPERS | 4014 | 4-7 |
| TOP SECRET WORKING PAPERS | 4015 | 4-7 |
| END OF DAY PROCEDURES (SF 701) | 4016 | 4-7 |
| SAFEGUARDING DURING CLASSIFIED VISITS AND MEETINGS | 4017 | 4-7 |
| REPRODUCTION | 4018 | 4-7 |
| DISSEMINATION | 4019 | 4-8 |
| PREPUBLICATION REVIEW | 4020 | 4-8 |
| TRANSMISSION AND TRANSPORTATION | 4021 | 4-9 |
| AUTHORIZED METHODS OF TRANSMISSION/TRANSPORTATION | 4022 | 4-9 |

I MARINE EXPEDITIONARY FORCE IPSP

| | | |
|--|------|------|
| CERTIFIED COURIERS | 4023 | 4-9 |
| PREPARING CLASSIFIED FOR TRANSPORT..... | 4024 | 4-10 |
| CLOSED STORAGE | 4025 | 4-10 |
| OPEN STORAGE | 4026 | 4-10 |
| STORAGE REQUIREMENTS | 4027 | 4-11 |
| WORKSPACE ACCESS ROSTERS | 4028 | 4-12 |
| COMBINATIONS FOR MECHANICAL AND DIGITAL LOCKS | 4029 | 4-12 |
| DESTRUCTION | 4030 | 4-13 |
| SECURITY VIOLATIONS | 4031 | 4-14 |
| LOSS OR COMPROMISE OF CLASSIFIED INFORMATION | 4032 | 4-14 |
| PROHIBITED DIGITAL DEVICES | 4033 | 4-15 |
| CLASSIFIED MATERIAL ANNUAL REVIEW | 4034 | 4-15 |
| INDUSTRIAL SECURITY PROGRAM | 4035 | 4-16 |
| RELEASE TO FOREIGN NATIONALS | 4036 | 4-16 |

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 4

INFORMATION SECURITY

4000. BASIC POLICY.

1. Every command that retains, processes, and creates classified material must establish an information security program (ISP), in accordance with SECNAV 5510.36 and MARADMIN 343/02, to track, safeguard and manage their classified material effectively.

2. Classified material is the property of the U.S. Government and not personal property. Military and civilian personnel, who resign, retire, separate from the DON, or are released from active duty, shall return all classified information in their possession to the command from which received, or to the nearest DON command prior to accepting final orders or separation papers.

3. Terminology. "Classified material" is used throughout this chapter as a generic term for all forms of classified and includes, but is not limited to documents, removable storage devices, compact disks, working papers, magnetic and optical storage devices and computerized hard drives.

4001. CLASSIFICATION MANAGEMENT. Executive Order 12958, as Amended, Classification National Security Information, 25 Mar 03, is the only basis for classifying national security information.

1. Information that requires protection against unauthorized disclosure in the interest of national security shall be classified as Top Secret, Secret, or Confidential.

4002. ORIGINAL CLASSIFICATION AUTHORITY (OCA). Original classification can only be applied by an appointed OCA when the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security.

1. A Listing of Department of Navy OCA's is provided in reference (b).

2. OCA's are appointed at either the Top Secret or Secret level.

3. The I MEF Commanding General is not an OCA.

4. The Commander, Marine Forces Pacific is an OCA appointed at the TOP SECRET level.

4003. CHALLENGING A CLASSIFICATION. Challenges to the classification of a product shall be submitted to the OCA of the product. Products classified using a Security Classification Guide (SCG) or a source document will be forwarded to the OCA of the SCG or document for review.

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

I MARINE EXPEDITIONARY FORCE IPSP

2. Every challenge must be submitted formally on command letterhead 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.

3. All challenges shall be submitted via the Security Manager to ensure proper format and mailing.

4. It is the responsibility of the requester to identify the appropriate OCA.

4004. DERIVATIVE CLASSIFICATION. When either a source document or a SCG is used to derive the classification of classified material it is referred to as a derivative classification. The vast majority of classified material is classified in this way.

4005. SECURITY CLASSIFICATION GUIDES (SCG). All Secret and Top Secret material require protection in accordance with E.O. 12958. SCG's or source documents are the references used to classify a product. SCG's are prepared by OCA's and are forwarded to the CNO (N09N2), and entered into a computerized database for record. These documents outline the criteria for classifying information and products as they pertain to specific operations, or programs. They also list the declassification guidance for the products.

1. There are lists of SCG's posted on the COMMARFORPAC website identifying commonly used SCG's.

2. Command personnel are strongly encouraged to contact the Security Manager for further guidance concerning SCG's and classification determinations.

4006. MARKING CLASSIFIED. All classified materials must be marked in accordance with Executive Order 12958, as amended 31 March 2003, DoD Regulation 5200.1 "Information Security Program," dated January 1997 and SECNAV M-5510.36.

1. All classified documents require page markings, subject line markings, portion markings, document date, derived from line, and declassification instructions.

2. The use of stamps or the appropriate sticker label (SFs 706, 707, 708, 709, 710, and 712 are also authorized for the marking of classified products.

3. Extensive guidance concerning the marking of all classified products can be found in reference (b), chapter 6 and the Information Security Oversight Office (ISOO) Marking Classified National Security Information Manual released May 2005. Further guidance can be obtained from the Command Security Manager.

4007. MARKING CLASSIFIED REMOVABLE IT STORAGE MEDIA AND IT SYSTEMS.

1. Removable Storage Media Markings: Mark classified removable IT storage media with the highest overall classification level using the appropriate label (SFs 706, 707, 708, 709, 710, and 712 (for SCI IT media)) and include

I MARINE EXPEDITIONARY FORCE IPSP

the abbreviated form of all applicable warning notices and intelligence control markings of the information contained therein. Removable IT storage media is any device in which classified data is stored and is removable from a system by the user or operator (i.e., optical disks, magnetic diskettes, removable hard drives, tape cassettes, etc.). When the approved standard form labels are not feasible due to interference with operation of the system or because of the size of the media, other means for marking may be used so long as they appropriately convey the classification and other required markings. In a totally unclassified working environment, there is no requirement to mark unclassified removable IT media.

2. IT System Marking: Each IT system shall be marked to indicate the highest classification level of the information processed by the IT system and the network to which it is connected. This is especially important with systems that have the capability to switch from a classified network connection to an unclassified network or system. The appropriate label (SF's 706, 707, 708, 709, 710, and 712 (for SCI IT media)) shall be placed on IT systems and components with memory such as workstations, external hard drives, printers, copiers, portable electronic devices, servers, and back-up devices.

a. Internal: Program the software of classified IT systems storing or processing information in a readily accessible format, such as email processed on a classified IT systems, to mark each classified file stored or processed by the system with the highest overall classification level and all applicable associated markings. When software does not provide for automated marking, information must nonetheless be marked. IT media containing classified files not programmed in a readily accessible format shall be marked on the outside with the highest overall classification level and all applicable associated markings (normally a sticker or tag) or have marked documentation kept with the media.

4008. MARKING CLASSIFIED DOCUMENTS PRODUCED BY IT SYSTEMS

1. Mark documents produced on IT systems, to include emails generated on a classified IT system and those that function as word processing systems, per this chapter. Special provisions for marking some IT system generated classified documents are as follows:

a. Mark interior pages of fan-folded printouts with the highest overall classification level. These markings shall be applied by the system even though they may not be conspicuous from the text. Mark the face of the document with all required associated markings or place these markings on a separate sheet of paper attached to the front of the printout.

b. Mark portions of printouts removed for separate use or maintenance as individual documents.

4009. SANITIZING A DOCUMENT. Sanitizing a document is the action of removing that which is classified from it and only leaving the unclassified portions.

1. When a classified document is properly classified in accordance with reference (b) this action is simple. However, it may result in a product

I MARINE EXPEDITIONARY FORCE IPSP

that no longer has any value.

2. This process must not be confused with declassifying a classified product as earlier defined in this chapter.

4010. SAFEGUARDING. Commanding officers shall ensure that classified information is processed only in secure facilities, on accredited Information Technology (IT) systems, and under conditions which prevent unauthorized persons from gaining access. This includes securing it in approved equipment or facilities whenever it is not under the direct control of an appropriately cleared person, or restricting access and controlling movement in areas where classified information is processed or stored. These areas may be designated, in writing, by the commanding officer as restricted areas. Decisions regarding designations of restricted areas, their levels, and criteria for access are at the discretion of the commanding officer.

4011. COVERSHEETS: Coversheets are sheets of paper that are placed on the top and sometimes the bottom of a document. The use of coversheets is mandatory and a tool to prevent inadvertent disclosure. They clearly display the classification of the paper product at the top and bottom. Cover sheets are often color coded red for secret and orange for top secret. The colors help to bring attention to the level of classification of the product but are not necessary. Coversheets can also be stapled to folders or attached to binders.

4012. TOP SECRET CONTROL MEASURES. All Top Secret information (including copies) originated or received by a command shall be continuously accounted for, individually serialized, and entered into a command Top Secret register or log. The register or log shall 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. If a disposition action such as destruction, downgrade or declassification affects the initial document page count, the page count does not need to be changed in the register or log if a list of the effective pages (LOEPs) is contained within the document. Top Secret registers or logs shall be retained for five years.

1. Top Secret Control Officers (TSCOs) shall obtain a record of receipt (typically a classified material receipt) from each recipient for Top Secret information distributed internally and externally.

2. Top Secret information shall be physically sighted or accounted for at least annually, and more frequently as circumstances warrant.

4013. SECRET CONTROL MEASURES. All Secret information retained by the command shall be retained in a manner outlined by this chapter and by those methods outlined in reference (b). Though Secret information does not require the administrative accountability that Top Secret information does, it is still the inherent responsibility of all cleared personnel to handle Secret material with the upmost care and professionalism. The Commanding General, at his discretion, may apply more stringent requirements for the handling and accounting for some or all classified Secret material.

I MARINE EXPEDITIONARY FORCE IPSP

4014. WORKING PAPERS. Secret and Confidential products 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. Dated when created;

b. Conspicuously marked centered 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;

c. Protected per the assigned classification level; and

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

2. Commanding officers shall establish procedures to control and mark all Secret and Confidential working papers in the manner prescribed for a finished document when retained more than 180 days from the date of creation or officially released outside the organization by the originator.

a. A document transmitted over a classified IT system is considered a finished document.

4015. TOP SECRET WORKING PAPERS. The accounting, control and marking requirements prescribed for a finished document will be followed when working papers contain Top Secret information.

4016. END OF DAY PROCEDURES (SF-701). All units, sections, and elements that retain or process classified material in their workspace shall execute a SF-701, End of Day checklist. This is done to ensure that all classified and sensitive materials have been appropriately secured, printers are turned off and cleared of any classified material, the shred bags have been processed and any other security requirements are accomplished before the area is secured for the day.

4017. SAFEGUARDING DURING CLASSIFIED VISITS AND MEETINGS. When the command hosts classified briefs, meetings, conferences, or symposiums it takes 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.

1. For no reason shall classified material be left unattended. A command member with sufficient clearance must remain with the classified at all times. Conditions may dictate that two or more individuals of sufficient access be posted when long periods of break are anticipated but the information must remain in position.

4018. REPRODUCTION. The reproduction of all classified material shall be kept to a minimal and excess destroyed immediately. Classified material may

I MARINE EXPEDITIONARY FORCE IPSP

only be reproduced on a device that has been accredited for that level of classification or higher.

1. Reproduction devices with imbedded hard drives must reside in an open storage workspace. Open storage workspaces are explained in detail further in this chapter.
2. Printers connected to classified networks or terminals must be turned off at the end of each working day. Only printers with volatile Random Access Memory (RAM) can be connected to classified networks in a closed storage facility or workspace.
3. 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 will be investigated.

4019. DISSEMINATION. In accordance with reference (b) the following dissemination requirements must be followed.

1. Top Secret information originated within the DoD shall not be disseminated outside the DoD without the consent of the originator or higher authority.
2. 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.
3. 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.

4020. PREPUBLICATION REVIEW

1. It is DoD policy that a security and policy review shall be performed on all official DoD information intended for public release including information intended for placement on publicly accessible websites or computer servers. Documents proposed for public release shall be first reviewed at the command level and may be found suitable for public release without higher-level consideration.
2. The Commanding General is authorized to release information to the public that is wholly within the command mission and scope. The Commanding General 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 is coordinated by the security manager in consultation with command subject matter experts.
3. If public release cannot be authorized within the chain of command, the material must be submitted for further review to the CNO (N09N2) or to the Commandant of the Marine Corps (ARS) (for Marine Corps matters).

I MARINE EXPEDITIONARY FORCE IPSP

4021. TRANSMISSION AND TRANSPORTATION

1. 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.
2. Outlined within this chapter are the procedures that must be taken and the methods authorized for transmitting or transporting classified material.
3. Further guidance concerning transmitting or transporting classified material can be obtained by speaking with the command security manager or by reviewing reference (b), chapter 9.

4022. AUTHORIZED METHODS OF TRANSMISSION/TRANSPORTION. Provided below is a list of methods authorized of the transmission/transportation of classified information.

1. Defense Courier Service (DoD funded program): DCS is a DoD funded program that is cleared to courier material as sensitive as Sensitive Compartmented (SCI) Material. Normally, it is only to be used for Top Secret and SCI material but can be utilized for transporting Secret material in situations when no other means is available or trusted.
2. Registered Mail: 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.
3. Commercial Carrier: The Information Security Oversight Office (ISOO) has approved use of all the small package domestic express Blanket Purchase Agreements (BPA) carriers (AIRBORN-F11626-02-A-0005, FEDEX - F11626-02-A-0007, UPS - F11626-02-A-0006 and ASTAR Air Cargo, Inc. (DHL) F11626-02-A-0008) for overnight domestic express delivery of Secret classified shipments.
4. Authorized Couriers: Appropriately cleared U.S. military, government civilian personnel and DoD contractors. This is the least preferred method of transportation due to the risk being greater for loss or compromise. This method of transportation will only be approved when no other method is available.
5. Authorized Department of Defense Network: The most preferred method to send and receive classified information is via a DoD approved computerized network certified to the level of classification of the product(s) being transmitted. Due to network limitation and file sizes this method is not always possible.

4023. CERTIFIED COURIERS. The Command Security Manager has 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 briefed by the Security Manager prior to transporting classified material. This process includes signing a courier statement of understanding provided by the security manager

I MARINE EXPEDITIONARY FORCE IPSP

and receiving a command courier brief.

2. Couriers are responsible when transporting classified material to ensure that upon arrival of their intended destination that 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.

4024. PREPARING CLASSIFIED FOR TRANSPORT.

1. When hand carrying classified material between buildings or from one command to another command aboard the same base the use of briefcases, courier bags, or envelopes that do not reveal the classification of the contents is required.

2. When preparing classified information for shipment, whether it is registered mail, commercial carrier, or certified courier the parcel must be double wrapped. Classified information shall be packaged so that classified text is not in direct contact with the inner envelope or container. Enclose the classified material in two opaque, sealed covers (e.g., envelopes, wrappings, or containers) durable enough to conceal and protect it from inadvertent exposure or tampering. Reinforced kraft tape is required.

a. All contents for shipment must be inventoried in the presence of a representative of the Security Manager's office. The inventory form to be used shall be provided by the Security Manager's office.

b. A receipt of all material must be placed with all classified parcels and a copy retained for a period of 5 years for Top Secret material and 2 years to Secret material. These records shall be kept by the Command Security Manager.

c. Coversheets identifying the classification of documents or the contents of binders shall be used.

d. For amplifying guidance see reference (b), chapter 9.

4025. CLOSED STORAGE. Spaces that have not been officially certified to store classified material outside of a GSA approved security container shall be referred to as Closed Storage. Such spaces must use only GSA approved security containers for the storage of classified material. See paragraph 4026 for further guidance concerning the storage of classified material.

4026. OPEN STORAGE. Spaces that permit the retention of classified material without the use of GSA approved security containers are referred to as Open Storage. Though the use of GSA approved security containers is not a requirement however this does not permit for classified material to be left

I MARINE EXPEDITIONARY FORCE IPSP

adrift or improperly protected with coversheets.

4027. STORAGE REQUIREMENTS. Classified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in a locked GSA approved security container, vault, modular vault, or secure room (open storage area construction per reference (b), chapter 10, exhibit 10A) as follows:

1. Store **Top Secret** information by one of the following methods;

a. In a GSA-approved security container with one of the following supplemental controls;

(1) The location housing the security container shall be subject to continuous protection by cleared guard or duty personnel;

(2) Cleared guard or duty personnel shall inspect the security container once every 2 hours;

(3) An Intrusion Detection System (IDS) with personnel responding to the alarm within 15 minutes of the alarm annunciation; or

(4) Security-in-Depth when the GSA-approved security container is equipped with a lock meeting Federal Specification FF-L-2740; or

(5) In a vault, modular vault or secure room constructed per reference (b), chapter 10, exhibit 10A, equipped with an IDS and a personnel response to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-in-Depth, or a 5-minute alarm response if it is not.

2. Store **Secret** information by one of the following methods:

a. In the same manner prescribed for Top Secret;

b. In a GSA-approved security container, modular vault, or vault without supplemental controls; or

c. Until 1 October 2012, in a non-GSA-approved container having a built-in combination lock. One of the following supplemental controls is required:

(1) The location housing the security container is subject to continuous protection by cleared guard or duty personnel;

(2) A cleared guard or duty personnel shall inspect the area once every 4 hours; or

(3) An IDS with the personnel responding to the alarm within 15 minutes of alarm annunciation.

d. Commands are encouraged to replace non-GSA-approved cabinets with GSA-approved security containers as soon as feasible prior to the mandatory replacement date of 1 October 2012.

I MARINE EXPEDITIONARY FORCE IPSP

3. Store **Confidential** information in the same manner prescribed for Top Secret or Secret except that supplemental controls are not required.

4. Secure Rooms, vaults, and safes all require the use of a SF-702, also referred to as the security container check sheet. This check sheet, when used properly, will identify when and who opened and secured the secure room, vault, or safe.

5. Under field conditions, during military operations, the Commanding General may require or impose security measures deemed adequate to meet the storage requirements in paragraphs 10-3.1a through c, commensurate to the level of classification.

4028. WORKSPACE ACCESS ROSTERS. Access rosters shall be placed on vaults and secure rooms to identify which personnel have unlimited access to the space and have been entrusted with the combination and/or keys to the locks protecting the space.

a. Access rosters shall identify personnel by rank, first name, last name, and the last four of the individual's social security number.

b. Access rosters must be updated when an individual listed no longer requires access to that specific space.

4029. COMBINATIONS FOR MECHANICAL AND DIGITAL LOCKS. Combinations to GSA approved digital security locks in use to protect vaults, secure rooms and GSA approved security containers at the Top Secret and Secret level shall be recorded and retained by the Security Manager using a Standard Form 700 (SF-700). The SF-700 must be handled and secured in the same manner of the classification it protects. SF-700 forms for locks used on safes and vaults retaining Sensitive Compartmented Information (SCI) shall be retained by the SSO.

1. SF-700: This form is used to retain the combination of any mechanical or digital combination lock used on a vault, secure room, or security container protecting National Security.

a. The Principle or Special Staff section utilizing the lock are responsible to provided updated SF-700 forms to the Command Security Manager.

b. All SF-700's will be labeled with the highest classification of information that the listed vault or container protects.

c. The combination shall never be stored in the same container it applies to.

d. A duplicate SF-700 may also be made and retained by the controlling section, but must be secured at all times to prevent the loss or compromise of the combination.

2. Changing a combination: Combinations shall be changed whenever anyone who knows the combination to a particular vault, secure room or security container has left the command, no longer requires access, or whose clearance has been revoked or denied. Combinations can and should be change

I MARINE EXPEDITIONARY FORCE IPSP

frequently, as a good security practice, when there has been no need to change a combination for a long period of time.

a. A new SF-700 must be created and secured in accordance with this manual and the old one destroyed.

b. A combination may also be changed by a command without reason, but as a security precaution.

4030. **DESTRUCTION.** Classified material that is no longer required shall be destroyed in a manner listed in reference (b) in order to minimize classified holdings and to protect the national security.

1. Approved methods of destruction include high security cross-cut shredders, wet pulping, pulverizing, and disintegrators. The National Security Agency (NSA) and the Department of Defense must approve all products for use before they can be utilized.

a. The command security manager can provide a list of approved equipment and distributors.

2. Some forms of classified cannot be destroyed within the command due to equipment limitations. In these instances the material will be sent to the NSA for final destruction. Some of the classified material that can not be destroyed within the command include but are not limited to hard drives, thumb drives, DVD's, flash drives, 4mm and 8mm tape.

a. The Security manager shall provide support for the preparation and mailing of classified material to the NSA for the purpose of destruction.

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

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

a. The I MEF Command Security Manager's office will keep record of all classified material mailed out for the purpose of destruction for a period of no less than 2 years in accordance with reference (b).

5. Cross-cut shredders are the most common method for destroying paper products. In accordance with reference (b), as of October 2008 all cross cut shredders in use must destroy all classified material to a size no larger than 5 square millimeters.

6. Though not a common practice in garrison, burning is also an approved method for items such as paper, diskettes, and CD's. Burning should only be done under extreme or combat conditions, when there is no other method available, and the retention of the excess classified material poses a threat to operations and the national security.

a. When burning is the only method of destruction available personnel must make every effort to apply the following procedures:

I MARINE EXPEDITIONARY FORCE IPSP

- (1) Identify a safe location for burning.
- (2) If available use a large metal barrel but if one is not accessible dig a narrow and deep pit.
- (3) Never burn at night and never during high winds. It is too easy to lose classified papers under these conditions.
- (4) Use a metal screen of some sort to cover the barrel or pit to prevent from material from flying out.
- (5) Burn must be stirred to reduce the papers to ash. This is the only way to ensure the material has been completely destroyed.

4031. SECURITY VIOLATIONS. A security violation is any action that intentionally or unintentionally places classified material in a position to be lost or compromised. Whether deliberate or unintentional, security violations must be reported and taken seriously.

1. 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 and will be held responsible for their lack of judgment and failure to report the violation.
2. Reporting a security violation immediately helps in minimizing the potential threat to national security.
3. Committing a security violation must be reported via JPAS to the appropriate central adjudication facility but does not necessarily warrant the loss of clearance.

4032. LOSS OR COMPROMISE OF CLASSIFIED INFORMATION. The loss or compromise of classified information presents a threat to National Security. Reporting loss or compromise ensures that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of the loss or compromise and to preclude recurrence. Once it becomes evident that classified information may have been lost or compromised it shall be reported to the commanding officer or the command security manager immediately.

1. PRELIMINARY INQUIRY: Initial process to determine the facts surrounding a possible loss or compromise.

a. A Preliminary Inquiry (PI) must be completed within 72 hours of the incident being reported. An investigating officer (someone other than the Security Manager) shall be appointed in writing by the Chief of Staff. The investigating official must be of sufficient rank and have the appropriate level of access to conduct the investigation.

b. The appointed Investigating Official shall report to the Security Manager for guidance and assistance. The Security Manager shall assist the appointed investigating official as necessary.

I MARINE EXPEDITIONARY FORCE IPSP

c. The intent of the PI is not to completely resolve the matter but determine if further investigation is warranted.

d. A copy of the PI shall be staffed through the Security Manager for review and endorsement.

e. More detailed guidance concerning a PI is outlined in reference (b), chapter 12.

2. JAGMAN INVESTIGATION: When loss or compromise of information can not be ruled out or determined remote as the result of a PI the Chief of Staff shall initiate a JAGMAN investigation. The purpose of a JAGMAN investigation is to provide a more detailed investigation and recommend disciplinary action or additional corrective action.

a. Should it be determine, during the course of the JAGMAN investigation, that loss or compromise has not occurred then the JAGMAN investigation shall be cancelled and all addressees required per SECNAV M-5510.36 and those courtesy copied shall be notified with a brief statement supporting the determination.

b. More detailed guidance concerning a JAGMAN is outlined in reference (b), chapter 12.

3. A copy of all PI's and JAGMAN investigations will be provided to and retained by the command 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.

4033. PROHIBITED DIGITAL DEVICES. Due to the threat that certain digital devices represent to national security the following devices are prohibited from command workspaces:

1. Personal computers;
2. All types of flash media (i.e. thumb drives, and SD cards);
3. Cameras and video recorders;
4. Audio recorders
5. Cellular devices are prohibited from some workspaces and permitted in others. Personnel must use cellular devices with extreme caution in spaces where they are permitted. They are prohibited from conferences, meetings, and training sessions where classified material will be discussed.

4034. CLASSIFIED MATERIAL ANNUAL REVIEW

1. Annually the command shall perform a review of all classified holdings. The intent of the review is to identify what classified material is no longer required and have it destroyed or considered for historical archiving.

I MARINE EXPEDITIONARY FORCE IPSP

a. Command wide annual reviews will be executed at the discretion of the Commanding General.

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 the required annual review are strongly encouraged.

4035. INDUSTRIAL SECURITY PROGRAM. Many civilian contractors are employed by the I MEF CE to perform a variety of tasks both unclassified and classified in nature.

1. Classified information shall never be turned over to civilian contractors unless the individual's clearance has been verified via the Security Manager and is in the performance of the individual's duties as outlined in DD-254.

a. Contractors in possession of a current I MEF security badge have been properly vetted and may be granted access to classified material without the requirement to contact the security manager's office.

b. The vetting process includes an endorsement letter and a valid visit certification via JPAS. The endorsement letter must be signed by an officer of GS-11 or higher or equivalent from the section they are assigned.

c. Contractors cannot endorse other contractors for classified access.

d. Contractors that require Top Secret access must provide a copy of the DD-254 prior to Top Secret access being granted.

2. Contractors shall only be granted access to restricted access areas and open storage areas in support of their duties as outlined in the contract they are fulfilling. All sections retain the right to deny access to contractors if the section feels there is not an established need-to-know.

3. Contractors that either work directly at the command, or who will have a long standing position within the command, are subject to all command policies pertaining to classified material. They will also be required to participate in all security education programs at the command.

4. The Commanding General retains the right to remove and deny access to any contractor he/she feels is not complying with command policy.

4036. RELEASE TO FOREIGN NATIONALS. Only that material that 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. In accordance with Presidential guidance, classified material marked as SECRET shall be considered as releasable to Canada, Great Britain, and Australia.

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 5

INTERNAL AND SUBORDINATE COMMAND INSPECTIONS

| | PARAGRAPH | PAGE |
|---|-----------|------|
| BASIC POLICY | 5000 | 5-2 |
| BACKGROUND | 5001 | 5-2 |
| INTERNAL COMMAND INSPECTIONS | 5002 | 5-2 |
| AFTERHOURS INSPECTIONS | 5003 | 5-2 |
| INSPECTIONS AND ASSIST VISITS OF SUBORDINATE COMMANDS | 5004 | 5-2 |
| SUBORDINATE COMMANDS SELF INSPECTIONS | 5006 | 5-3 |
| SUBORDINATE COMMANDS ASSIST VISIT AND INSPECTION PROGRAM | 5007 | 5-3 |
| TURNOVER AND TRAINING | 5008 | 5-3 |

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 5

INTERNAL AND SUBORDINATE COMMAND REVIEWS & INSPECTIONS

5000. BASIC POLICY. The Commanding General is responsible to ensure that on an annual basis a review of this commands security posture is executed. In addition, direct subordinate units will annually receive an assist visit from the Command Security Manager.

5001. BACKGROUND. It is required that all commands perform self inspections annually in accordance with reference (a), (b), and (c). When the inspections are performed properly and routinely they provide a clear picture of the commands overall security posture.

5002. INTERNAL COMMAND INSPECTIONS

1. The Security Manager shall perform announced and unannounced inspections of all I MEF CE facilities and workspaces at least once a year. More frequent inspections may be required depending on operational tempo and findings from recent inspections.

2. Inspections shall be written and recorded for a period of two years. A written record of findings for a building or section shall be provided to the appropriate section security representatives.

3. Inspections shall include but are not limited to windows, doors, SIPRNET lock boxes, safes, vaults, cipher locks (if used), intrusion detection system (IDS) (if used), classified handling procedures, access control, and the inspection of individuals entering and exiting a facility or workspace.

4. Significant findings shall also be reported to the Chief of Staff formally with recommendations for corrective action.

5003. AFTERHOURS INSPECTIONS. Afterhours inspections help the command identify whether or not end of day security procedures are being executed. After hours inspections permit the inspecting personnel to find vulnerabilities that would not be evident during normal working hours. It is highly recommended that Counterintelligence (CI) personnel be requested for such inspections in coordination with the Security Manager. After hours inspections are an essential tool to the Commanding General and Command Security Manager to assess the commands security posture.

5004. INSPECTIONS AND ASSIST VISITS OF SUBORDINATE COMMANDS

1. The Security Manager shall conduct inspections, assist visits, and reviews of direct subordinate commands. The Command Security Manager must conduct a formal inspection using the current edition of the HQMC IGMC inspection checklist 270. However, inspections and assist visits will not be limited solely to the 270 checklist. Relevant MARADMINs, DON messages, and portions of references (a), (b), and (c) that are not covered by the checklist shall also be applicable.

2. Assist Visit/Review/Inspection: Annually the Command Security Manager shall conduct security inspections of direct subordinate commands in order to access their information and personnel security program (IPSP).

I MARINE EXPEDITIONARY FORCE IPSP

a. All inspections shall be formally recorded and an outbrief provided to the units security manager and commanding officer. Deficiencies and observations shall be provided in a formal report to the Commanding Officer and Security Manager of the unit being inspected.

b. Subordinate units shall keep at a minimum a two year record of inspections performed by the I MEF Command Security Manager.

c. Subordinate commands may request an assist visit prior to an inspection by the I MEF Security Manager. It is highly recommended that commands request an assist visit when the security manager or when significant changes to a commands security office personnel occur.

5006. SUBORDINATE COMMAND SELF INSPECTIONS

1. During an assist visit and/or inspection it will be requested that the visited command identify how it performs self inspections.

2. Internal self inspections is a necessary tool for commands to assess themselves in order to strengthen their program and minimize the likelihood of loss or compromise.

5007. SUBORDINATE COMMAND ASSIST VISIT AND INSPECTION PROGRAM

1. Subordinate commands that have units directly beneath them will provide documentation of their assist visits and inspections during an I MEF Command Security Manager assist visit or inspection.

2. It is absolutely essential to the security posture of the entire Department of the Navy that senior commands perform inspections of their direct subordinate commands.

5008. TURNOVER AND TRAINING

1. The greatest challenges facing most security programs are a high rate of turnover and the inability to get proper and timely training for their appointed security personnel.

2. The high rate of turnover many commands face make it extremely important to have a clearly defined security program and administrative procedures.

3. Establishing a turnover folder and a share folder with important documents, forms, reports, and security publications is strongly encouraged in order to minimize the difficulties faced with a high rate of turn-over.

4. A commands ability to train its appointed security personnel is critical to managing a security program. The I MEF Security Manager's office is available to provide training to units upon request. Training the I MEF Security Manager's office is available to provide includes all aspects of information security, personnel security, and JPAS usage. Any training provided by the I MEF Security Manager does not supersede the requirement for Unit security managers to attend the CNO Security Manager Course.

5. Turnover and lack of training will be taken into consideration during inspections and assist visits but they will never be an acceptable justification for a program that shows obvious signs of neglect.

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 6

EMERGENCY ACTION PLAN

| | PARAGRAPH | PAGE |
|--|-----------|------|
| PURPOSE | 6000 | 6-2 |
| BACKGROUND | 6001 | 6-2 |
| INFORMATION | 6002 | 6-2 |
| NATURAL DISASTER | 6003 | 6-2 |
| CIVIL DISTURBANCE | 6004 | 6-2 |
| COMMAND AUTHORITY | 6005 | 6-2 |
| SECURING CLASSIFIED | 6006 | 6-2 |
| SECURING A FACILITY | 6007 | 6-3 |
| RELOCATING CLASSIFIED MATERIAL | 6008 | 6-3 |
| ADMITTANCE OF EMERGENCY PERSONNEL | 6009 | 6-3 |
| EMERGENCY DESTRUCTION | 6010 | 6-3 |
| EXECUTION OF EMERGENCY DESTRUCTION | 6011 | 6-4 |
| AUTHORIZED METHODS OF DESTRUCTION | 6012 | 6-4 |
| EMERGENCY DESTRUCTION REPORT | 6013 | 6-4 |

I MARINE EXPEDITIONARY FORCE IPSP

CHAPTER 6

EMERGENCY ACTION PLAN FOR CLASSIFIED MATERIAL

6000. PURPOSE. Establish the course of action to be taken by command personnel in the event of an emergency situation where national security information may be at risk of loss or compromise.

6001. BACKGROUND. During a natural disaster or civil disturbance, the possibility of loss or compromise of classified military information increases. It is essential that procedures be outlined to minimize the possible loss or compromise of classified material without endangering personal safety.

6002. INFORMATION. These instructions are provided to protect classified material during times of emergency. Key points are emphasized below:

1. In any emergency, personnel safety is the primary concern. Individuals tasked with carrying out this plan will not sacrifice their own safety or the safety of others in the execution of this plan.
2. Beginning emergency actions early will enhance the success of this plan. It is important to contact the appropriate officials, to advise of the situation and determine if execution of the emergency action plan, and to what degree is required.

6003. NATURAL DISASTER. In the case of a natural disaster such as fire, flood, or earthquake personnel are to follow their respective facility emergency action plan. Keep in mind that preservation of life takes precedence over the proper storage or destruction of classified material.

6004. CIVIL DISTURBANCE. Civil disturbances, such as rioting, are generally not a concern for the I MEF CE historically. The physical location of the commands facilities makes it nearly impossible for a civil disturbance to pose a significant level of interruption or threat to commands operations.

6005. COMMAND AUTHORITY. The Commanding General shall decide the course of action to take concerning the security of the commands classified holdings during an emergency. In the event that the commanding General is unavailable then the authority shall pass to the next senior command official.

1. Principle and Special Staff Officers of the command may decide the appropriate course of action to take during an emergency concerning the classified holding within their section when there is an imminent threat to personnel safety or national security. In such instances the individual responsible will be required to provide a letter of justification for their decision.

6006. SECURING CLASSIFIED. During a natural disaster or civil disturbance all non essential classified material shall be secured in a GSA approved security container, vault, or modular vault. These items include but are not limited to documents, binders, CD's, diskettes, external hard drives, thumb drives, computers (laptop and desktop), maps, and crypto used on secure phones.

I MARINE EXPEDITIONARY FORCE IPSP

6007. SECURING A FACILITY. Depending on the emergency, cleared command personnel shall provide a perimeter around the facility or facilities until it is been deemed safe to return to the building.

1. The perimeter security will not be terminated until the classified holdings of the building or buildings can be safely accounted for and secured in GSA security containers or extracted and moved to a facility with sufficient safeguards to protect the material appropriately.

2. In the event that base power and the backup generator fail for a facility, that is dependent on an intrusion detection system to provide sufficient protection for the classified material held within, a perimeter guard shall be established until power is restored.

3. Personnel assigned to provide perimeter security shall be instructed to report any suspicious activities immediately to the Senior Watch Officer or Security Manager as appropriate.

4. Personnel assigned to provide perimeter security have the authority and responsibility to challenge all persons intending to or attempting to access the facility.

6008. RELOCATING CLASSIFIED MATERIAL. If after an emergency the condition of a facility is determined inadequate to house classified material, all CMI shall be relocated to a more secure and safe location. Classified material, even if relocated after an emergency, must be stored in a manner outlined in chapter 4 of this manual or reference (b).

6009. ADMITTANCE OF EMERGENCY PERSONNEL. Admittance of emergency personnel (Paramedics, Police, Fire Fighter, etc.) into a restricted or controlled access space will be allowed under conditions that require immediate attention such as fire, flood, earthquake or medical emergency. The safeguarding of classified material shall not be construed as authority to bar or otherwise obstruct firemen, rescue workers and medical personnel.

1. Guide emergency personnel directly to the location of the crisis.

2. Sanitize the immediate area and any area emergency personnel may be exposed to prior to their arrival if time permits.

3. Obtain the names of all emergency personnel once the emergency has been resolved or when it is reasonably possible.

4. Report the names to the Security Manager as soon as possible. A "Non-Disclosure Statement" for all emergency personnel must be completed.

5. Radio communication by emergency personnel is authorized.

6010. EMERGENCY DESTRUCTION. Emergency destruction is the act of destroying all classified material via any means possible that renders the material useless in order to prevent Classified Military Information (CMI) from falling into the hands of unauthorized persons to include but not limited to enemy combatants, foreign entities and terrorists.

I MARINE EXPEDITIONARY FORCE IPSP

1. This action shall only be taken when the command no longer has the means to defend itself and classified material is in jeopardy of falling into the hands of unauthorized personnel.

2. The emergency destruction guidance provided is intended for OCONUS operations and exercises.

6011. EXECUTION OF EMERGENCY DESTRUCTION

1. Priority of Destruction.

a. Priority One--Top Secret Material, Cryptographic equipment and keying material to include STU-III and STE keys (COMSEC).

b. Priority Two--Secret Material

c. Priority Three--Confidential Material.

2. If a combination to a vault or security container is unknown contact the I MEF security manager office.

3. Subordinate commands in the local area shall be contacted and may be directed to execute an emergency destruction.

6012. AUTHORIZED METHODS OF DESTRUCTION. The use of any device or material, such as but not limited to incendiary grenades, cross-cut shredders, burn barrels, disintegrators, hammers, and any object that destroys or sufficiently damages equipment and material from being reconstructed is authorized. Time limitations and the sensitivity of the material must be taken into consideration when performing the emergency destruction.

1. Proper destruction methods such as shredders, burn barrels, disintegrators and CD destroyers shall remain a main method of destruction.

2. Use of hammers, incendiary grenades or similar items may be used when no other method is available or time doesn't permit for the main method of destruction to be performed.

3. Ultimately the desired result is to destroy classified material to a degree that eliminates risk of recognition or reconstruction of the information.

4. Sections shall report to the security manager once they have completed the destruction of all priority One and Two material and again when they have destroyed all priority Three material.

6013. EMERGENCY DESTRUCTION REPORT

1. All instances of an Emergency Destruction being executed must be recorded and reported in writing to the Command Security Manager.

2. These reports must at a minimum shall outline the conditions that warranted the action, the individual who authorized the emergency destruction, time and date of execution, and the effectiveness of the destruction.

I MARINE EXPEDITIONARY FORCE IPSP

3. These reports will be kept on record with the Command Security Manager for no less than 5 years.
4. The report will be submitted to HQMC (PP&O) via COMMARFORPAC immediately.