



UNITED STATES MARINE CORPS

2D MARINE AIRCRAFT WING
II MARINE EXPEDITIONARY FORCE
POSTAL SERVICE CENTER BOX 8050
CHERRY POINT, NC 28533-0050

WgO 5510.1T

SEC MGR

JUL 18 2011

WING ORDER 5510.1T

From: Commanding General, 2d Marine Aircraft Wing
To: Distribution List

Subj: 2D MARINE AIRCRAFT WING INFORMATION AND PERSONNEL
SECURITY PROGRAM (SHORT TITLE: 2D MAW IPSP)

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCO P5510.18A Ch 1
(d) IRM 5239-08A
(e) IRM 5239-10
(f) SECNAVINST 5720.44B
(g) SECNAVINST 5720.42F
(h) MCO 5530.14A

1. Situation. To publish procedures for the security of classified information and personnel within the 2d MAW. References (a) and (b) incorporate policy and guidance set forth in the Department of Defense (DoD) Information Security Program Regulation and are the basic directives governing the IPSP within the U.S. Navy and Marine Corps.

2. Cancellation. WgO P5510.1S.

3. Mission. To implement an IPSP in accordance with references (a) through (e).

4. Execution. To issue procedures and guidance for the 2d MAW IPSP to be in compliance with references (a) through (c) and to achieve and implementation of the IPSP throughout 2d MAW and Subordinate Commands.

5. Administration and Logistics. This revision contains substantial changes and must be reviewed in its entirety.

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

~~2011~~ 18 2011

6. Command and Signal

a. Command. This Order is applicable to 2d MAW and Subordinate Commands.

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


R. W. REGAN
Chief of Staff

DISTRIBUTION: A

JUL 18 2011

LOCATOR SHEET

Subj: 2D MARINE AIRCRAFT WING (2D MAW) INFORMATION AND PERSONNEL
SECURITY PROGRAM (IPSP)

Location: _____
(Indicate the location(s) of copy(ies) of this Order.)

JUL 18 2011

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

JUL 18 2011

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 1	COMMAND SECURITY PROGRAM AUTHORITIES AND BASIC POLICY	
1.	Purpose1-1
2.	Applicability1-1
3.	Scope1-1
4.	Department of the Navy Security Program Management.1-2
5.	Policy Guidance1-2
Chapter 2	COMMAND SECURITY PROGRAM MANAGEMENT	
1.	Policy.2-1
2.	Commanding General.2-1
3.	Command Security Manager.2-1
4.	Duties of the Command Security Manager.2-1
5.	Assistant Command Security Manager.2-3
6.	Top Secret Control Officer.2-3
7.	Security Officer.2-3
8.	Contracting Officer's Representative (COR)2-4
9.	Special Security Officer.2-4
10.	Other Security Assistants2-4
11.	Special Staff Section Responsibilities.2-5
12.	Internal Security Procedures.2-6
13.	Security Servicing Agreements2-6
14.	Inspections, Assist Visits and Reviews.2-7
Chapter 3	SECURITY EDUCATION	
1.	Policy.3-1
2.	Purpose3-1
3.	Responsibility.3-1
4.	Scope3-2
5.	Security Briefings.3-3
6.	Special Briefings3-4
7.	Debriefings3-4
8.	Training for Security Personnel3-5
9.	Continuing Security Awareness3-6

JUL 18 2011

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 4	LOSS, COMPROMISE, AND OTHER SECURITY VIOLATIONS	
1.	Policy4-1
2.	Administrative Sanctions, Civil Remedies and Punitive Actions.4-1
3.	Incident Reporting Responsibilities.4-2
4.	Preliminary Inquiry.4-2
5.	JAGMAN Investigations.4-4
6.	Investigative Assistance4-4
7.	Reporting Losses or Compromises of Special Types of Classified Information and Equipment.4-4
8.	Report of Finding CMI Previously Reported as Lost or Destroyed.4-5
9.	Compromise Through Public Media.4-5
10.	Unauthorized Disclosure Through Spillage4-5
11.	Security Violations.4-6
12.	Unsecured Security Containers.4-6
13.	Improper Transmission.4-6
Chapter 5	COUNTERINTELLIGENCE MATTERS TO BE REPORTED TO THE COMMAND SECURITY MANAGER	
1.	Policy5-1
2.	Sabotage, Espionage, International Terrorism or Deliberate Compromise5-1
3.	Contact Reporting.5-1
4.	Special Reporting Situations5-2
5.	Foreign Connections.5-3
Chapter 6	CLASSIFICATION MANAGEMENT	
1.	Policy6-1
2.	Original Classification Authority.6-1
3.	Original Classification Principles and Considerations6-2
4.	Specific Classifying Criteria.6-2
5.	Classification Designations.6-3
6.	Tentative Classification6-4
7.	Limitations on Classifying6-4
8.	Challenges to Classification6-5

JUL 18 2011

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 6	CLASSIFICATION MANAGEMENT	
9.	Duration of Original Classification.6-5
10.	Derivative Classification.6-5
11.	Accountability of Classifiers.6-6
12.	Foreign Government Information (FGI)6-6
Chapter 7	CLASSIFICATION REVIEW	
1.	Policy7-1
2.	Marking Requirements7-1
3.	Review Requirements.7-1
4.	Mandatory Declassification Reviews7-2
Chapter 8	CMI CONTROL MEASURES	
1.	Policy8-1
2.	Applicability of Control Measures.8-1
3.	Top Secret Control Measures.8-2
4.	Secret Control Measures.8-3
5.	Secret Naval Messages and E-mail8-4
6.	Secret Working Papers.8-5
7.	Confidential Control Measures.8-6
8.	Confidential Working Papers.8-6
9.	Special Handling Requirements.8-7
10.	Control Measures for Special Types of Classified and Controlled Unclassified Information.8-7
Chapter 9	CMI DISSEMINATION	
1.	Policy9-1
2.	Top Secret Dissemination9-1
3.	Secret Dissemination9-1
4.	Confidential Dissemination9-1
5.	Dissemination of Special Types of Classified and Controlled Unclassified Information.9-2
6.	Dissemination to Contractors9-2
7.	Disclosure to Foreign Governments and International Organizations.9-2

JUL 18 2011

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 9	CMI DISSEMINATION	
8.	Dissemination of Intelligence Material	.9-2
9.	Pre-Publication Review9-3
Chapter 10	CMI SAFEGUARDING	
1.	Policy10-1
2.	Responsibility for Safeguarding.10-1
3.	Restricted Areas10-1
4.	Safeguarding Working Spaces.10-2
5.	Safeguarding During Working Hours.10-4
6.	Safeguarding in Storage.10-5
7.	Safeguarding During Visits10-5
8.	Safeguarding During Classified Meetings10-5
9.	Safeguarding CMI While Being Hand Carried10-6
10.	Safeguarding CMI While in Travel Status.10-6
11.	Safeguarding CMI Located in Foreign Countries.10-8
Chapter 11	CMI DUPLICATION AND DISTRIBUTION	
1.	Policy11-1
2.	Controls on Reproduction11-3
3.	Controls on Copy Devices11-3
4.	Controls on Facsimile (FAX) Devices.11-5
5.	Controls on Printer Devices.11-6
6.	Control of Audio Recording Devices.11-6
7.	Control of Visual Recording Devices.11-6
8.	Control of Secondary Storage Media11-7
9.	Clearing and Purging of CMI from Media and Devices.11-8
Chapter 12	CMI DESTRUCTION	
1.	Policy12-1
2.	Destruction Procedures12-2
3.	Media Destruction Guidance12-2
4.	Emergency Destruction.12-4

JUL 18 2011

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 13	INDUSTRIAL SECURITY PROGRAM	
1.	Policy13-1
2.	Classified and Operationally Sensitive Contracts and the DD-25413-1
3.	COR.13-1
4.	Visits by Cleared DoD Contractor Emergency.13-2
5.	Facility Access Determination (FAD).13-2
Chapter 14	PERSONNEL SECURITY POLICY	
1.	Policy14-1
2.	Applicability.14-1
Chapter 15	PERSONNEL SECURITY INVESTIGATIONS	
1.	Policy15-1
2.	Command Responsibilities15-1
3.	Investigative Request Requirements15-1
4.	Joint Personnel Adjudication System (JPAS)15-2
5.	Office of Personnel Management (OPM)15-2
6.	Preparation and Submission of PSI Requests15-2
7.	Follow-Up Actions on PSI Requests.15-3
8.	Personnel Security Folders15-3
Chapter 16	PERSONNEL SECURITY DETERMINATIONS	
1.	Policy16-1
2.	Department of the Navy Central Adjudication Facility (DONCAF)16-1
3.	Joint Personnel Adjudication System (JPAS)16-1
4.	Eligibility Determination.16-2
5.	Unfavorable Determination.16-3
6.	Validity and Reciprocal Acceptance of Personnel Security Determinations.16-3

JUL 18 2011

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 17	PERSONNEL SECURITY ACCESS	
1.	Policy17-1
2.	Request for Access17-1
3.	Classified Information Nondisclosure Agreement (SF-312)17-1
4.	Verbal Attestation17-3
5.	Temporary Access (Interim Clearance)17-3
6.	Access Termination, Withdrawal, or Adjustment17-4
7.	Suspension of Access for Cause17-5
Chapter 18	VISITOR CONTROL	
1.	Policy18-1
2.	Facilitating Classified Visits18-1
3.	Visits by Foreign Nationals.18-2
APPENDIX A	GUIDELINES FOR COMMAND SECURITY INSTRUCTION	
1.	Command Security Program Elements.A-1
2.	Information Security Program Elements.A-1
APPENDIX B	GUIDELINES FOR EMERGENCY ACTION PLANS	
1.	Purpose.B-1
2.	BackgroundB-1
3.	Information.B-1
4.	Natural DisasterB-1
5.	Civil Disturbance.B-1
6.	Command Authority.B-1
7.	Securing Classified.B-2
8.	Securing a Facility.B-2
9.	Relocating Classified MaterialB-2
10.	Admittance of Emergency Personnel.B-2
11.	Enemy AttackB-3
12.	Emergency Destruction.B-3
13.	Execution of Emergency Action.B-3
14.	Authorized Methods of Destruction.B-3
15.	Emergency Destruction ReportB-4

JUL 18 2011

CHAPTER 1

COMMAND SECURITY PROGRAM AUTHORITIES AND BASIC POLICY

1. Purpose. This Order establishes the 2d MAW IPSP.

a. This Order identifies procedures for classification, safeguarding, transmission and destruction of Classified Military Information (CMI) as well as regulations and guidance for the Personnel Security Program. CMI is information originated by or for the DoD or its agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated Top Secret (TS), Secret and Confidential, as described in Executive Order (EO) 12356. CMI may be oral, visual or material form and has been subdivided further into eight categories. (DODD 5230.11 dtd June 16, 1992).

b. This Order implements the IPSP within 2d MAW in compliance with references (a) through (c), to promote an effective Command Security Program.

c. This Order is also intended to serve as an example for Subordinate Commands in establishing their Command's Security Program. The format of this Order, described in Appendix A, should be followed when developing local Command Security Program Manuals.

2. Applicability. This Order applies to all personnel; military, DoD Civilian, DoD Contractor and Subcontractor, assigned to or employed by 2d MAW and Subordinate Command. Each person who handles CMI is responsible for safeguarding it and is individually responsible for compliance with this Order in all respects.

3. Scope. This Order applies to all official information that has been determined to require safeguarding and/or protection against unauthorized disclosure and is so designated by an appropriate classifying authority.

a. Special Types of CMI. Certain information, per reference (a), is controlled in 2d MAW Assistant Chief of Staff (AC/S) G-2, Subordinate Commands. As such these are not addressed in this Order. For those Security Managers whose command routinely handle special types of CMI, refer to the reference for governing regulations.

b. Controlled Unclassified Information. DoD 5200.1-R, January 1997, Appendix 3, Controlled Unclassified Information, covers several types of unclassified controlled information, including "For Official Use Only" information, "Sensitive But Unclassified" (formerly "Limited Official Use") information, "DEA Sensitive Information," "DoD Unclassified Controlled Nuclear Information," "Sensitive Information," as defined in the Computer Security Act of 1987 and technical documents with limited distribution statements and provides basic information about the nature of this information and the procedures for identifying and controlling it.

4. Department of the Navy Security Program Management

a. The Secretary of the Navy (SECNAV) is responsible for implementing an IPSP in compliance with Executive Orders, Public Law and special directives. The Special Assistant for Naval Investigative Matters and Security (CNO (N09N)) is the senior Department of the Navy security official, while the Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant Director, IPSPs (NCIS-21) provide staff support for these functions and responsibilities.

b. The Commandant of the Marine Corps (CMC) administers the Marine Corps IPSP within the Marine Corps. The Director of Administration and Resource Management (AR) has been designated to manage the IPSP for the Marine Corps. CMC (Code ARS) is responsible for developing and implementing security related programs and policies Marine Corps wide.

c. The Commanding General (CG), 2d MAW administers the 2d MAW IPSP. The 2d MAW Command Security Manager manages, and is responsible for implementing the IPSP within 2d MAW and its Subordinate Commands.

5. Policy Guidance. The Department of the Navy (DoN) Information Security Program Regulation, of reference (b), provides the basic guidance for the security and safeguarding of CMI and the Department of the Navy Personnel Security Program (NPSP), of reference (a), provides the basic guidance for personnel security matters. The United States Marine Corps (USMC) IPSP Order, reference (c), provides Marine Corps specific guidance for information and personnel security matters. This Order provides 2d MAW specific guidance for information and personnel security matters.

a. Where policy and procedure identified in this Order differs from the references, this Order takes precedence. Challenges directed to or requests for further guidance and interpretation of this Order are encouraged and should be addressed to the 2d MAW Command Security Manager for resolution.

b. The 2d MAW Command Security Manager periodically publishes security awareness and training items in various formats, such as e-mails entitled SECURITY AWARENESS SHORT TAKES and the newsletter entitled SECURITY STANDARD. These publications are not directive in nature but reflect official interpretation of emerging security policies and procedures impacting the IPSP.

c. Combat Operations. Commanding Officers (COs) may modify the safeguarding requirements of this regulation 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.

d. Waivers and Exceptions. When conditions exist that prevent compliance with a specific safeguarding standard or costs of compliance exceed available resources, General/Special Staff and Commanders may submit a request for a waiver or exception to the Order, in writing, to the 2d MAW Command Security Manager.

CHAPTER 2

COMMAND SECURITY PROGRAM MANAGEMENT

1. Policy. The CG, 2d MAW is ultimately responsible for compliance and implementation of the 2d MAW IPSP. The CG delegates the authority to ensure compliance and implementation to his Subordinate Commanders.

2. Commanding General

a. An effective security program relies on a team of professionals working together to fulfill the CGs responsibilities. The CG will designate, in writing, security personnel to implement the command's IPSP.

b. CG's Responsibilities.

c. Per reference (c), paragraph 2001.

3. Command Security Manager

a. The Command Security Manager will be afforded direct access to the CG and/or AC/S to ensure effective management of the Command Security Program.

b. The Command Security Manager will be an Officer or civilian employee in the Security Administration Series GS-0080 in the pay grade GS-11 or above, with sufficient authority and staff to manage the Command's Security program.

c. Per reference (c), paragraph 2002.

4. Duties of the Command Security Manager

a. The Command Security Manager is the principal advisor on information and personnel security within the command and is responsible to the CG for the management of the program. The Command Security Manager must be cognizant of command security functions and ensure the security program is coordinated and inclusive of all requirements. The Command Security Manager must ensure that those in the command who have security duties are kept abreast of changes in policies and procedures and must provide assistance in solving security problems. The Command Security Manager is key in developing and administering the command's IPSP.

JUL 18 2011

b. The below listed duties apply:

(1) Ensures coordination of staffing Foreign Visit Requests received from the HQMC Foreign Disclosure Officer, to include Extended Foreign Visits, the Foreign Liaison Officer (FLO) Program, and the Marine Corps Foreign Personnel Exchange Program (MCFPEP). Ensure that Delegation of Disclosure Letters are maintained, with assignment letters and acknowledgment of responsibility letters, as applicable, signed by the Foreign Officer and assigned U.S. Contact Officers.

(2) Ensures all personnel granted access to the Secret Internet Protocol Router Network (SIPRNET) receive a North Atlantic Treaty Organization (NATO) SECRET security brief and a debrief when their access is rescinded, with documentation of the events recorded in Joint Personnel Adjudication System (JPAS).

(3) Ensures all personnel requiring access to CMI TS or Special Access Programs provide a verbal attestation of their responsibilities to protect that material, with documentation of the event recorded in JPAS and either on their Non-Disclosure Agreement or in their Personnel Security File.

(4) For Subordinate Commands who have Certifying Officials assigned per the DoD Directive 5210.2, provide certification and de-certification of access to Restricted Data (RD) to include Critical Nuclear Weapons Design Information (CNWDI) to eligible Explosive Ordnance Disposal (EOD) technicians in the MOS's 2305 and 2336 in accordance with the current edition of MCO 3751.2, with documentation of the event recorded in their Personnel Security File and JPAS. For Subordinate Commands who do not have Certifying Officials assigned, the 2d MAW Command Security Manager will provide guidance.

(5) Ensures that all personnel who have had access to CMI who no longer require access or are leaving the command for any reason (i.e. transferring, Temporary Additional Duty (TAD) for more than 60 days, retiring, reached the end of their contract) receive a command debrief, with documentation of the event recorded in their Personnel Security File and JPAS.

(6) Ensures Security participation in the Intra-Command Security Review of prepublication material prepared by the Public Affairs Officer (PAO) as required by the current edition of reference (f).

(7) Ensures Security collaboration with the Staff Judge Advocate (SJA) in reviewing requests received under the Freedom of Information Act that are or could possibly be considered for, exemption from release under certain categories described in the current edition of reference (g).

(8) Ensures professional development of the security management staff through attendance and participation in security classes (on-line, offsite and within the command) and at conferences and seminars of interest to security professionals.

(9) Per reference (c), paragraph 2003.

5. Assistant Command Security Manager

a. Per reference (c), paragraph 2005.

6. Top Secret Control Officer (TSCO). Major Subordinate Commands (MSCs) that handle TS CMI will designate a TSCO in writing. The Security Manager may serve concurrently as the TSCO. The TSCO must be a Gunnery Sergeant or above or a civilian employee in the pay grade of GS-07 or above. The TSCO must be a U.S. citizen and have been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI-Periodic Review (PR) completed within the previous five years. The TSCO is responsible for all TS CMI handled within their command with the exception of TS Sensitive Compartmented Information (SCI) material, which is controlled by the Special Security Officer (SSO). TS CMI will be controlled per reference (a) and this Order.

a. The TSCO shall maintain a system of accountability to record the receipt, reproduction, transfer, transmission, downgrading, declassification and destruction of TS information, less SCI TS CMI. The TSCO, with assistance from the Classified Material Control Center (CMCC) will maintain all records and reports reflecting the processing of TS Material for a period of five years past the date of the event or in the event of designation or access authorization letters, five years after termination of tenure.

b. The TSCO shall ensure inventories of TS information are conducted semi-annually, with results maintained for five years.

7. Security Officer. The CG shall designate in writing, the Security Officer responsible for the Physical Security and Loss

Prevention Program. The Security Officer will be guided by the provisions of the current edition of reference (h).

8. Contracting Officer's Representative (COR). When assigned, the COR will be a Security Specialist, appointed in writing by the Contracting Officer. The Command Security Manager may serve concurrently as the COR. The COR is responsible to the Command Security Manager for coordinating with program managers and technical and procurement officials. The COR will ensure that the industrial security functions are accomplished when CMI or unclassified controlled information (as defined in DoD 5200.1-R, January 1997, Appendix 3) or operationally sensitive information is provided to industry for performance on a classified or unclassified contract. The COR will be guided by the provisions of the current edition of reference (a).

9. Special Security Officer. The SSO is responsible for the Sensitive Compartmented Information Facility (SCIF) and the security, control, dissemination and use of all SCI and Special Intelligence (SI) CMI. The SSO is also responsible for personnel security associated with this type of CMI.

10. Other Security Assistants

a. Depending upon local requirements, the Command Security Manager may choose to implement assistants in fulfilling the command's security program. Security Assistants may be assigned duties within the Security Office or special staff sections.

b. Those special staff sections maintaining billets requiring the processing of CMI, and desiring assignment of a Security Assistant, will nominate to the Command Security Manager, a Security Assistant. Upon Command Security Manager concurrence, an appointment letter signed by the Command Security Manager will be forwarded to the Security Assistant through the special staff section.

(1) Security Assistants will maintain liaison with the Command Security Manager relative to security matters and are responsible to their section for dissemination of and compliance with security policy and procedures.

(2) Security Assistants have the authority to review locally produced CMI (either originally or derivatively classified) for correct classification and marking.

JUL 18 2011

(3) The Security Assistant should be an individual senior enough to exercise authority to manage the IPSP within their respective section.

(a) Security Assistants may be assigned duties pertaining to Personnel Security, CMCC, TS Control, Secondary Control Points (SCPs) and others as required. Some assignments lend themselves to concurrent tenure; approval by the Command Security Manager is required.

1. Personnel Security Assistants. If desired, the Command Security Manager may incorporate Personnel Security Assistants to handle the routine administration of personnel security clearances, access requests and control, visitor requests, to include foreign visitor requests and security record keeping.

2. SCP Custodians SCP. Each special staff section authorized to receive, store or process CMI will designate both a Primary and Alternate SCP Custodian. The custodian will be responsible for all CMI originated, stored, received or processed by their respective section. The duties of the SCP Custodian will be assigned in writing. The SCP is an extension of the CMCC; therefore the custodians are responsible to the CMCC for accountability of CMI maintained within their respective SCPs.

3. TS Control Assistants. If required, each division, branch or special staff section authorized to receive, store or process TS CMI will designate a TS Control Assistant. The TS Control Assistant will be responsible for all TS CMI originated, stored, received or processed by their respective section. The duties of the TS Control Assistant will be assigned in writing. The TS Control Assistants are responsible to the TSCO.

11. Special Staff Section Responsibilities

a. The AC/S G-2 will manage, advise and assist the Command Security Manager on counterintelligence matters, special access programs and management of the SSO functions.

b. The AC/S G-3 will manage, advise and assist the Command Security Manager on operations security (OPSEC) and Anti-Terrorism/Force Protection (AT/FP) issues.

18 2011

c. The AC/S G-4 will manage, advise and assist the Command Security Manager on security equipment procurement matters.

d. The AC/S G-6 will manage, advise and assist the Command Security Manager on Information Systems Security (INFOSEC), Information Assurance (IA), Communications Security (COMSEC) and the Global Command and Control System (GCCS).

e. The PAO will advise and assist the Command Security Manager on security review before public release of briefs and articles.

f. The Provost Marshall Office (PMO) will advise and assist the Command Security Manager on physical security and loss prevention.

g. The CMCC will manage, advise and assist the Command Security Manager on document and material security administration and control.

12. Internal Security Procedures

a. All special staff sections that handle CMI are required to prepare and keep current, written security procedures specifying how the requirements of this Order will be accomplished within their specific offices.

b. Internal security procedures should include, but are not limited to, accounting and control of CMI, physical security measures for protecting CMI, control of CMI reproduction and destruction, review of CMI for proper classification and marking, downgrading and declassification, requiring and recording clearance and access, security education and the control of visitors. The Command Security Manager will provide format and guidance to Security Assistants in developing their specific commodity area's internal security procedures.

13. Security Servicing Agreements (SSA)

a. Specified security functions may be performed for other commands via SSAs. Such agreements may be appropriate in situations where security, economy and efficiency are considerations.

b. The SSA shall be specific and shall clearly define the security responsibilities of each participant. All agreements

JUL 18 2011

shall include requirements for advising Commanders of any matters that may directly affect the security integrity of the command.

c. SSAs are normally signed and authenticated by respective Command Chiefs of Staff or an equivalent command official.

14. Inspections, Assist Visits and Reviews. Commanders are responsible for evaluating the security posture of their subordinate commands.

a. 2d MAW will, on an annual basis, conduct inspections, assist visits or reviews to examine overall security posture of 2d MAW Groups.

b. 2d MAW Groups will, on an annual basis, conduct inspections, assist visits or reviews to examine overall security posture of their Squadrons.

c. Internal reviews of Command Security Functions will be conducted as required by this Order and the Command Security Manager using the Automated Inspection Reporting System (AIRS) Checklist available on the Inspector General of the Marine Corps, Inspections Division, web page.

JUL 18 2011

CHAPTER 3

SECURITY EDUCATION

1. Policy. Each command within the DoN, which handles CMI, is responsible for establishing and maintaining an active security education program to instruct all personnel, regardless of position or grade, in the command's security policies and procedures.

2. Purpose

a. Basic to a security education program is the appreciation that there is a need for protecting and safeguarding CMI from hostile threats. The purpose of the IPSP is to provide a framework for the protection of information essential to national security.

b. The purpose of the security education program is to make sure that all personnel understand the need to protect CMI and know how to safeguard it. The goal is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties and the security of CMI becomes a natural element of every task.

3. Responsibility

a. The Command Security Manager is responsible for ensuring that all personnel (Active, Reserve, DoD (USN) Civilians, Contractors and Sub-Contractors), who will have access to CMI, receive an orientation briefing at the time of assignment. Thereafter, personnel will participate in a continuous security education program consisting of selected briefings and OJT within the scope of information contained in the paragraph below.

b. The Command Security Manager is responsible for ensuring that all DoD (USN) civilians, who are entering employment with the Civil Service at their command and who have never held a clearance, receive a security indoctrination brief as detailed in reference (a).

c. The Command Security Manager is responsible for ensuring that if the Commander, as an Original Classification Authority (OCA), is trained in the fundamentals of security

classification, the limitations of classification authority and OCA duties and responsibilities upon assignment as detailed in reference (b).

d. Special staff sections, with assistance from the Command Security Manager, are responsible for identifying the security requirements for the functions under their cognizance and for seeing that personnel under their supervision are familiarized with the security requirements for their particular assignments. Special staff sections Security Assistants will provide OJT within all offices as an essential part of their command's security education program.

4. Scope. Basic security education must be provided to all 2d MAW whether they have access to CMI or not. A more extensive security education program is available to those individuals who have been granted access. The Security Education Program developed must accomplish the following:

a. Advise personnel of the need for protecting and safeguarding CMI, the adverse effects to national security resulting from unauthorized disclosure and their legal responsibility to protect CMI in their knowledge, possession or control.

b. Advise personnel of the responsibility to adhere to standards of personal conduct required for personnel holding security clearances or assignment to sensitive duties.

c. Advise personnel of their obligation for self-reporting and the requirement to report information with potentially serious security significance regarding someone with access to CMI or assigned to sensitive duties.

d. Advise supervisors of the requirement for continuous evaluation of personnel for eligibility for access to CMI or assignment to sensitive duties.

e. Familiarize personnel with the principles, criteria and procedures for the classification, derivative classification, downgrading, declassification, marking, control and accountability, storage, destruction and transmission of CMI and alert them to the strict prohibitions against improper use and abuse of the classification system.

f. Familiarize personnel with procedures for challenging classification decisions believed to be improper.

g. Familiarize personnel with the security requirements for their particular assignments and identify restrictions.

h. Instruct personnel having knowledge, possession or control of CMI how to determine, before disseminating the information, that the prospective recipient has been authorized access, needs the information to perform his/her official duties and can properly protect (store) the information.

i. Advise personnel of the strict prohibition against discussing CMI over an unsecured telephone or in any other manner that may permit interception by unauthorized persons.

j. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain CMI.

k. Inform personnel of their particular vulnerability to compromise during foreign travel.

l. Advise personnel that they are to report to the Command Security Manager significant contacts with any individual, regardless of nationality, whether within or outside the scope of the individual's official activities, in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(2) The member is concerned that he or she may be the target of exploitation by a foreign entity.

m. Advise personnel of the penalties for engaging in espionage.

5. Security Briefings. The following are the types of security briefs required to be locally developed:

a. Security Orientation Briefing. A basic orientation to the IPSP of the command; this briefing is normally conducted when processing individuals for security access.

b. Security Indoctrination Briefing. Designed for newly assigned personnel (generally DoD (USN) Civilians, as all Marines receiving the indoctrination during recruit training) who have never held a clearance. The indoctrination provides a basic understanding of what classified military information is and why and how it is protected.

11/18/2014

c. Annual Refresher Briefings. Refresher briefings are required on an annual basis for all individuals who have been granted access to CMI. Refresher briefings cover day-to-day operations of the command.

d. Counterintelligence Briefings. All personnel who have access to CMI classified Secret or above, must be given a Counterintelligence (CI) briefing annually. A Special Agent of the Naval Criminal Investigation Service (NCIS) normally provides CI briefings; the Command Security Manager coordinates scheduling.

6. Special Briefings. Certain special briefings are given as required by the Command Security Manager. These include the following:

a. NATO Briefings. All personnel requiring SIPRNET accounts will be briefed to NATO SECRET before SIPRNET access is granted. NATO debriefs will be conducted in conjunction with the Command Security Debrief (see Paragraph 3006) and recorded within JPAS.

b. Courier Responsibilities Brief. All couriers will be informed of and acknowledge their security responsibilities when escorting or hand-carrying CMI.

c. SCI. The SSO is responsible for briefing and debriefing those personnel with SCI access and documenting within JPAS.

d. CNWDI. Certain commands are listed as certifying officials for CNWDI, per the provisions of DoD 5210.2, access to and dissemination of RD and are authorized and responsible for providing briefing and debriefing in the CNWDI program for select EOD and Chemical, biological, Radiological and Nuclear (CBRN) personnel. For those commands not listed as certifying officials per the DoD 5210.2, the 2d MAW Command Security Manager will provide CNWDI certification and decertification. Record RD/CNWDI briefing/debriefing within JPAS.

e. Other special briefings as circumstances dictate.

7. Debriefings. Under pre-defined conditions, the Command Security Manager must provide a Command Security Debrief and ensure a Security Termination Statement (OPNAV 5511/14 Rev 9-05) is completed and processed for those members of the command who have had access to CMI.

JUL 18 2011

a. A termination statement will be executed and a command debriefing will be given under the following conditions:

- (1) Prior to termination of active military service or civilian employment.
- (2) At the conclusion of the access period when a Limited Access Authorization has been granted.
- (3) When security access is administratively withdrawn.
- (4) When a member of the command who possesses no clearance or access, has inadvertently gained access to CMI.
- (5) When security clearance eligibility is revoked for cause by the DoN CAF.

b. A command debriefing will be given under the following conditions:

- (1) When a member of the command, who possess a clearance and access, inadvertently has substantive access to information which the individual is not eligible to receive.
- (2) When a member of the command transfers from one command to another.
- (3) Temporary separation for a period of sixty days or more including sabbaticals and leave without pay.

c. The original termination statement must be placed in the Marine's Service Record Book (SRB) or Officer Qualification Record (OQR) (Official Personnel File for DoD Civilians) prior to "closing out" the record, except in the case of revocation for cause. In this case, the original termination statement and a copy of the revocation letter will be forwarded to Headquarters Marine Corps (HQMC) (MMSB 20). The command debriefing form will be retained in the individual's Personnel Security Folder.

8. Training for Security Personnel. The CNO (N09N2) website displays STAAT (PAC and LANT) schedule information for the Security Manager's Course. The Naval Education and Training Professional Development and Technology Center (NETPDTC) website offers the Intro to the DoN IPSP online. The Defense Security Service (DSS) website offers links to Security Professional Development reading and many security related courses online.

JUL 18 2011

9. Continuing Security Awareness. The previous paragraphs describe the security education program through scheduled and as-required briefs. To enhance security in a continuing program, all command personnel should be frequently exposed to current and relevant security information.

a. OJT. Supervisors must assure themselves that subordinates know the security requirements impacting on the performance of their duties. OJT is that phase of security education that must be a continuous process and constantly evaluated to ensure that the security posture of the office is being maintained per this Order.

b. Security Awareness Materials. Security posters, 2d MAW Security Awareness Short Takes, 2d MAW Security Standard Newsletter, 2d MAW Users Guide to Security, the 2d MAW security websites, as-required training lectures and security information handouts, videos and computer based training are some of the methods and media that may be used to boost security awareness and support the continuing program. Special staff section Security Assistants should request security education and training materials through the Command Security Manager.

CHAPTER 4

LOSS, COMPROMISE AND OTHER SECURITY VIOLATIONS1. Policy

a. The loss or compromise of CMI represents a threat to national security. Reports of loss or compromise ensure 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.

(1) A loss of CMI occurs when it cannot be physically located or accounted for.

(2) A compromise is the unauthorized disclosure of CMI to a person who does not have a valid clearance, authorized access or a need-to-know. The unauthorized disclosure may have occurred knowingly, willfully or through negligence. Compromise is confirmed when conclusive evidence exists that CMI has been disclosed to an unauthorized person.

(3) A possible compromise occurs when CMI is not properly controlled. Compromise is possible when some evidence exists that CMI has been subjected to unauthorized disclosure.

b. Compromise obviously presents the greater threat to security, but other security violations must also be treated seriously as they demonstrate weakness within the 2d MAW security program. For this reason, loss, compromise and possible compromise must be reported and vigorously investigated to correct the cause of the threat.

c. Incidents of an individual's failure to comply with the policies and procedures for safeguarding CMI will be evaluated to determine their eligibility to hold a security clearance.

2. Administrative Sanctions, Civil Remedies and Punitive Actions

a. Civilian employees are subject to administrative sanctions, civil remedies and criminal penalties if they knowingly, willfully or negligently disclose CMI to an unauthorized person or knowingly or willfully violate provisions of this Order for classification and protection of CMI. Sanctions include, but are not limited to, a warning, written

JUL 18 2011

notice, reprimand, suspension without pay, forfeiture of pay, removal or discharge.

b. Military personnel are subject to punitive action, either in civil courts or under the Uniform Code of Military Justice (UCMJ), as well as administrative sanctions, if they disclose CMI to an unauthorized person or violate provisions of this Order for classification and protection of CMI.

c. Disciplinary action is used primarily to make it clear to the offender and other personnel, that lax security procedures will not be tolerated. Action taken for involvement in security violations will suit the offense and be applied regardless of grade.

3. Incident Reporting Responsibilities. Any individual or custodian of CMI with knowledge of a loss or compromise or subjection to compromise through unauthorized disclosure, abstraction, destruction, loss or theft, must report the incident to the Command Security Manager and their superior officer immediately. The Command Security Manager will, in turn:

a. Immediately notify the local NCIS office to apprise them of the incident and ascertain their interest in opening an investigation.

b. Coordinate with the CO to initiate a Preliminary Inquiry (PI).

4. Preliminary Inquiry. The following provides detailed guidance concerning the conduct of a PI. The possibility of disciplinary or administrative action in a violation that does not include a compromise of CMI is just as real as in the case of a security violation that leads to compromise CMI.

a. Per the current edition of reference (b), a PI will be initiated when CMI is lost, compromised or subjected to compromise. The CO will assign an Officer to conduct the PI.

b. PIs will be conducted by an individual assigned external to the Security Branch or special staff sections requiring the inquiry. At a minimum, the Officer conducting the PI will complete the following actions:

c. Identify incident circumstances in the course of the inquiry as indicated:

(1) Identify the incident CMI completely and accurately. This identification should include the classification of the CMI, all identification or serial numbers, the date, the OCA or the derivative classifier and the derivative classification authority, the subject, downgrading and declassification instructions and in the case of documents, the number of pages involved.

(2) Identify all witnesses to the incident and informally interview them to determine the extent of the incident.

(3) Identify the individual responsible, if possible.

(4) Identify procedural weaknesses, security and otherwise, that allowed the incident to occur.

(5) Identify the incident to determine the extent of potential damage to national security and the action necessary to minimize the effects of the damage.

b. Establish either:

(1) That an unauthorized disclosure of CMI did not occur or that compromise may have occurred but under conditions presenting a minimal risk to national security.

(2) That compromise is confirmed or that the probability of damage to the national security cannot be discounted.

c. Determine overall classification of PI results. Every effort shall be made to keep the PI unclassified and without enclosures. However, if the lost information is beyond the jurisdiction of the U.S. and cannot be recovered, the PI shall be classified commensurate to the security classification level of the lost information to prevent its recovery by unauthorized personnel.

d. All PIs will be initially completed within three working days and reported via naval letter format to the Appointing Officer via the Command Security Manager. The Command Security Manager will then transcribe the PI into naval message format addressed to CMC (ARS), CNO (N09N2), the originators of lost or compromised CMI, OCAs if known, NCIS and or any other commands involved in the PI.

e. If during the conduct of the PI a determination is made that compromise or possible compromise in fact did not occur, the PI will still continue to completion to determine what security weaknesses existed that permitted the violation to occur. 2d MAW Commands will provide an info copy of PIs subject to this paragraph to the 2d MAW Command Security Manager.

f. If during the conduct of the PI a determination is made that compromise is confirmed or that probability of damage to national security cannot be discounted or a significant security weakness is revealed or punitive action is appropriate, the Command Security Manager will assist in converting the PI in naval letter format to naval message format, addressed to HQMC (ARS), CNO (N09N2), the originator, the OCA and the local NCIS office. When a PI determines that compromise has occurred or that damage to national security cannot be discounted or a significant security weakness is revealed or that punitive action is appropriate, a formal command investigation (JAGMAN) will be initiated.

5. JAGMAN Investigations. The purpose of the JAGMAN investigation is to provide a more detailed investigation and to recommend any corrective or required disciplinary actions when a PI confirms a compromise or that the probability of damage to national security cannot be discounted or a significant security weakness is revealed. Procedures for initiating, conducting and reporting a JAGMAN investigation is included in Chapter 12 of reference (b). Subordinate Commands will address their completed JAGMAN investigations to CNO Washington DC (N09N2) via Commander, 2d MAW and CMC Washington DC (ARS).

6. Investigative Assistance. A PI or JAG investigation may, under certain circumstances, require professional or technical assistance. The individual conducting the inquiry or investigation may seek the assistance of the Command Security Manager, the SJA, CI personnel assigned to the command or NCIS. All requests for assistance will be coordinated through the Command Security Manager.

7. Reporting Losses or Compromises of Special Types of Classified Information and Equipment

a. Report losses or compromises involving computer systems to the CNO (N09N2), who will notify the Director, Information Assurance, OASD (C3I). Subordinate Commands will route all correspondence involving losses or compromises via the 2d MAW Command Security Manager.

b. Report losses or compromises involving COMSEC via an Initial Report, per the procedures contained in the current edition of Electronic Key Management System (EKMS)-1. This Initial Report will suffice for the PI requirements of this Order and will be forwarded to the 2d MAW Command Security Manager, CNO (N09N2), NSA and the local NCIS office. No other deviations from the reporting procedures of this Chapter are authorized.

c. Report losses or compromises involving RD/CNWDI to the Marine Corps Forces Pacific (MARFORPAC) Command Security Manager, CMC (ARS) and CNO (N09N2) with a copy to the local NCIS office.

d. Report losses or compromises involving SCI per the current edition of DoD 5105.21-M-1, DoD Sensitive Compartmented Information Administrative Security Manual.

e. Immediately report incidents indicating a deliberate compromise of classified information or indicating possible involvement of a foreign intelligence agency, to the local NCIS office. 2d MAW units will info 2d MAW Command Security Manager on all correspondence involving losses or compromises.

8. Report of Finding CMI Previously Reported as Lost or Destroyed. When CMI previously reported as lost or destroyed is subsequently found, the Command Security Manager will be notified. 2d MAW units will info 2d MAW Command Security Manager on all correspondence involving CMI previously reported as lost or compromised.

9. Compromise Through Public Media. If any member of the MSC becomes aware that CMI may have been compromised as a result of disclosure in the public media, i.e., newspaper, magazine, radio or television, the member must notify the Command Security Manager, who in turn will notify the 2d MAW Command Security Manager, CMC (ARS) and the CNO (N09N2).

10. Unauthorized Disclosure Through Spillage. The term "Spillage" is an INFOSEC term that refers to any compromise incident where CMI is introduced on an IT System/Network that is not authorized to hold or process such data. Upon discovery of spillage, the contaminated device will be immediately disconnected from the network. Immediacy of this action is mandatory to prevent further contamination. The Command Security Manager and the Information Assurance Manager will be promptly notified and take appropriate action per current

JUL 18 2011

Information Assurance directives. Paragraph 4003 above provides detailed guidance concerning the conduct of a PI.

11. Security Violations. Security violations identified during unannounced after hours security inspections, involving or not involving the compromise of CMI, will be reported to the Command Security Manager. Normally, security violations demonstrate a weakness in the security program. For this purpose, a PI must also be vigorously and thoroughly conducted. This unit or special staff sections a "second chance" to shore up their security program before a compromise does occur.

12. Unsecured Security Containers. If a container in which CMI is stored is found unlocked in the absence of assigned personnel, report the incident immediately to the Command Duty Officer (CDO). The container will be guarded until the CDO arrives at the location of the unlocked container. The CDO will then inspect the CMI involved, lock the container and notify the Command Security Manager the following working day. If the CDO believes that the CMI may have been compromised, the CDO will immediately notify the Command Security Manager and recall the person responsible for the container to make a complete inventory.

13. Improper Transmission

a. All CMI received at 2d MAW is normally received via the CMCC. However, because confidential and secret CMI can be sent through either the U.S. Postal Service (USPS) (First Class REGISTERED) or the current holder of the GSA contract for overnight delivery services (i.e. FEDEX, Airborne Express, DHL, etc.), it is possible that 2d MAW Subordinate Commands and special staff sections could receive CMI directly from the mailroom or the overnight delivery carrier.

b. All official registered mail should be opened within the CMCC immediately upon receipt to ensure that it does not contain CMI. If CMI is received outside of CMCC, it should be immediately delivered to the Security Branch/CMCC with all wrappings and labels received, accompanied by a brief statement of circumstances (verbally or in writing).

(1) For all incoming CMI that shows improper handling where compromise is not assumed, such as addressing or improper preparation for transmissions, i.e., no inner wrapping, no classification marking on the inner wrapping, etc., the Command

WgO 5510.1T
JUL 18 2017

Security Manager will notify the transmitting command of the discrepancy via Security Discrepancy notice OPNAV 5511/11.

(2) All instances of mishandling, where compromise cannot be ruled out must be formally reviewed through a PI, as discussed in paragraph 4 above.

CHAPTER 5

COUNTERINTELLIGENCE MATTERS TO BE REPORTED
TO THE COMMAND SECURITY MANAGER

1. Policy. Certain matters affecting national security must be reported to the Command Security Manager, who will report the matter to NCIS. All military and civilian personnel, whether they have access to CMI or not, will report to their Command Security Manager or if on leave/TAD, the nearest command, any activities described in this chapter involving themselves, their dependents or others.

2. Sabotage, Espionage, International Terrorism or Deliberate Compromise

a. Individuals becoming aware of sabotage, espionage, terrorism, deliberate compromise or other subversive activities will immediately notify the Command Security Manager, who in turn will notify the local NCIS office. If the servicing NCIS office cannot be contacted immediately and the report concerns sabotage, terrorism, espionage or imminent flight or defection of an individual, the command will immediately contact the Director, NCIS (DIRNAVCRIMINSERV WASHINGTON DC) by SECRET IMMEDIATE naval message, with CG2DMAW//CMC WASHINGTON DC//ARS// and CNO WASHINGTON DC//N09N2// as an information addressee.

b. The Command Security Manager will be notified immediately of any requests, through other than official channels, for classified or national defense information from anyone without an official need-to-know, regardless of nationality. The Command Security Manager will also be notified of any requests for unclassified information from any individual believed to be in contact with a foreign intelligence service. Examples of requests to be reported include attempts to obtain: names, duties, technical manuals, regulations, command directories, alpha rosters or unit Table of Organization data; and information about the designation, strength, mission and combat posture of any command. The Command Security Manager will notify the local NCIS office of these requests.

3. Contact Reporting

a. All command personnel who possess a security clearance are to report to the Command Security Manager contacts with any individual, regardless of nationality, whether within or outside

Jul 18 2011

the scope of the individual's official activities in which illegal or unauthorized access is sought to classified or otherwise sensitive information; contacts include contacts in person, by radio, telephone, letter, e-mail or other forms of communication for social, official, private or any other reason.

b. Personnel must report to the Command Security Manager if they are concerned that they may be the target of exploitation. The Command Security Manager will review, evaluate and report the information to the local NCIS office.

4. Special Reporting Situations

a. Suicide or Attempted Suicide. When a member of the command commits suicide or attempts suicide, Subordinate Command Security Managers will immediately report the incident to the local NCIS office, the 2d MAW Command Security Manager and Department of the Navy Central Adjudication Facility (DONCAF). An incident report shall be submitted via JPAS. Additionally, command initiated investigations must be coordinated with the local NCIS office.

b. Unauthorized Absentees (UAs). When a member of the command, who currently has or has had access to CMI, is in an unauthorized absence status, the Command Security Managers will initiate an inquiry to determine if there are indications from the individual's activities, behavior or associations that the absence may be contrary to the interests of national security. If the inquiry develops such concerns, the Command Security Managers will report all information to the local NCIS office, info to 2d MAW Command Security Manager and DONCAF. NCIS will advise whether they will conduct an investigation. An incident report shall be submitted via JPAS, all access will be terminated.

c. Death or Desertion. When a member of the command, who currently has or has had access to CMI dies or deserts, the Command Security Managers will initiate an inquiry to identify any unusual indicators or circumstances that may be contrary to the interests of national security. If the inquiry develops such concerns, the Command Security Manager will report all information to the local NCIS office, info to 2d MAW Command Security Manager and DONCAF. NCIS will advise whether they will conduct an investigation. An incident report shall be submitted via JPAS, all access will be terminated; the subject will be removed from any JPAS owning or servicing relation.

JUL 18 2011

5. Foreign Connections

a. A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom the individual is bound by affection or obligation, are not citizens of the U.S. Having a financial interest in a foreign country may also present a security risk.

b. The assessment of risk due to an individual's relationship with foreign nationals and foreign entities is a part of the personnel security adjudicative process. Changes or issues regarding a cleared individual and his or her foreign connections should be reported to the DONCAF.

JUL 18 2011

CHAPTER 6

CLASSIFICATION MANAGEMENT1. Policy

a. EO 12958, as amended and EO 13292, further amendment to EO 12958, Classified National Security Information is the only basis for classifying information except as provided in the Atomic Energy Act of 1954, as amended. It is the policy of the DON to make available to the public as much information concerning its activities as possible, consistent with the need to protect national security. Therefore, information will be classified only to protect national security.

b. Information classified by DON OCAs shall be declassified as soon as it no longer meets the standards for classification in the interest of national security.

2. Original Classification Authority

a. The authority to originally classify information as TS, Secret or Confidential rests with the Secretary of the Navy and designees.

(1) 2d MAW does not have OCA by authority of the SECNAV as an agency head under EO 12958 and may not be further delegated.

(2) Commanders with authority for original classification decisions are listed as DON Original Classification Authorities in the CNO (N09N2) website at www.navysecurity.navy.mil. The website is updated as changes occur and should be relied on as a sole source of accurate OCA info.

(3) Deputy Commanders and the Chiefs of Staff may be empowered to exercise the OCA when they officially assume the OCA position in an "acting" capacity and have been trained and certified to the CNO (N09N2) their indoctrination in OCA duties and responsibilities.

b. When division, branch or special staff sections generate CMI, they will ensure that the material is signed off in the name of the Commander.

c. The Command Security Manager is responsible for providing the Commander, Deputy Commander and Chief of Staff, with OCA training in the fundamentals of security classification, the limitations of his classification authority and his OCA duties and responsibilities. The Command Security Manager shall prepare a written indoctrination letter for the Commander's signature, addressed to CNO (N09N2) confirming that training has been accomplished.

3. Original Classification Principles and Considerations. The following should be used as a guide in determining whether information/material should be classified:

a. Evaluate the information to form the basis for classification. Material is classified either because of the information it contains or because of the information it may reveal when associated with other information, including that already officially released into the public domain.

b. Identify the specific elements of information that serve as the basis for a particular national advantage and could adversely affect national security, if compromised.

c. Weigh the advantages and disadvantages of classifying. The decision to classify must be the result of a reasoned judgment.

d. Specific principles and considerations for original classification are contained in OPNAVINST 5513.1E, DON Security Classification Guides.

4. Specific Classifying Criteria

a. There are two decisions to be made by an OCA in making a determination to classify in the original classification process; first, that the information meets one or more of the criteria in sub-paragraphs 2.a. through 2.j. below; and second, that unauthorized disclosure of the information could cause damage to national security, because information may fall under one or more of the criteria below, do not presume that it automatically meets the damage criterion.

b. Consider classifying information if it concerns:

(1) Military plans, weapons or operations.

JUL 18 2007

(2) Vulnerabilities or capabilities of systems, installations, projects or plans relating to national security.

(3) Foreign government information.

(4) Intelligence activities (including special activities) or intelligence sources or methods.

(5) Foreign relations or foreign activities of the U.S.

(6) Scientific, technological or economic matters relating to national security.

(7) U.S. Government programs for safeguarding nuclear materials or facilities.

(8) Cryptology.

(9) A confidential source.

(10) Other categories of information related to national security and requiring protection against unauthorized disclosure as determined by the SECNAV.

c. Unauthorized disclosure of Foreign Government Information (FGI), the identity of a confidential foreign source or intelligence sources or methods, is presumed to cause damage to the national security. The level of classification is dependent on the anticipated degree of damage.

5. Classification Designations

a. Information which requires protection against unauthorized disclosure in the interest of national security must be classified in one of three designations: "TS", "Secret" or "Confidential." The markings for Controlled Unclassified Information, as defined in DOD 5200.1-R, January 1997, Appendix 3, such as "For Official Use Only," "Sensitive But Unclassified" (formerly "Limited Official Use"), "DEA Sensitive Information," "DoD unclassified Controlled Nuclear Information" and "Sensitive Information," as defined in the Computer Security Act of 1987, cannot be used to identify classified information, nor can an individual use modifying terms in conjunction with authorized classification designations such as "Secret Sensitive."

b. "TS" is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security.

c. "Secret" is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security.

d. "Confidential" is the designation applied to information the unauthorized disclosure of which could reasonably be expected to cause damage to national security.

6. Tentative Classification. All Commands that originate information believed to contain CMI, will take the following precautions:

a. Safeguard the information for intended classification.

b. Mark the information with the intended classification, preceded by the word "tentative."

c. Forward the information to an official identified in paragraph 6001 above for a security determination. If a determination cannot be made, then the material will be forwarded to the Command Security Manager for review.

7. Limitations on Classifying. Original classifiers may not:

a. Use classification to conceal violations of law, inefficiency or administrative error, to prevent embarrassment to a person, organization or agency or to restrain competition.

b. Classify basic scientific research information that is not clearly related to national security.

c. Classify a product of non-governmental research and development that does not incorporate or reveal CMI to which the producer or developer was given prior access, unless the government acquires a proprietary interest in the product.

d. Classify or use as a basis for classification, references to classified documents when the reference citation does not in itself disclose CMI.

e. Use classification to limit dissemination of information that is not classifiable under this Order or to prevent or delay the public release of the information.

8. Challenges to Classification. If a member of the command has substantial reason to believe that certain information is classified improperly or unnecessarily, whether originating from within DoD the matter will be referred to the member's Command Security Manager for review.

9. Duration of Original Classification

a. Information will be classified for as long as required by national security considerations. OCAs should assign dates or events for declassification whenever possible. Chapter four of reference (b) provides instructions on establishing durations of original classifications.

b. Only OCAs may extend a specified duration of classification and only if all known holders of the information can be notified prior to the date or event originally set for declassification.

10. Derivative Classification

a. Original Classification is the initial determination that, in the interest of national security, information requires protection against unauthorized disclosure and a further determination of level of protection required. However an estimated 99 percent of the classified information produced by Commands is derivatively, rather than originally classified.

b. Derivative Classification can be accomplished by anyone who incorporates, paraphrases, restates or generates in new form, information that is already classified, while retaining consistency in marking that apply to the source. This includes classification of information based on OCA classification guidance (Security Classification Guides(SCG)).

(1) SCGs serve both legal and management functions by recording DON original classification determinations made under EO 12958, as amended and EO 13292, further amendment to EO 12958, Classified National Security Information.

(2) SCGs are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements.

(3) SCGs for systems, plans, programs or projects involving more than one DoD component are issued by the Office

of the Secretary of Defense (OSD) or other DoD component designated by the OSD as executive or administrative agent.

c. A derivative classifier must:

(1) Observe and respect original classification decisions made by the OCAs, as codified in classified source documents and security classification guides.

(2) Use caution when paraphrasing or restating information extracted from a classified source document to determine whether the classification may have been changed in the process.

(3) Carry forward to any newly created documents the pertinent classification and declassification markings, per EO 12958, as amended and EO 13292, further amendment to EO 12958, Classified National Security Information.

11. Accountability of Classifiers. Original and derivative classifiers are accountable for the accuracy of their classification decisions. Officials with command signature authority shall ensure that classification markings are correct. Any questions regarding original or derivative classification should be referred to the Command Security Manager for resolution.

12. Foreign Government Information (FGI). If any Command with 2d MAW received CMIs originated by a foreign government. The following guidelines pertain to the protection of FGI.

a. Information classified by a foreign government or international organization retains its original classification designation or it is assigned a U.S. designation that will provide protection equivalent to that provided by the originator of the information. Authority to assign the U.S. designation does not require an OCA.

b. FGI provided with the expectation, expressed or implied, that it, the source or both are to be held in confidence, must be classified by an OCA. Because EO 12356 presumes damage to the national security will occur if that information is disclosed, FGI must be classified at least Confidential. It may be classified at a higher level if it meets the damage criteria of paragraph 6003 above.

JUL 18 2011

c. Do not assign a date or event for automatic declassification to FGI unless specified or agreed to by the foreign entity. If no guidance is provided by the foreign government, declassification instructions will be determined with the assistance of the Command Security Manager and CNO (N09N2).

JUL 18 2011

CHAPTER 7

CLASSIFICATION REVIEW

1. Policy. The Command Security Manager must provide for the systematic review of locally produced CMI (either original or derivatively classified) to ensure correct classification and marking and to comply with certain reporting requirements of the Information Security Oversight Office (ISOO).

2. Marking Requirements. All CMI within 2d MAW and its Subordinate Commands shall be clearly marked with the date and office of origin, the appropriate classification level and all required "Associated Markings." "Associated Markings" include those markings that identify the derived source of classification (or for original decisions, the authority and reason for classification); downgrading and/or declassification instructions; and warning notices, intelligence control markings and other miscellaneous markings. Marking guidance contained in the following documents is to be adhered to:

- a. Reference (b) Chapter six.
- b. EO 12958, as Amended, Classification Marking Guide.
- c. DoD 5200.1-PH, DoD Guide to Marking Documents.

3. Review Requirements. The Command Security Manager has responsibility for ensuring all locally produced CMI (either originally or derivatively classified) is reviewed upon completion for appropriate classification and marking. The Command Security Manager may delegate the authority to complete these reviews to the command or special staff section Security Assistants.

a. The Command Security Manager will provide training to the Security Assistants in the performance of their reviewing duties.

b. All CMI produced and reviewed will be registered with the CMCC.

c. The Command Security Manager retains the right to provide final determination of proper classification and marking.

JUL 18 2011

4. Mandatory Declassification Reviews. Mandatory declassification is the review for declassification of CMI information in response to a specific request. If tasked to conduct a mandatory review, details of the requirements can be found in Chapter four of reference (b).

JUL 18 2011

CHAPTER 8

CMI CONTROL MEASURES1. Policy

a. Commanders shall ensure that CMI is processed only in secure facilities, on accredited Automated Information Systems (AIS) and under conditions that prevent unauthorized persons from gaining access.

b. CMI is the property of the U.S. Government, not personal or contractor property. CMI must be controlled through its entire life cycle.

(1) Regarding "personal notes" taken during classified briefs or training: they are considered "working papers" and contain classified elements that are the property of the U.S. Government. Therefore they are to be controlled per the provisions of this Order to include transmittal, safeguarding and destruction.

(2) Classified Hard Disk Drives (HDDs) residing in SIPRNET computers will be marked with appropriate magnetic media classification labels and will be entered into the CMCC accounting system by serial number or six digit control number. The control number can be made up of numbers and letters. The HDDs contain classified elements that are the property of the U.S. Government; local procedures must be established to insure positive control is maintained on the HDDs through their life cycle terminating in approved purging or destruction.

c. Military or civilian personnel who are relieved of classified duties, transfer, resign, retire, separate from the DON or are released from active duty, shall return all classified information in their possession to their SCP or CMCC as applicable prior to assuming new duties, accepting final orders or separation papers.

2. Applicability of Control Measures. Classified information must be afforded a level of accounting and control commensurate with its assigned security classification level. The control measures defined in this chapter encompasses all classified information regardless of the media on which it may be represented.

JUL 18 2011

3. Top Secret Control Measures

a. All TS CMI (including copies) received by 2d MAW and Subordinate Commands shall be continuously accounted for, individually serialized with a locally developed "control number" and entered into a command TS Control Log. The log shall completely identify the information and at a minimum, include the date originated or received, individual serial numbers, copy number, title, change number if applicable, originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified, etc.) and date of each disposition action taken. The TS Control Log will be retained for five years after the material is transferred, downgraded or destroyed.

b. In addition to the marking requirements of Chapter six of reference (b), TS derivatively classified by 2d MAW or Subordinate Commands shall be marked on their "control number" with an individual copy number in the following manner "Copy No. __ of __ copies;" exceptions to this rule are allowed for publications containing a distribution list by copy number. In this case, adequate and readily available documentation shall be maintained indicating the total copies produced and the recipients of the copies.

c. OCA developed TS CMI will not be copied without the consent of the originator. Derivatively classified material may be copied with approval from the command's TSCO.

d. Working papers that contain TS information require the applicable TS accounting, control and marking requirements prescribed for finished product CMI.

e. TS documents will contain a list of effective pages which will include a Record of Page Checks. When this is impractical, as in correspondence or messages, number the pages in the following manner "Page __ of __ Pages."

f. The TSCO will page check TS documents for completeness and accuracy on initial receipt and after entry of a change involving page entry or removal. (The change residue, including pages removed, must also be page-checked before destruction.) Page checks by the relieving Officer, upon relief of the TSCO, are required.

g. TS documents will be physically sighted or accounted for by examination of written evidence of proper disposition, such

JUL 18 2017

as certificate of destruction, transfer receipt, etc., at least once annually and more frequently when circumstances warrant. At the same time, TS records will be audited to determine completeness and accuracy.

h. Retention of TS documents within 2d MAW and its Subordinate Command will be kept to a minimum. When TS CMI is destroyed, the CMCC section will prepare a Classified Material Destruction Report, OPNAV 5511/12 identifying the material destroyed and the two officials who witnessed its destruction, and their signatures. The TSCO will retain these destruction records for a period of five years.

i. Whenever TS or Secret CMI changes hands, the TSCO must ensure it is done under a continuous chain of receipts. This continuous chain of receipts may be documented on a Correspondence/Material Control (four PT), OPNAV 5216/10. TSCOs shall obtain a classified material receipt, which may be documented on a correspondence/Material Control (four PT), OPNAV 5216/10, from each recipient for TS information distributed externally.

j. TS CMI is disclosed to properly cleared personnel only on a need-to-know basis. Personnel authorized to handle TS CMI must always use extreme care to prevent unauthorized or inadvertent access to it.

k. When TS messages of an urgent nature are received requiring an immediate response, the recipient and TSCO will both be notified promptly so that the necessary action can be taken to answer the requirements of the message and simultaneously bring the message under control.

l. See reference (b) for additional TSCO duties.

4. Secret Control Measures

a. Commanders shall establish procedures for the control of Secret CMI based on the local environment and an assessment of the threat, the location and the mission of the command. The CMCC shall be the focal point of all activity involving Secret control; administrative procedures will include the following:

(1) Records of CMI originated, received or reproduced by the command.

JUL 18 2011

(2) Records of CMI distributed or routed to sub-elements of or activities within the command.

(3) Records of CMI disposed of by the command through transfer of custody or destruction.

(4) Requirements for an annual inventory.

b. Signed receipts are required for accountable Secret CMI distributed or routed within the command. All Secret CMI transferred from one section to another within the command will be routed through their CMCC.

c. Correspondence/Material Control Sheets (four PT), OPNAV 5216/10 or a locally developed "buck-tag" will be attached to all Secret CMI under the control of CMCC; classified removable HDD will have the "buck-tag" affixed with the HDDs serial number or the six digit control created by the command.

d. When transmitting Secret CMI to another command, CMCC will enclose a receipt identifying the material. This receipt must be signed and returned to the transmitting command, regardless of the method of transmission. The registered mail receipt does not replace the Secret receipt. A registered mail receipt merely acknowledges that a package was received; it doesn't assure the sender that each piece of Secret CMI has been entered into the accountability system of the recipient. The transmitting command is responsible for the classified material until the recipient signs the receipt and returns it.

5. Secret Naval Messages and E-mail. Due to the large volume of Secret messages and e-mails available through SIPRNET, decentralized printing, copying and accounting procedures at the SCP level is authorized. The following guidance is to be adhered to:

a. SCPs will establish accounting procedures for each stand-alone (not part of a set of working papers) Secret message or e-mail maintained.

b. SCPs are authorized to destroy Secret messages and e-mails without record. This rule does not pertain to "special handling" messages, which are under the control of CMCC, for copying, accounting, distribution and destruction.

c. All other SECRET CMI printed from the SIPRNET will be:

NOV 18 2011

(1) Reviewed to ensure it is properly marked, contacting the originator for determination if no markings exist.

(2) Reviewed for disposition; one of the following procedures apply:

(a) Turn over to the CMCC for entry into their accounting system.

(b) Mark as "working papers."

(c) Turn over to SCP for immediate destruction by authorized means.

d. Marking e-mail generated on the SIPRNET

(1) All SIPRNET generated e-mail must be marked, prior to transmission, with appropriate security classification and associated markings, including UNCLASSIFIED; this applies to all elements of the e-mail: subject, body, portions and attachments.

(2) 2d MAW and Subordinate Commands are encouraged to use Commercial Off-the-Shelf (COTS) software on their SIPRNET computers, requiring SIPRNET e-mail users to select the appropriate classification and associated markings prior to sending the e-mail.

6. Secret Working Papers

a. Secret working papers such as classified notes from a training course or conference, research notes, rough drafts and similar items that contain Secret information shall be:

(1) Dated when created.

(2) Conspicuously marked, center top and bottom, of each page with the highest overall classification level of any information they contain, along with the words "Working Papers."

(3) Protected per the assigned classification level.

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

b. All Secret working papers, retained for more than 180 days from the date of creation, will be entered into the CMCC accounting system prescribed for finished product CMI.

c. All Secret working papers to be transferred from the command, regardless of date of creation, will be entered into the CMCC accounting system prescribed for finished product CMI prior to its transfer via the CMCC.

7. Confidential Control Measures. The control requirements of Confidential information is less stringent than those for Secret: decentralized printing, copying and accounting and disposition procedures at the SCP level is authorized. The following guidance is to be adhered to:

a. SCPs will establish their own control procedures for accounting for finished product Confidential CMI.

b. SCPs are authorized to destroy Confidential CMI without record. This rule does not pertain to "special handling" material, which are under the control of CMCC, for copying, accounting, distribution and destruction.

8. Confidential Working Papers

a. Confidential working papers such as classified notes from a training course or conference, research notes, rough drafts and similar items that contain Confidential information shall be:

(1) Dated when created.

(2) Conspicuously marked, center top and bottom, of each page with the highest overall classification level of any information they contain, along with the words "Working Papers."

(3) Protected per the assigned classification level.

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

b. All Confidential working papers, retained for more than 180 days from the date of creation, will be entered into the command or special staff section SCP accounting system prescribed for finished product CMI.

c. All Confidential working papers to be transferred from the command within 180 days of creation will be entered into the CMCC accounting system prescribed for finished product CMI, prior to its transfer via the CMCC.

9. Special Handling Requirements. Commanders, with the advice of the Command's Security Manager, must establish security rules and procedures for the control of "special handling" messages and material, such as Special Category (SPECAT), Limited Distribution (LIMDIS) and "Personal For (P4s)."

10. Control Measures for Special Types of Classified and Controlled Unclassified Information

a. RD and Formerly Restricted Data (FRD). RD, including CNWDI is controlled per the current edition of DoD Directive 5210.2, access to and dissemination of restricted data.

b. SCI. Control SCI per the current edition of DoD 5105.21-M-1, DoD Sensitive Compartmented Information Administrative Security Manual. SCI is managed under the SSO.

c. COMSEC Material. Control COMSEC per the current edition of EKMS-1, Electronic Key Management System.

d. For Official Use Only (FOUO). Control FOUO per the current edition of SECNAVINST 5720.42F, DON Freedom of Information Act.

e. Sensitive But Unclassified (SBU) Information. Control SBU information per the current edition of SECNAVINST 5720.42F, DON Freedom of Information Act.

f. Controlled Unclassified Information (CUI). DoD 5200.1-R, January 1997, Appendix 3, Controlled Unclassified Information, covers several types of unclassified controlled information, including "DEA Sensitive Information," "DoD Unclassified Controlled Nuclear Information," "Sensitive Information," as defined in the Computer Security Act of 1987 and provides basic procedures for identification and control.

CHAPTER 9

CMI DISSEMINATION

1. Policy

a. Within 2d MAW and its Subordinate Commands, the dissemination of classified and controlled unclassified material, which was either originated or received at the individual commands, will be kept to a minimum consistent with operational requirements and based on the need-to-know principle.

b. All CMI dissemination external to the command will be conducted in accordance with the guidance contained in Chapter nine of reference (b).

c. Non-DoD originated classified materials will not be distributed outside of the DoD without the approval of the originating department or agency.

2. Top Secret Dissemination. Internal to the command, all TS CMI will only be routed from the TSCO to an SCP and returned to the TSCO. TS CMI will not be routed from one SCP to another SCP.

3. Secret Dissemination. Internal to the command, Secret CMI, with the exception of working papers, e-mails and naval messages, will not be permanently routed from one SCP to another SCP without being processed via the CMCC for appropriate accountability. An exception to this procedure is authorized for temporary loan of CMI not to exceed 10 days duration; however, nothing herein shall be construed as relieving either SCP from exercising appropriate accountability and control of temporarily loaned CMI. The borrowing SCP will not make copies of the CMI without processing the CMI through the CMCC.

4. Confidential Dissemination. Internal to the command, the dissemination requirements of Confidential CMI are less stringent than those for Secret CMI. Confidential CMI may be permanently routed from one SCP to another SCP without being processed via the CMCC.

JUL 13 2011

5. Dissemination of Special Types of Classified and Controlled Unclassified Information

a. SCI. SCI will only be disseminated per the provisions of the current edition of DoD 5105.21-M-1, DoD Sensitive Compartmented Information Administrative Security Manual (IASM), under the management of the SSO.

b. RD and FRD including CNWDI. RD, FRD and CNWDI will only be disseminated per the provisions in the current edition of DoD Directive 5210.2, Access to and Dissemination of RD and reference (a), DoN Personnel Security Program Regulation.

c. Cryptographic and COMSEC Distributed Information. All cryptographic and COMSEC distributed information will be disseminated per the provisions of the current edition of the EKMS-1.

d. FOUO. FOUO material may be disseminated within DoD components. All requests from non-DoD entities to disseminate FOUO outside 2d MAW and its Subordinate Commands must be routed through the command's Freedom of Information Act (FOIA) Officer.

e. SBU. SBU material will be handled in the same manner as FOUO.

f. Sensitive Information. Sensitive information as defined by the Computer Security Act of 1987 shall be disseminated on a need-to-know basis.

6. Dissemination to Contractors. Cleared personnel, to include cleared contractors, are prohibited from discussing or releasing classified information and documents with other contractors regardless of their level of clearance, unless the visit has been approved through the Command Security Manager and the contractor has need-to-know as defined in his contract.

7. Disclosure to Foreign Governments and International Organizations. Command personnel will not discuss CMI with representatives of foreign governments or international organizations unless approved by the Command Security Manager. At no time will classified or unclassified documents be released to representatives of foreign governments or international organizations.

8. Dissemination of Intelligence Material. The dissemination of intelligence materials will be controlled by the local AC/S

JUL 18 2011

G-2 within all of 2d MAW. All requests for intelligence information will be provided/forwarded to the local AC/S G-2 for appropriate action.

9. Pre-Publication Review. All material prepared for public release in any format will be subject to an Intra-Command Security Review per the current edition of the reference (g) and MCO 5510.9.

JUL 18 2011

CHAPTER 10

CMI SAFEGUARDING

1. Policy. CMI will be used only where there are facilities or conditions, adequate to prevent unauthorized persons from gaining access to it. The exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances. Security requirements must permit the accomplishment of essential functions while affording CMI appropriate security. The requirements specified in this Order represent the minimum acceptable standards.

2. Responsibility for Safeguarding

a. Command personnel in possession of CMI are responsible for safeguarding it at all times and particularly for locking CMI in appropriate security containers whenever it is not in use or under the direct supervision of authorized persons. Personnel must follow procedures that ensure unauthorized persons do not gain access to CMI by sight, sound or other means. CMI will not be discussed with or in the presence of unauthorized persons.

b. Individuals will not remove CMI from designated offices or working areas except in the performance of their official duties and under conditions providing the protection required by this Order. Under no circumstances will an individual remove CMI from designated areas to work on it during off duty hours or for any other purpose involving personal convenience.

3. Restricted Areas

a. Within military facilities, there are areas with differing degrees of security importance, depending upon their purpose and the nature of the work conducted therein. To meet the security needs of these restricted areas requires the application of protective measures commensurate with these varying degrees of security importance.

b. To facilitate the varying degrees of restricted access, control of movement and the type of protection required for CMI, the following applies to restricted areas:

(1) Level Three. An area containing CMI, which is of such a nature that unauthorized access to the area would cause GRAVE DAMAGE to the mission or national security. Only persons

JUL 18 2011

whose duties actually require access and who have been granted the appropriate security clearance will be allowed into level three areas.

(2) Level Two. An area containing CMI and in which uncontrolled movement would permit access to CMI that would cause SERIOUS DAMAGE to the command mission or national security if compromised. All persons admitted to a level two area with freedom of movement must have an appropriate security clearance. Persons who have not been cleared for access to the information contained within a level two area may with appropriate approval, be admitted to the area but they must be controlled by an escort, attendant or other security procedures to prevent access to CMI.

(3) Level One. An area within which uncontrolled movement will not permit access to CMI, but if compromised, would cause DAMAGE to the command mission and national security. This area is designed for the principle purpose of providing administrative control, safety or a buffer area of security restriction for limited or exclusion areas.

c. Level one, two and three areas will not be designated in any way that outwardly notes their relative sensitivity. Identify any such areas as a "RESTRICTED AREA." In locations where a language other than English is prevalent, display restricted area warning notices in English and the local language. Signs for restricted areas, in both English and foreign languages, may be contracted for from Naval Surface Warfare Center (NSWC) Crane, Indiana (Code 4044).

d. All restricted areas require a Physical Security Survey conducted by the servicing PMO on an annual basis. To this end Command Security Managers will review their assigned restricted areas by level and report same to their servicing PMO annually on a calendar year basis during the month of January.

4. Safeguarding Working Spaces

a. All working spaces containing classified information should be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified information, specifically including security measures to prevent persons outside the building or spaces from viewing or hearing classified information.

JUL 18 2011

b. All office spaces where material is stored, processed or discussed should be sanitized when un-cleared personnel are performing repairs, routine maintenance or cleaning. These individuals will be escorted at all times and all individuals will be alerted to their presence.

c. Ensure adequate controls are established to prevent unauthorized individuals gaining access to areas where classified material can be adrift.

d. Extraneous material (such as unclassified papers and publications) should be kept off the tops of security containers to prevent inadvertent intermingling of classified with unclassified material.

e. Burn bags will not be co-located with trash receptacles as the subconscious act of discarding waste material could result in classified material being discarded with regular trash.

f. Classified information shall not be discussed over unsecured telephone lines. Secure Telephone Equipment (STE) and Secure Telephone Unit, Third Generation (STUIII) are special instruments that can be switched to a secure mode for discussion of classified information. Caution should be used during the unclassified portion of the call that goes on before the secure telephone is switched to secure mode to ensure the conversation remains unclassified. Additionally, the level of conversation shall not exceed the accredited classification level of the secure phone.

g. Do not store or process CMI on any unclassified AIS system. Do not download and transfer any unclassified CMI from a classified AIS system to an unclassified AIS system without explicit approval and assistance from the Information Assurance Manager (IAM).

h. Current 2d MAW policy prohibits, cameras, photo-capable cell phones or wireless Personal Electronic Devices (PEDs), to include "cordless phones" in areas where classified material is stored or processed unless jointly approved by the Command Security Manager and the IAM. The use of these devices poses a serious threat to national security.

i. Technical Surveillance Countermeasure (TSCM) Services are available to Commanders for the purpose of detecting any attempts to obtain classified information from command

JUL 18 2011

restricted areas, through the use of clandestine listening devices. All TSCM service requests will be classified at the Secret level and will support surveys of meeting venues where Top Secret CMI will be processed or discussed; requests will be forwarded to the servicing NCIS Resident Agent.

5. Safeguarding During Working Hours. During working hours, take the following precautions to prevent access to classified information by unauthorized persons:

a. After removing classified documents from storage, keep them under constant surveillance and face down or covered when not in use. Classified material cover sheets, Standard Form (SF) 703, 704 or 705 or reasonable facsimiles thereof, are the only forms authorized for covering classified documents.

b. All classified and unclassified AIS recording media, (including classified HDDs, excluding unclassified HDDs), shall be marked with an SF 706, 707, 708, 709, 710, 711 or 712 SCI as applicable.

c. All Non-classified Internet Protocol Router Network (NIPRNET) computers and cabled peripherals (with the exception of keyboards, mice and speakers) will be labeled with "SENSITIVE UNCLASSIFIED" System Accreditation Labels, IRM-523908A. All SIPRNET computers and cabled peripherals will be labeled with "SECRET" System Accreditation Labels, CCO 5230.3.

d. Discuss classified information only if unauthorized persons cannot overhear the discussion. Take particular care and alert fellow workers when visitors or maintenance workers are present.

e. Protect preliminary drafts, notes, worksheets, computer storage media, ribbons and carbons and all similar items containing classified information. Either destroy them using an approved method or give them the same classification and safeguarding as the original classified material held.

f. End of the day security check procedures are facilitated with the use of Activity Security Checklist, Standard Form 701. These forms, modified if necessary to accommodate local conditions, are to be used to ensure that all areas which process classified information are properly secured. Additionally, an SF 702, Security Container Check Sheet, shall be utilized to record that classified vaults, secure rooms and containers have been properly secured at the end of the day.

JUL 18 2011

The SF 701 and 702 shall be annotated to reflect after hours, weekend and holiday activities in secure areas. These form should be maintain for 60 days after completely fill in.

6. Safeguarding in Storage

a. Commanders are responsible for the safeguarding of all classified information the within their commands which includes ensuring CMI either not in use or under personal observation of an appropriately cleared person shall be guarded or stored in a locked GSA-approved security container, vault, modular vault or secure room. Electrically actuated locks (for example, cipher and magnetic strip card locks) do not afford the degree of protection required for classified information and are prohibited for use in safeguarding classified material.

b. Detailed specifications and requirements for safeguarding in storage are addressed in Chapter ten of reference (b), DoN ISP. Additional information relevant to command responsibilities in this reference include:

- (1) Key and Lock control.
- (2) Safe and Door combination changes.
- (3) Records of security container combinations.

c. Commanders must develop, with assistance from the Command Security Manager local procedures for emergency access to locked security containers.

7. Safeguarding During Visits. Commanders shall establish procedures to ensure that only visitors with an appropriate clearance level and "need-to-know" are granted access to classified information. At a minimum, these procedures shall include verification of the identity, clearance level, access (if appropriate) and need-to-know for all visitors. Visitor control procedures are contained in Chapter eighteen of this Order.

8. Safeguarding During Classified Meetings

a. Commanders shall ensure that classified discussions at meetings are held only when disclosure of the information serves a specific U.S. Government purpose. Current office of the Secretary of Defense policy directs classified meetings shall be held only at a U.S. Government agency or a cleared DoD

contractor facility with an appropriate Facility Clearance (FCL) where adequate physical security and procedural controls have been approved.

b. TSCM Services are available to Commanders for the purpose of detecting any attempts to obtain classified information from meeting venues through the use of clandestine listening devices. All TSCM service requests will be classified at the Secret level and will support surveys of meeting venues where TS CMI will be processed or discussed; requests will be forwarded to the Command Security Manager.

c. Telephones, office intercommunications, public address systems and imaging systems will not be permitted in classified meeting venues or conference rooms, except those devices previously accredited to transmit classified material by the IAM. All PEDs, standard or wireless, such as cell phones, audio recorders, imaging devices, blackberry's, are prohibited within classified conference rooms.

d. Permit note taking during the classified session of the meeting only if such action is necessary and safeguard, transmit and transport classified information created, used or distributed during the meeting per the procedures contained in this Order and reference (b).

9. Safeguarding CMI while being Hand Carried. Internal to the command, classified cover sheets are required on all classified documents when they are not secured in a safe (when visual access is available to persons not having the proper clearance or need-to-know). Bulk materials will also be protected with appropriate covers to prevent casual observation by unauthorized personnel. Personnel should assume that visual access is available any time classified material is outside of its secure storage container. Use the following classified cover sheets:

- a. CONFIDENTIAL: Standard Form 705.
- b. SECRET: Standard Form 704.
- c. TS: Standard Form 703.

10. Safeguarding CMI while in Travel Status

a. If there is a compelling requirement to hand carry CMI while traveling off base on official business, the individual must be designated as a "courier." A designated courier must

hold either a DD Form 2501 courier card or a courier letter authorizing the conveyance of CMI. The Commander or his designated representative, usually the Command Security Manager, must sign the authorization.

b. Couriers traveling OCONUS, where the courier's mode of travel is other than government conveyance, must receive pre-approval by the 2d MAW Command Security Manager prior to embarking. Whenever this delegated authority is exercised, a copy of the letter prepared per Paragraph 9-13 of reference (b) will be provided to the 2d MAW Command Security Manager via NIPRNET e-mail or fax.

c. CMI must be double wrapped when hand carried outside the command. A locked briefcase may serve as the outer cover, except when hand carrying aboard commercial aircraft.

d. CMI may not be read, studied, displayed or used in any manner on a public conveyance or in a public area.

e. When CMI is carried in a private, public or government conveyance, it will not be stored in any detachable storage compartment, such as an automobile luggage rack, aircraft travel pod or modified "drop" tank.

f. Couriers will be briefed in the following safeguard requirements.

(1) The CMI will be in the courier's possession at all times, unless proper storage at a U.S. Government activity (such as U.S. Military bases, American Embassies or appropriately cleared DoD contractor facilities (within the U.S. only)) is available.

(2) Hand carrying CMI on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage in a U.S. Government activity. The Command Security Manager must approve the use of such a facility prior to the courier conducting the travel.

(3) When surrendering any package containing CMI for temporary storage (e.g., overnight or during meals), the courier must obtain a receipt signed by an authorized representative of the contractor facility or government installation accepting responsibility for safeguarding the package.

JUL 18 2011

g. A list of all classified material carried or escorted will be maintained by the CMCC and must be accounted for upon return through the receipts system.

h. Unless unusual circumstances exist, all courier routes are one way; hand carried classified material will be returned to the originating headquarters by one of the approved methods of transmission, preferably via Registered U.S. Mail.

11. Safeguarding CMI located in Foreign Countries

a. Commands located outside the U.S. and its territories require an Emergency Destruction Supplement for their Emergency Plan. Commands should conduct emergency destruction drills annually to ensure personnel are familiar with the plan and associated equipment. Any instances of incidents or emergency destruction of classified information shall be reported to the 2d MAW Command Security Manager.

b. The priorities for emergency destruction are:

(1) Priority One - TS CMI.

(2) Priority Two - Secret CMI.

(3) Priority Three - Confidential CMI.

c. For effective emergency destruction planning, limit the amount of classified information held at the command and if possible, store less frequently used classified information at a more secure command. Consideration shall be given to the transfer of the information to AIS media, which will reduce the volume needed to be transferred or destroyed. Should emergency destruction be required, any reasonable means of ensuring that classified information cannot be reconstructed is authorized?

d. Commanders should take into account the following factors to develop practical, reasonable emergency destruction plans: volume, level and sensitivity of the classified material held by the activity. Proximity to hostile or potentially hostile countries with unstable governments and the degree of defense the command and readily available supporting forces can provide.

e. The Emergency Destruction Supplement shall emphasize the procedures, methods (e.g. document shredders or disintegrators) and location of destruction; indicate the location of classified

JUL 18 2011

information and priorities for destruction; identify personnel responsible for initiating and conducting destruction; authorize the individuals supervising the destruction to deviate from established plans if warranted; and emphasize the importance of beginning destruction in time to preclude loss or compromise of classified information.

CHAPTER 11

CMI DUPLICATION AND DISTRIBUTION1. Policy

a. The policy within 2d MAW and its Subordinate Commands is to keep the duplication and distribution of classified material to the absolute minimum while maintaining operational effectiveness. In order to accomplish this, prohibitions, restrictions and other management controls must be placed on the duplication and distribution methods of CMI. Prohibitions are as follows:

(1) Wireless personal devices pose an unacceptable risk to national security. Therefore, wireless PEDs and other innovative secondary storage media devices that use the electromagnetic spectrum to remotely transfer data without physical connections are not approved for storage, processing or transfer of CMI and are strictly prohibited in any area where CMI is processed, stored or discussed.

(2) USB "Pen Drives" or "Thumb Drives" pose a substantially high risk to national security, therefore until further notice, use of any these portable secondary media storage device which uses a Universal Serial Bus (USB) connection is prohibited on the Marine Corps Enterprise Network (MCEN), both NIPRNET and SIPRNET. (See MARADMIN 647/08).

b. Before controls can be implemented, the methods must be defined. Few definitions could be all-inclusive given the fast pace of technology, however the following are provided as they currently represent the most common methods by which CMI may be duplicated or prepared for distribution, subject to the rules defined in later paragraphs of this chapter.

(1) Duplication: reproduction refers to large-scale initial print or duplication jobs normally tasked to a cleared professional team within a cleared reproduction facility, which renders CMI proof material into printed-paper product, collated and bound as required.

(2) Imaging, consisting of copying, faxing and scanning to fax or copy is included as a method of CMI duplication and can be rendered on accredited multipurpose or single purpose devices, desktop or stand-alone. These devices have the ability

~~JUL~~ 18 2011

to render a paper copy of CMI locally or in the case of faxes, to send a copy of CMI to a distant-end machine via secure telephone line.

(3) Printing is a method of duplicating CMI resident on a classified network, drive or secondary storage device accessible by an accredited classified computer which is either direct or network-linked to an accredited classified printer, either desktop or stand-alone.

(4) Audio/visual duplication of CMI can be through the use of photos, videos and audio recordings captured via currently available and approved methods that are formatted for distribution exclusively outside an accredited classified computer network. Hand written transcripts or notes of classified oral briefings or conversations, qualify as audio CMI duplication and will be handled accordingly.

b. Distribution:

(1) Removable secondary storage media devices can retain file copies of CMI to facilitate non-network file distribution. Secondary storage media is considered any non-volatile storage media. A non-volatile storage medium retains its data after the device is turned off or removed from the data processing device. Examples of removable secondary storage media are floppy diskettes, zip disks, cd-roms, fire wire hard drives, PCMCIA hard drives, flash media, memory cards (compact flash (CF)), smart media, memory stick, jump drives, etc. and other PEDs that are capable of storing information.

(2) Conventional secondary storage media devices are designed to download files and data while physically connected to a drive or device on an accredited classified computer and then allow for non-network file transfer when physically introduced to another accredited classified computer's drives and devices. Certain secondary storage media pose a substantially high risk to national security particularly the USB "pen" and "thumb" drives.

(3) Wireless secondary storage media devices, primarily defined as Wireless PEDs can also accomplish computer file copy to facilitate non-network file distribution, however it is a remote function using the electromagnetic spectrum through the atmosphere, rather than direct through physical connections. As such, the wireless devices pose an unacceptable risk to national security.

c. A discussion of classified computer HDD primary storage is covered under paragraphs 8000.2.b, 80003.3 and 10004.2 of this Order.

d. For purposes of this Order, all "finished product" and "working paper" CMI computer files of any type maintained within an accredited classified computer hard drive or shared within a classified network drive or classified website, will be subject to CMCC control only when rendered by one of the applicable and approved duplication methods described above; Chapter eight of this Order details the procedures to follow for CMCC control.

e. Ultimately, the Commander is responsible for protecting the classified material under his cognizance and barring specific guidance from higher authority, must determine if the controls he has established on emerging methods for duplication and distribution effectively mitigate risks to national security.

2. Controls on Reproduction. The Command Security Manager exercises responsibility for the reproduction of all CMI within his/her command.

a. Command Security Managers will ensure the CMCC is the only section that can approve the reproduction of CMI at locally authorized reproduction facilities. Command Security Managers will confer with the TSCO to determine procedures and authorizations for the reproduction of TS CMI.

b. All classified projects for reproduction will be delivered to the CMCC to ensure documents are correctly marked prior to reproduction. Materials not properly marked will be returned to the requesting section for correction.

c. All original and reproduced CMI will be returned directly from the reproduction facility to the CMCC for appropriate controls as required by Chapter eight of this Order.

d. Samples, waste or overruns resulting from the reproduction process will be safeguarded according to the classification of the information involved. This material will be promptly destroyed as classified waste.

3. Controls on Copy Devices. To maintain positive control of CMI, the following rules apply to copying:

JUL 18 2011

a. Accountable (finished product) CMI will only be copied by the CMCC on a "classified copier."

b. TS CMI will not be copied except by the TSCO or his designee, on an approved "classified copier" and only with the approval of the originator.

c. SCI will only be copied by the SSO.

d. Confidential and Secret messages and working papers may be copied by the command and special staff sections under the following conditions:

(1) The command or special staff section has a "classified copier" that has been approved by the Command Security Manager for copying CMI.

(2) Classified copiers will be prominently marked:

"THIS DEVICE IS AUTHORIZED FOR PROCESSING CLASSIFIED MILITARY INFORMATION UP TO AND INCLUDING (classification), BY DIRECTION OF THE COMMAND SECURITY MANAGER. USE OF THIS DEVICE TO PROCESS CMI MUST BE APPROVED BY (SCP)."

(3) Copiers not authorized for CMI reproduction will have a warning notice:

"THIS DEVICE IS NOT AUTHORIZED FOR PROCESSING CLASSIFIED MILITARY INFORMATION"

e. The SCP Custodian of the particular command or special staff section will provide local approval authority for all CMI copied within their custodial area of responsibility.

f. In all cases of CMI copying, the copied material must be properly marked with classifications, caveats and associated markings that appear on the original material. All copied material should be checked and remarked if the markings are unclear.

g. Samples or overruns resulting from the copying process and printed waste from copier malfunctions will be safeguarded according to the classification of the information involved. This material will be promptly destroyed as classified waste.

h. Upon completion of copying, check the copier to ensure the original and all copies have been removed.

4. Controls on Facsimile (FAX) Devices

a. Those commands and special staff sections possessing an approved secure fax device connected to phone lines via an approved secure activated encryption device may send CMI via fax providing the equipment is appropriately marked:

"THIS DEVICE IS AUTHORIZED FOR PROCESSING CLASSIFIED MILITARY INFORMATION UP TO AND INCLUDING (classification), BY DIRECTION OF THE COMMAND SECURITY MANAGER. USE OF THIS DEVICE TO PROCESS CMI MUST BE APPROVED BY (SCP)."

b. Additionally, the command and special staff sections will ensure that CMI sent via secure outgoing fax is authorized by the section's SCP Custodian and a record of traffic sent is maintained in a logbook for a minimum of two years; retention standards for records of TS CMI faxed is five years. The logbook entry will contain, at a minimum:

- (1) Receiving fax number.
- (2) Person receiving fax.
- (3) Date material sent.
- (4) Authorizing official.
- (5) Description of material sent, i.e. "Encl (1) of DIAM 5813, Vol II."

c. CMI received via secure fax will be promptly entered into the CMCC accounting system as required by Chapter eight of this Order.

d. If the print cartridge used to print received classified faxes retains an image of the fax, it will be considered classified to the level of accreditation for the fax device and appropriate media classification labels will be affixed. The classified print cartridge must be promptly destroyed as classified waste when it is consumed.

e. If the fax machine is a multi-function device (fax/scan/copy) and is accredited as a mixed media machine (those used for multiple classification categories, such as SECRET, CONFIDENTIAL and UNCLASSIFIED), the user must purge any latent images of the CMI on the multi-function device components

JUL 18 2011

immediately after processing CMI; see Paragraph 11002.7 above for detailed requirements.

f. Fax devices connected to unsecured phone lines will not be used to transmit CMI and all such machines will be prominently marked:

"THIS DEVICE IS NOT AUTHORIZED FOR PROCESSING CLASSIFIED MILITARY INFORMATION"

g. Controls on Scanner Devices. Scanners accredited to process CMI will process CMI only when they are configured to scan to a computer accredited to process CMI. Any scanner not configured to scan to a computer accredited to process CMI is not authorized to scan CMI, regardless of the scanner's accreditation.

5. Controls on Printer Devices

a. Classified computers may only print to printers accredited to process CMI. Any computer not configured to print to a printer accredited to process CMI is not authorized to print CMI, regardless of the computer's accreditation. Appropriate accreditation labels will be affixed.

b. Once printed, all CMI will be considered either "working paper" or "finished product," properly marked with classifications, caveats and associated markings and registered with the CMCC via the division, branch or special staff section SCP as required by Chapter eight of this Order.

6. Control of Audio Recording Devices

a. Audio recording or transmitting devices of any format, to include cell phones and cordless phones, are not authorized in areas where CMI is discussed without approval of the Command Security Manager.

b. All audio recording media containing CMI will be considered either "working paper" or "finished product," properly marked with classifications, caveats and associated markings and registered with the CMCC via the command or special staff section SCP as required by Chapter eight of this Order.

7. Control of Visual Recording Devices. Command Security Managers will ensure that only official photography and/or videography (when required) is authorized in areas under their

cognizance. Normally, such photography/videography is used for events such as awards, promotions and reenlistments.

a. No visual recording devices of any format (to include cell phones with cameras) are permitted in spaces where classified material is processed unless specifically approved by the Command Security Manager, in consultation with the IAM.

b. Visitors are not authorized to take photographs unless special permission is received from the Command Security Manager.

c. Requests for photographs of classified material will be provided to the CMCC who will coordinate the project with the Command Combat Camera or other approved facility. Upon completion, the material, photographs, negatives or flash memory will be considered either "working paper" or "finished product," properly marked with classifications, caveats and associated markings and registered with the CMCC via the command or special staff section SCP as required by Chapter eight of this Order.

8. Control of Secondary Storage Media. Special permissions and handling are required for certain secondary storage media device.

a. Only those devices approved jointly by the IAM and the Command Security Manager are authorized for downloading CMI. USB secondary storage media, primarily in the form of "thumb" drives or "pen" drives and similar flash memory devices are restricted for use with CMI and all classified computer USB ports not used for "essential interface" (monitor/keyboard/mouse printer) will be disabled unless formally requested and approved on a case-by-case basis, for a limited duration, from the Command Security Manager; as such, these USB flash memory devices should be considered "data transfer" vice "data storage" devices. The Command Security Manager will only consider government purchased devices for CMI storage or transfer approval; personally owned devices are strictly prohibited under any circumstance.

b. Wireless PEDs and other innovative secondary storage media devices that use the electromagnetic spectrum to remotely transfer data without physical connections are not approved for storage, processing or transfer of CMI and are strictly prohibited in any area where CMI is processed, stored or discussed, whether government purchased or personally owned.

c. All approved devices are subject to the marking and registration requirements. Removable secondary storage media devices containing classified computer files will be considered either "working paper" or "finished product," properly marked with classifications, caveats and associated markings and registered with the CMCC via the command or special staff section SCP as required by Chapter eight of this Order.

9. Clearing and Purging of CMI from Media and Devices.

Detailed instructions for clearing and purging devices and media are contained in the DoN Information Assurance Publication 5239-26, May 2000, Remanence Security.

a. All candidate media and devices for purging will be turned over to the CMCC for accounting, control and coordination with the IAM for purge processing.

b. Media and devices no longer required or no longer required at their current classification level, that by design or as a result of malfunction, cannot be cleared or purged, must be destroyed. Destruction of media and devices are covered thoroughly in Chapter twelve of this Order.

JUL 18 2011

CHAPTER 12

CMI DESTRUCTION

1. Policy. Command Security Managers shall establish procedures to ensure that all classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel.

a. CMI record material may be destroyed only when destruction is the disposition authorized by the current edition of SECNAVINST 5212.5D, Disposal of Navy and Marine Corps Records. Classified information that cannot be destroyed shall be reevaluated and when appropriate, downgraded, declassified or retired to a designated record center.

b. All other CMI, including "finished product," "working papers" and DMS messages, will be destroyed when no longer required. Early destruction of unnecessary CMI assists in reducing security costs, preparing for emergency situations and better protecting necessary CMI. CMI over five years old will not be retained without proper justification being provided to the Command Security Manager.

c. 2d MAW policy requires unclassified messages and all unclassified controlled information as defined by DoD 5200.1R, including "For Official Use Only" information, "Sensitive But Unclassified" (formerly "Limited Official Use") information, "DEA Sensitive Information," "DoD Unclassified Controlled Nuclear Information," "Sensitive Information," as defined in the Computer Security Act of 1987 and technical documents with limited distribution statements be destroyed with destruction methods and devices approved for CMI when no longer required. Due to the widespread availability of approved destruction devices, there are no exceptions to this requirement.

d. Destruction of SCI, Special Access Program (SAP) and COMSEC materials is outside the scope of this directive and will be accomplished by designated personnel only, in accordance with the current directives governing those programs.

e. Command Security Managers will establish at least one day each year as "cleanout" day, when specific attention and effort are focused on disposition of unneeded classified and controlled unclassified information.

JUL 18 2011

2. Destruction Procedures

a. CMI will only be destroyed by authorized means and by personnel cleared to the level of the material being destroyed.

b. CMI awaiting destruction, whether filed or in "burn bags," will be afforded the protection equal to the highest classification of CMI contained.

c. The CMCC is responsible for the destruction of all accountable CMI entered into the command's accountability system.

(1) Confidential CMI, Secret "working papers" and Secret messages are not accountable and may be destroyed without a record of destruction, by any individual in the command cleared to the level of the material being destroyed.

(2) The physical task of destroying accountable Secret CMI may be delegated to the SCPs. The destruction is not required to be witnessed by two persons; however, the SCP will forward a signed destruction report to the CMCC.

(3) When authorized by the TSCO, TS CMI will be destroyed by two individuals: one individual will destroy the material and the other will witness the destruction. At least one individual will be a Sergeant or above. The signed and witnessed destruction report will be forwarded via the TSCO to the CMCC.

d. The CMCC will record the destruction of all TS and accountable "finished product" Secret CMI (does not include Secret "working papers" or Secret messages). Destruction records for TS CMI will be retained for five years; for Secret CMI, two years.

3. Media Destruction Guidance. Various methods and equipment may be used to destroy or purge CMI: most common is cross-cut shredding, degaussing and disintegrating.

a. Evaluated Products Listings (EPLs) provided by the National Security Agency (NSA) at www.nsa.gov/ia/government/mdg.cfm list equipment approved for purging or destroying of media containing sensitive or classified information. The website currently lists products designed for paper, punched tape and magnetic media. The

JUL 18 2011

listing also includes names, model numbers, capacities, manufacturers and distributors.

b. For any media destruction devices not currently listed on the website, such as for CDs and DVDs, contact NSA at (800) 688-6115 and select option three to request a faxed copy of the EPL for the particular media.

c. For those command temporarily lacking facilities or funding for destruction equipment or when infrequent need for destruction doesn't justify investment in destruction devices, offsite facilities are available to assist. All CMI, including classified HDDs, to be transferred to an offsite facility will be handled in accordance with the guidance contained in Chapter nine of reference (b).

(1) The NSA provides destruction services for all types of media containing CMI and CUI as defined by DoD 5200.1-R. This is particularly helpful when the requirement to destroy non-standard media cannot be met at the command location. The NSA's Classified Material Conversion facility customer service number is (301) 688-6672.

(2) All Marine Corps System Command (MARCORSYSCOM) classified HDDs requiring destruction must be sent to the Cryptologic Systems Group (CPSG) located at Lackland Air Force Base (AFB), San Antonio, Texas. CPSG provides depot-level support for certified repair, replacement, destruction and disposal of failed classified hard disk drives.

(a) CPSG has received MARCORSYSCOM funding support to provide HDD repair/replace or destroy service for the following USMC program AIS:

1. Tactical Combat Operations (TCO).
2. Intelligence Analysis System (IAS).
3. GCCS.

(b) All CPSG destruction requests should be coordinated through their Customer Support, at (210) 977-2564/2565 or DSN 969-2564/2565. The Customer Support Rep can fax or e-mail detailed instructions and required forms with examples.

JUL 18 2011

4. Emergency Destruction. Command located outside the U.S. and its territories require an Emergency Destruction Supplement for their Emergency Plan. Exhibit 2b of reference (b) gives detailed instructions on how to format an Emergency Destruction Supplement.

a. The priorities for emergency destruction are as follows:

- (1) Priority One - TS CMI.
- (2) Priority Two - Secret CMI.
- (3) Priority Three - Confidential CMI.

b. Reporting Emergency Destruction. Accurate information about the extent of emergency destruction of classified material is second in importance only to the destruction of the material itself. Report the facts surrounding the destruction to the 2d MAW Command Security Manager by SIPRNET e-mail or secure telephone. The 2d MAW Command Security Manager will notify Chief of Naval Operations (N09N2) and other interested commands.

(1) Include the following information in the initial report:

- (a) The items of CMI that may not have been destroyed.
- (b) The CMI presumed to have been destroyed.
- (c) The classification of CMI destroyed.
- (d) The method of destruction.
- (e) The anticipated date/time of submission for a follow-on statement (described below).

(2) Provide a follow-on statement to correct any inaccuracies of the initial report; submit this statement to the 2d MAW Command Security Manager as soon as practical after the initial report, providing additional information as follows:

- (a) Describe the character of the records destroyed.
- (b) Describe when and where the destruction was accomplished.

(c) Identify the circumstances under which the emergency destruction was implemented.

CHAPTER 13

INDUSTRIAL SECURITY PROGRAM

1. Policy. When Commanders approve cleared DoD contractors to operate within areas under their direct control or when commands solicit bids or let contracts containing classified or operationally sensitive information, they have the responsibility to coordinate security oversight over classified work carried out by the cleared DoD contractors; this function should be delegated to the Command Security Manager.

2. Classified and Operationally Sensitive Contracts and the DD-254

a. If a Command develops a classified or operationally sensitive contract, the Contracting Officer and the COR will insure that a DD-254, Contract Security Classification Specification, is fully incorporated. An original DD-254 shall be issued with each request for proposal, other solicitations, contract award or follow-on contract to ensure that the prospective contractor is aware of the security requirements and can plan accordingly.

(1) A revised DD-254 shall be issued as necessary during the lifetime of the contract when security requirements change.

(2) A final DD-254 shall be issued on final delivery or on termination of a classified contract.

b. Contractors under 2d MAW control who are fulfilling their responsibilities under a classified or operationally sensitive contract developed by another command or agency shall follow the security requirements and classification guidance provided within that contract's DD-254, to include attachments, supplements and incorporated references.

3. COR. The Command's Contracting Officer shall designate, in writing, the COR when a classified or operationally sensitive contract is proposed. The COR must be a security specialist; the Command Security Manager may be assigned duties concurrently. The designation is for the purpose of signing the DD-254 and revisions thereto.

a. The COR is responsible to the Command Security Manager for coordinating with program managers and procurement officials.

b. The COR shall ensure the industrial security and the operational security functions specified within Chapter eleven of reference (b) are accomplished when classified information is provided to industry for performance of a classified contract.

4. Visits by Cleared DoD Contractor Emergency. Unless special circumstances dictate, Commanders should allow cleared DoD Contractors access as "visitors," either short-term or long-term, under the Command's Visitor Control Program. Contractor employees shall conform to this IPSP and will be included in applicable portions of the command's security education program, per the provisions of Chapter eleven of reference (b).

a. Per the Under Secretary of Defense, the JPAS is the personnel security system of record throughout the DoD and shall be used to verify the personnel security clearance level for visitors requiring access to classified information. Cleared contractors, whether under a local command contract or another command or agency's contract, shall provide advance notification of their employee's visits via JPAS, to the command Security Management Office (SMO) number.

b. The Command Security Manager will validate the visitor's access requirement command or special staff section point of contact listed on the visit request, verify the level of clearance held by the contractor is commensurate to the level of access required and issue appropriate security identification and access passes/devices.

c. The responsibility for determining the need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit, usually the visitor's point of contact within the command.

5. Facility Access Determination (FAD). Contractor employees are not normally subjected to background investigations unless access to classified information is required. However, Commanders can allow contractors without classified access into command installations and operational areas when their duties require it.

a. The Commander reserves the authority and responsibility under the Internal Security Act of 1950 to request investigations on these persons and to protect persons and property under their command against the actions of untrustworthy persons.

(1) Should the Commander exercise this authority, the Contracting Officer will include the FAD program requirements in the contract specifications.

(2) The Command Security Manager will coordinate the submission of an SF 85P, "Questionnaire for Public Trust Positions" per the current procedures listed on the CNO (N09N2) website at www.navysecurity.navy.mil/facaccess.htm.

b. Alternatively, the FBI determined that National Crime Information Center (NCIC) searches by DoD personnel for security purposes are justified under homeland security/homeland defense; the NCIC Interstate Incident Index (III) must be coordinated by the Commander and his Command Security Manager through the Base PMO.

(1) The NCIC III provides arrest information and its use is restricted to certain circumstances detailed more specifically in the CMCs letter 11000 LFF/mjo dated 9 April 2004, subject: "Guidance Concerning the Contracted Workforce on Marine Corps Installations."

(2) The Command Security Manager is required to submit fingerprints to OPM on every subject of a NCIC search.

JUL 18 2011

CHAPTER 14

PERSONNEL SECURITY POLICY

1. Policy. The Command Security Manager is responsible for administering the personnel security program. The Command Security Manager is the Special Staff Officer for the Personnel Security Program and advises the Commander concerning personnel security matters relative to subordinate elements and the Headquarters staff.

2. Applicability

a. The personnel security policies in this Order apply primarily to the eligibility and authorization for access to classified information at the General Service (GENSER) level or assignment to sensitive duties and the requisite investigations and evaluations endorsing that access.

b. Detailed requirements for specific programs are found in the regulations governing those special access programs.

c. Commanders. Every CO must have a favorably adjudicated SSBI investigation.

d. Designation of Civilian Sensitive Positions

(1) Command Security Managers will assist the Commander in completing a survey of all National Security Positions within their commands for DoD civilian personnel. Category designations of Special Sensitive (SS), Critical Sensitive (CS) and Non-Critical Sensitive (NCS) will be applied to each position; any position not meeting the criteria for a National Security Position will be referred to as "Non-Sensitive."

(2) It is imperative the civilian position description accurately reflects the required duties and corresponding position sensitivity requirements. Command Security Managers must make liaison with command's civilian personnel office for assistance in this matter. Further:

(a) The applicant for employment in a DoD Civilian National Security Position must be able to meet position sensitivity investigation and adjudication requirements.

(b) The incumbent in a DoD Civilian National Security Position must be able to maintain the clearance

JUL 18 2011

eligibility for the corresponding position sensitivity. Loss of eligibility must be reported to the command's civilian personnel office.

(c). DoD civilian employees who possess clearance eligibility and access beyond what their position description requires will either have their access downgraded or their position description upgraded to meet the current eligibility. The command's civilian personnel office must provide assistance in resolving issues that fall under this situation.

(3) The determination of eligibility to occupy a sensitive position is made by the DONCAF based on the appropriate investigation. The same criteria are applied to both security clearances and sensitive position eligibility determinations. A determination by the DONCAF that an individual is not eligible for assignment to sensitive duties or a clearance will also result in the corresponding removal of clearance eligibility or assignment to sensitive duties.

JUL 18 2011

CHAPTER 15

PERSONNEL SECURITY INVESTIGATIONS

1. Policy. No individual will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding their loyalty, reliability and trustworthiness. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations.

2. Command Responsibilities. Prior to submission of a PSI, the Command Security Manager must ensure the following functions are complete:

a. Determine existence of a previous investigation, which would form the basis for current eligibility (providing there were no breaks in service greater than 24 months) and negate the immediate need for a PSI.

b. Validate U.S. citizenship, when no previous investigation has been adjudicated.

(1) Only U.S. citizens will be granted clearances and access to classified information or assigned sensitive duties.

(2) Citizenship will be verified per Appendix I of reference (a).

(3) Immigrant aliens will not be granted access to classified information unless it is in the national interest to do so and a compelling need exists. The final decision rests with the Command Security Manager.

3. Investigative Request Requirements

a. All PSI requests will be prepared following guidance found at the CNO(N09N2) website at www.navysecurity.navy.mil.

b. The Command Security Manager or his assistant, acting on behalf of the Commander, are the only officials authorized to request PSIs on individuals within their commands.

c. PSIs and Periodic Reinvestigations (PR) will not be requested for any civilian or military personnel who will be retired, resigned or separated with less than one year service remaining. Exceptions will be granted only for those personnel

31 10 2011

whose participation in a SAP is documented with appropriate orders and whose assignment is contingent upon completion of the required PR.

d. The scope of the PSI requested from Office of Personnel Management (OPM) will be commensurate with the level of sensitivity of the access required or position occupied. Only the minimum investigation to satisfy a requirement will be requested. The various types of investigations are described in Chapter six of reference (a).

e. All requests for access to SCI will be validated and approved by the SSO. Each nominee for SCI must be personally interviewed by the SSO Office.

4. JPAS. The JPAS, at <https://jpas.dsis.dod.mil/> provides accurate, updated investigation information on personnel from all branches of the service, DoD civilians and DoD contractors. PSIs will be initiated through Electronic Questionnaires for Investigative Processing (E-QIP Direct) and not JPAS (See CMC Message DTG: 131928z Aug 09 / Sub: Implementation of E-QIP Direct). Security personnel requiring access to JPAS can research the requirements at www.navysecurity.navy.mil, click on JPAS Requests.

5. Office of Personnel Management (OPM). The OPM conducts all PSIs for the Marine Corps. Commands are prohibited from conducting their own PSIs.

6. Preparation and Submission of PSI Requests

a. Each individual approved for submission of a PSI will forward their completed SF-86, Questionnaire for National Security Positions, to the Command Security Manager via E-QIP for validation and processing.

b. All PSI requests will require certification and investigation release forms signed by the individual submitting the PSI; and all investigation requests, less SSBI-Periodic Reinvestigations (SSBI-PRs), will require submission of fingerprints.

c. Currently authorized methods for submitting PSIs and fingerprints are published in the CNO (N09N2) website. 2d MAW Security's Website provides updated and appropriate instructions to assist the Subordinate Command Security Manager.

7. Follow-Up Actions on PSI Requests

a. OPM returns investigative request packages that have been rejected for administrative errors to the originator as indicated by the Submitting Office Number (SON).

(1) The SON is a four-character identifier provided by OPM-Federal Investigations Processing Center (FIPC). Each Subordinate Command requesting investigations must have a SON; call the FIPC Program Services Office (PSO) at (724) 794-5612, to verify.

(2) To update the command's SON address or points of contact, submit a "Personnel Investigations Processing System (PIPS) Form 12" and forward to OPM. PIPS Forms are available on the CNO (N09N2) website.

b. Rejected PSI requests must have corrective action taken immediately and the request re-submitted. On the corrected investigation request package, have the subject of the investigation re-sign and re-date (with a current date) his certification and release forms; if the subject's signatures and dates on the certification and releases are more than sixty days old upon receipt at OPM, the package will again be rejected.

8. Personnel Security Folders. In recognition of the sensitivity of personnel security reports and records, particularly with regards to personal privacy, completed SF-86s and results of investigations must be handled with the highest degree of discretion. The Personnel Security Folder provides a repository for sensitive items that should not be proliferated outside the Command Security Manager's office.

a. The file copy of an individual's completed SF-86, maintained in the Personnel Security File, is not required for retention after adjudication. The SF-86 may either be returned to the individual for safekeeping or destroyed. While it is maintained in the Personnel Security Folder it should be afforded FOUO level protection, at a minimum.

b. In rare instances, Command Security Managers may receive copies of investigative material and reports from investigative agencies, such as OPM, for temporary purposes.

(1) These investigative materials and reports contain extremely sensitive information and will not be divulged to the

JUL 18 2011

subject of the report, whether favorable or unfavorable, unless directed by the investigating agency.

(2) If the investigating agency does not specify release, but the individual desires to view their report, the individual must submit a FOIA request to the investigating agency. The investigating agency will process the request and communicate with the individual directly. Involvement in this process by the Command Security Manager is limited to assisting in identifying the name and address of the FOIA Requesting Officer at the investigating agency; the Command Security Manager is prohibited from providing local access to investigative reports pursuant to a FOIA request made to an investigating agency.

(3) The investigative materials and reports may be kept in the personnel security folder, but in all cases will be stored in a vault or safe. Retention of copies of investigative material and reports longer than 120 days after final action has been completed on the individual is prohibited; copies should either be returned to the investigating agency or destroyed. Under no circumstances will the investigation material or reports be placed in a Marines SRB, Officer's Qualification record or OMPF.

c. The Personnel Security Folder should also be the repository for current JPAS print-outs, clearance and access letters and endorsements, NATO, CNWDI and other program brief/debrief acknowledgements, command debrief letters and copies of Security Termination Statements.

d. The Personnel Security Folder must be retained (less the SF-86 and investigative material and reports) for a period of two years after termination of the individual's access at the command.

JUL 18 2011

CHAPTER 16

PERSONNEL SECURITY DETERMINATIONS1. Policy

a. The standard which must be met for security clearance eligibility or assignment to sensitive duties is that, based on all available information, the individual's loyalty, reliability and trustworthiness are such that entrusting them with classified information or assigning the individual to sensitive duties is clearly consistent with the interests of national security.

b. In making determinations regarding an individual's loyalty, reliability and trustworthiness, all information, favorable and unfavorable, is considered and assessed for accuracy, completeness, relevance, importance and overall significance. The final determination is the result of an overall common-sense "whole person" adjudication reached by application of thirteen adjudicative criteria (see Appendix G of reference (a)).

2. Department of the Navy Central Adjudication Facility (DONCAF). The DONCAF will assign clearance eligibility at the highest level supportable by the investigation completed by OPM. DONCAF posts clearance eligibility information directly to JPAS.

3. Joint Personnel Adjudication System (JPAS)

a. The JPAS at <https://jpas.dsis.dod.mil> provides accurate, updated eligibility information on personnel from all branches of the service, DoD Civilians and DoD Contractors and is sufficient to award access at the level of clearance eligibility specified. Security personnel requiring a JPAS account can research the requirements on the CNO (N09N2) at www.navysecurity.navy.mil, click on JPAS Requests.

b. Commands authorizing access to CMI or any special program, must annotate that access in JPAS.

c. JPAS enables security personnel to communicate eligibility/access issues with DONCAF.

JUN 18 2011

4. Eligibility Determination

a. The DONCAF will adjudicate information from PSIs and other relevant information to determine initial or continued eligibility for security access and/or assignment to sensitive duties. The DONCAF will communicate the results to the requesting command via JPAS or in the case of unfavorable determinations, in writing.

(1) DONCAF can validate and certify personnel security clearance eligibility.

(2) DONCAF can issue a Letter of Intent (LOI) to deny or revoke security clearance eligibility to an individual for whom an unfavorable personnel security determination is being contemplated.

(3) The DONCAF can issue a Letter of Notification (LON) to an individual for whom an unfavorable personnel security determination has been made, advising the individual of their right to appeal the DONCAF determination.

b. The Commander must review all locally available information to determine eligibility for initial or continued security access and/or assignment to sensitive duties and must communicate with DONCAF on issues of importance relating to access.

(1) The Command Security Manager must ensure prior to granting initial command access, that individual have not had any incident that will disqualify he/she from having access. If so report any negative findings to DONCAF via an "Incident Report" in JPAS.

(2) The Command Security Manager must continuously evaluate command personnel with regard to their eligibility for access to CMI. Chapter ten and Appendix G of reference (a) provides excellent guidance on the "Continuous Evaluation Program."

(3) The Command Security Manager must advise the Commander if suspension of access at the local command level is warranted when negative or adverse information is developed through the Continuous Evaluation Program. Suspension must be reported to DONCAF in conjunction with the "incident" via JPAS and to the subject of the suspension in a letter from the

JUL 18 2011

Command Security Manager. Chapter nine of the most current edition of reference (a) provides excellent guidance.

5. Unfavorable Determination

a. An unfavorable personnel security determination will result in one or more of the following personnel security actions:

(1) Denial or revocation of security clearance eligibility.

(2) Denial or revocation of a Special Access Authorization (including SCI access eligibility).

(3) Non-appointment to or non-selection for sensitive assignment.

b. Procedures for processing, serving, responding and appealing unfavorable determination notifications (either LOIs or LONs) are sufficiently addressed in Chapter seven of reference (a).

6. Validity and Reciprocal Acceptance of Personnel Security Determinations

a. A personnel security eligibility granted by an authority of the DoD remains valid and will be mutually and reciprocally accepted within the DoD until:

(1) The individual is separated from the Armed Forces or civilian employment or terminates an official relationship with the DOD.

(2) The clearance has been officially terminated, withdrawn, adjusted or it has been suspended for cause.

a. The Command Security Manager will be the determining authority for validating and accepting other government agency issued security clearances.

JUL 18 2011

CHAPTER 17

PERSONNEL SECURITY ACCESS1. Policy

a. Access to classified information may be granted only if allowing access will promote the furtherance of the DoN mission while preserving the interests of national security.

b. Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based on need-to-know.

c. Commanders will ensure that personnel under their command are briefed in accordance with paragraph 3004 of this Order before granting access to CMI.

2. Request for Access. All requests for access will be provided to the Command Security Manager for validation and authorization.

a. Validation of current security clearance eligibility in the JPAS is required prior to awarding access to classified national security information. If there is no current eligibility, the Command Security Manager must initiate a PSI request per Chapter fifteen of this Order.

b. The Marine Corps Total Force System (MCTFS) is specifically prohibited from making security access determinations, as is the Defense Clearance and Investigations Index (DCII) database and Marine Online. None of these systems provides accurate or updated information and they may not be used to make this determination. Further, travel orders that contain clearance information will not be used as proof of eligibility for access.

c. Access authorization is a local command responsibility and is based on need-to-know established by the Commander; access must not be granted automatically and does not have to be granted up to the level of eligibility authorized by the DONCAF. At no time will access be granted based upon the desires of the individual requesting access.

3. Classified Information Nondisclosure Agreement (SF-312). The SF-312 is a nondisclosure agreement between the U.S. and an individual. The one-time execution of this agreement by an

individual is necessary before that individual's access to classified information may be granted.

a. All individuals who have not previously executed (signed) the SF-312 agreement must do so before access to classified information is granted.

b. The execution of the agreement will be witnessed, with the witness' entry affixed at the time of execution.

(1) Commanders must designate appropriate individuals (usually the Command Security Manager and his assistants) to accept SF-312's on behalf of the United States Government. The acceptor may then accept, on behalf of the U.S. Government, an SF-312 executed by a member of the same command. The entry of the acceptor must be affixed on the SF-312 as soon as possible after the execution.

(2) The witness and the acceptor may be the same individual, if appropriately designated by the Commander. In this case, both entries should be affixed to the SF-312 at the time of execution.

(a) The use of the "Security Debriefing Acknowledgement" portion of the SF-312 will not be used and should be crossed out with two opposing diagonal lines running from corner to corner over the debriefing section.

(b) Reporting the Nondisclosure Agreement.

c. HQMC (MMSB 20) is designated as the Marine Corps repository for these agreements. The original copy of the SF-312 will be retained at HQMC for 70 years following its date of execution. Forward the executed, witnessed and accepted original SF-312 to MMSB 20 at the following address:

COMMANDANT OF THE MARINE CORPS
HEADQUARTERS U S MARINE CORPS
(MMSB-20) MCCDC
2008 ELLIOT RD
SUITE 114
QUANTICO VA 22134-5030

d. To capture the date of the execution, a one-time JPAS entry in the executor's Personal Summary screen is mandatory upon completion.

JUL 18 2011

4. Verbal Attestation

a. The Deputy Secretary of Defense determined that additional measures were warranted to increase the awareness of individuals who were entrusted with access to CMI at all levels of eligibility and and/or indoctrinated into Special Access Programs. In compliance, the statement below will be read aloud and 'attested to' by personnel seeking access to CMI, in the presence of a witness other than the person administering the brief:

"I accept the responsibilities associated with being granted access to classified NSI. I am aware of my obligation to protect classified NSI through proper safeguarding and limiting access to individuals with the proper security clearance and official need-to-know. I further understand that, in being granted access to CLASSIFIED INFORMATION, SENSITIVE COMPARTMENTED INFORMATION or a SPECIAL ACCESS PROGRAM, a special trust and confidence has been placed in me by the U.S. Government."

b. This attestation is not a legally binding oath and will not be sworn to. Attestation administration is required only one time, usually when the original SF-312, Classified Information Nondisclosure Agreement or 1879-1, Sensitive Compartmented Information Nondisclosure agreement is signed. This will implement the attestation statement as a part of their command's annual security refresher training. Reporting the attestation will be accomplished via JPAS on the individual's "Personal Summary" screen.

c. Executing an SCI Nondisclosure Agreement does not eliminate the necessity to execute an SF-312.

5. Temporary Access (Interim Clearance). Commands may grant interim security clearance and access (except for SCI access) pending completion of full investigative requirements and pending establishment of a final security clearance by DONCAF. Interim clearances may be granted by the Commander under the following conditions:

a. Interim TS Security Clearance.

(1) Either Secret or Confidential security clearance eligibility exists or a favorable National Agency Check with Law and Credit (NACLC) or Access National Agency and Written Inquiries (ANACI) (other investigation types may be allowed,

JUL 13 2011

refer to reference (a)) has been completed within the past ten years (with no break in service).

(2) A favorable review of local records is accomplished.

(3) A favorable review of the Personnel Security Questionnaire (PSQ) is accomplished (ten year scope).

(4) The SSBI has been submitted to the OPM.

b. Interim Secret or Confidential Security Clearance.

(1) A favorable review of local records.

(2) A favorable review of the completed PSQ (seven year scope).

(3) The appropriate ANACI or NACLIC investigation has been submitted to OPM.

c. Commands will record interim security clearances in JPAS. The interim Clearance will be granted by the Commander or designee who has been the subject of a favorably completed SSBI.

d. If the command receives a LOI from the DONCAF to deny an individual's security clearance, the Command Security Manager will withdraw any interim security clearance. Procedures for suspending access are found in Chapter nine of reference (a).

e. Subordinate Command should refer to Chapters six and eight of reference (a) for when interim clearance requirements are necessary. Additional guidance may be given through MARADMINS to support various contingencies worldwide.

6. Access Termination, Withdrawal or Adjustment

a. When a Marine executes a Permanent Change of Station (PCS) or Permanent Change of Assignment (PCA) or a civilian transfers within the DoN, local termination of access and a debriefing per Chapter three, Paragraph 3006 of this Order, is required at the losing command. A "debrief" and an "out-process" action is required in JPAS on the individual's Person Summary screen.

b. For those Marines and Civilians retiring or terminating service, a debriefing and a Security Termination Statement

JUL 18 2011

(OPNAV 5511/14 Rev 9-05) are required per Chapter three, Paragraph 3006 of this Order.

(1) DONCAF will be notified via JPAS of the reasons for termination.

(2) A "Debrief" and an "Out-Process" action are required in JPAS.

(3) The completed Security Termination Statement (OPNAV 5511/14 Rev 9-05) will be immediately forwarded to HQMC MMSB-20 for inclusion in the individual's SRB, Officer Qualification Record or Civilian Employee Personnel File prior to that record's close-out and transfer to a records retention facility.

c. When there is a change in an individual's level of access required or position sensitivity, access may be adjusted accordingly, provided the change in access is supported by DONCAF's determination of eligibility for that individual. If the eligibility is insufficient for the new, higher level of access, a new PSI will be initiated.

7. Suspension of Access for Cause. When questionable or unfavorable information becomes available, such as that information that may be obtained from the Continuous Evaluation Program, concerning an individual who has been granted access, the Commander may suspend access locally. Details regarding such suspensions are adequately addressed in Chapter nine of reference (a). All local suspensions will be reported to DONCAF via JPAS with an "Incident Report."

JUL 18 2011

CHAPTER 18

VISITOR CONTROL

1. Policy. For security purposes, the term "visitor" applies to all individuals who are not permanently assigned to the command.

a. Subordinate Commands are responsible for visitors to their respective commands and for ensuring the safeguarding of classified information under their jurisdiction.

b. The movement of all visitors will be restricted to protect classified information. When escorts are used, they must ensure that visitors have access only to information they have been authorized to receive.

c. As a matter of convenience and courtesy, Flag Officers, General Officers and their civilian equivalents are not required to sign visitor records or display identification badges when being escorted. The escort should be present at all times when the visitor is in sensitive areas of the command area of responsibility.

d. General visiting by the public will only be allowed on an unclassified basis: no classified areas or information will be shown or divulged. General visiting by the public will be conducted and monitored based on the probable presence of foreign agents among the visitors.

2. Facilitating Classified Visits

a. JPAS is the personnel security system of record for the DoD. Use of this system will reduce the administrative burden associated with many routine security actions.

b. JPAS shall be used to verify the personnel security clearance level for visitors requiring access to CMI. Visit Authorization Letters (VALs) are no longer required for civilian, military and contractor personnel whose access level and affiliation are accurately reflected in JPAS.

(1) All Command Security Managers will use the "Visit Request" function of JPAS for sending visit requests to other Marine Corps or Navy units. For visit requests to and from units and activities outside of the Marine Corps or Navy JPAS

should be utilized to the maximum extent possible, depending on the level of sophistication of the external unit involved.

(2) All contractors who participate in the NISP have been authorized to use the "Visit Request" function of JPAS in lieu of sending VALs for classified visits.

c. The responsibility for establishing the positive identification of visitors and determining need-to-know prior to the disclosure of any classified information continues to rest with the command disclosing the classified information.

3. Visits by Foreign Nationals. The USMC fully supports participation in Foreign Visits and Extended Foreign Visits through the FLO Program and the MCFPEP. It is essential that visit requests be coordinated so that the interests of the U.S. Government and the USMC are adequately served; these programs must be conducted in a manner which limits risks of exposure of classified or sensitive information to foreign personnel not otherwise authorized access to this information.

a. Requests for official visits conducted by foreign governments or representatives to command activities must be submitted through the visitor's Embassy in Washington, D.C. to HQMC. Official visits include one-time, recurring and extended visits.

b. Foreign Visit Requests (FVRs) received by HQMC, intended for Subordinate Command of 2d MAW will be routed through 2d MAW. Coordinating instructions will be provided with the forwarded request.

(1) All requests must be responded to in the manner directed in the coordinating instructions.

(2) All approvals, modifications or cancellations will be forwarded from HQMC through 2d MAW. Approved FVRs will detail the level of disclosure authorized for the specified visit.

c. Extended FVRs (FLOs & MCFPEPs) will be supported from HQMC with a Delegated Disclosure Letter (DDL), forwarded to the MSC via MARFORPAC, detailing the level of disclosure authorized. Commands hosting FLOs and MCFPEPs must maintain a file of the current DDL, U.S. Contact Officer assignment letters and Foreign Officer statements of understanding, as applicable.

NOV 18 2011

(1) The original Contact Officer assignment letter should be sent to the Commandant, HQMC (Foreign Disclosure Office (PP&O)), via CG, 2d MAW (Security).

(2) Subordinate Commands will forward copies of the Foreign Officer Statement of Understanding letters to the 2d MAW Command Security Manager.

d. The current edition of MCO 5510.20 provides detailed information for Foreign Disclosure Officers and should be reviewed by Command Security Managers whose commands host foreign visitors.

JUL 18 2011

APPENDIX A

GUIDELINES FOR COMMAND SECURITY INSTRUCTION

1. Command Security Program Elements. The Command Security Manager shall assess the vulnerability of the command's CMI to loss or compromise. This includes obtaining information on the local threat, volume and scope of classified information, mission of the command, countermeasures available and the cost effectiveness of alternative courses of action. Results of this assessment shall be used to develop a command security instruction that resembles the organization of this Order while identifying any unique command requirements. The command security instruction shall supplement this regulation and other directives from authorities in the command administrative and operational chain.

2. Information Security Program Elements. Incorporate the following into the command security instruction in a manner apportioned to the findings of the command's vulnerability assessment. Citing references that are accessible at the command are encouraged, to enhance form and reduce redundancy.

a. PART I - Command Security Program Elements

(1) Identify purpose, applicability and relationship to other directives, particularly the reference (a) through (b).

(2) Describe the security organization and identify positions.

(3) Identify the chain of command.

(4) Describe procedures for internal and subordinate security reviews and inspections.

(5) Develop an IPSP security education program. Assign responsibilities for briefings and debriefings.

(6) Specify internal procedures for reporting and investigating loss, compromise and other security discrepancies.

(7) Establish procedures to report CI matters to the nearest NCIS office.

JUL 18 2011

b. PART II - Information Security Program Elements

(1) State whether the Commander and any other command officials have been delegated TS or Secret Original Classification Authority.

(2) Specify command responsibilities and controls on any special types of classified and controlled unclassified information.

(3) 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.

(4) Identify requirements for the safeguarding of classified information to include how classified information shall be protected during working hours; stored when not in use; escorted or hand-carried in and out of the command and protected while in a travel status.

(5) Establish reproduction controls to include compliance with reproduction limitations and any special controls placed on information by originators.

(6) Establish command destruction procedures. Identify destruction facilities or equipment available. Attach a command emergency destruction plan as a supplement, when required.

(7) Develop an Industrial Security program and identify key personnel, such as the COR, if applicable.

(8) Other elements of command security which may be included are key and lock control; safe and door combination changes; location of records of security container combinations; procedures for emergency access to locked security containers; protecting telephone conversations; conducting classified meetings; the safeguarding of U.S. classified information located in foreign countries, AIS processing equipment and residential storage arrangements.

c. PART III - Personnel Security Program Elements

(1) Explain each step of the command's internal administrative procedures leading to access to classified information or assignment to sensitive duties for command personnel as well as procedures for safeguarding and maintaining classified information. The text will:

JUL 18 2011

(a) Explain each requirement step by step, specifying responsible entities as necessary.

(b) Assign responsibilities for final preparation of investigative request forms.

(c) Establish procedures for documenting clearance and access granted.

(d) Identify the adjudicative guidelines, remind command personnel of their continuing responsibilities to notify security of derogatory information or suspicious behavior.

(e) Assign responsibilities for continuous evaluation. Establish procedures for reporting derogatory information to the DONCAF.

(f) Formulate guidelines for foreign travel briefings and identify the individual responsible for briefing/debriefing.

(2) Establish command visitor control procedures to accommodate visits to the command involving access to or disclosure of, classified information. Identify procedures to include verification of personnel security clearances and need-to-know.

(a) Assign responsibilities for processing classified visit requests to or from the command.

(b) Specify any restrictions on movement for foreign exchange personnel, FLOs, foreign students and caution command personnel regarding their responsibilities.

(c) Include in this section a list of areas within the command authorized for general visiting and clearly identify all areas that are off limits to visitors.

JUL 18 2011

Appendix B

GUIDELINES FOR EMERGENCY ACTION PLANS

1. Purpose. Per the reference, 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.

2. Background. In the event of a natural disaster, civil disturbance or enemy attack, the protection of CMI must be ensured. The DoN Information Security Program Manual directs all commands in possession of CMI, to develop an emergency action plan for the protection of that material.

3. Information. These instructions are provided to protect classified material during times of emergency. Key points are emphasized below.

a. 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.

b. Beginning emergency actions early will enhance the success of this plan. It is important to contact the appropriate official to advise of the situation and determine if execution of the emergency action plan is required and to what degree.

4. Natural Disaster. In the case of a natural disaster such as fire, flood, tornado or hurricane, 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.

5. Civil Disturbance. The perimeter security of the base and the command element provide sufficient protection that a civil disturbance or riot could not potentially pose a threat.

6. Command Authority. The CG, 2d MAW shall decide the course of action to be taken concerning the security of the commands classified holdings during an emergency. In the event that the CG, 2d MAW is unavailable then the authority shall pass to the next senior command official. Principal and Special Staff Officers of the command may decide the appropriate course of action to take during an emergency concerning the classified

11 13 2011

holding within their section. This is only authorized when there is an imminent threat to personnel safety or national security. In such instances the individual responsible must provide a letter of justification for their actions.

7. Securing Classified. During a natural disaster or civil disturbance all non-essential classified material shall be secured by any means available without endangering personnel and with time permitting.

8. Securing a Facility. Depending on the emergency, cleared command personnel shall provide a security perimeter around the facility or facilities damaged until it has been deemed safe to return to the building. 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.

9. 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. A security sweep by cleared personnel must be completed to the extent possible once it is believed all classified material has been removed to ensure nothing has been overlooked.

10. Admittance of Emergency Personnel. Admittance of emergency personnel (eg., Paramedics, Police, Fire Fighter, etc.) into a restricted or limited access space will be allowed under conditions that require immediate attention such as fire, flood, tornado, hurricane 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.

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

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

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

d. Report the names of emergency personnel to the Security Manager as soon as possible. A "Non-Disclosure Statement" will be executed for all emergency personnel by the Command Security Manager.

JUL 18 2011

e. Radio communication by emergency personnel is authorized.

11. Enemy Attack. In the event that it appears that the command or facilities containing classified material may fall into the hands of enemy combatants, immediate actions must be taken to protect CMI. Actions directed shall be executed without endangering the lives of personnel. An emergency destruction of all classified holdings must be a consideration.

12. Emergency Destruction. The act of destroying all classified material via any means possible that renders the material useless in order to prevent CMI from falling into the hands of unauthorized persons to include but not limited to enemy combatants, foreign entities and terrorists. This action shall only be taken when the command no longer has the means to defend itself and the extraction of classified material to a safe location is no longer an option.

13. Execution of Emergency Action

a. The destruction of classified material shall occur in the order listed:

(1) Priority One - TS Material, Cryptographic equipment and keying material.

(2) Priority Two - Secret Material.

(3) Priority Three - Confidential Material.

b. Subordinate commands in the local area shall be contacted, if deemed necessary, to direct them to initiate emergency destruction.

14. 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.

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

JUL 18 2011

b. 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.

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

d. 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.

15. Emergency Destruction Report. All instances of an Emergency Destruction must be recorded and reported in writing to the Command Security Manager.

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

b. These reports will be kept on record at this command for no less than five years.

c. The report will be submitted to II Marine Expeditionary Force (II MEF) Security Manager, Marine Forces Command Security Manager and Headquarters Marine Corps (ARS).