



UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE
PSC BOX 20005
CAMP LEJEUNE NC 28542-0005

MCIEAST-MCB CAMLEJO 5510.2A
SECMGR

APR 12 2019

MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE CAMP LEJEUNE ORDER 5510.2A

From: Commanding General
To: Distribution List

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCO 5510.18B
(d) MCO 5530.14A
(e) DoDM 5200.01, Volume 1-4, "DoD Information Security Program, February 24, 2012, Incorporating Change 2, March 19, 2013
(f) DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," February 28, 2006
(g) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011
(h) MCO 3571.2H
(i) SECNAVINST 5720.42
(j) SECNAV M-5210.1
(k) OPNAVINST 5513.1F
(l) Department of the Navy Information Assurance Publication 5239-22, September 2008, Protected Distribution System (PDS)
(m) Atomic Energy Act of 1954, as amended
(n) Computer Security Act of 1987
(o) Homeland Security Presidential Directive 12 (HSPD-12)
(p) EKMS-1, Electronic Key Management System
(q) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," August 22, 2008
(r) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009
(s) Department of the Navy Information Assurance Publication 5239-26, May 2000, Remanence Security Guidebook
(t) MARADMIN 274/16 of 27 May 16
(u) MARADMIN 317/17 of 28 Jun 17
(v) MCO 5510.20B
(w) MCIEAST-MCB CAMLEJO 5510.3

Encl: (1) Information and Personnel Security Program

1. Situation. Pursuant to references (a) through (w), this Order promulgates policy and guidance for the Marine Corps Installations East-Marine Corps Base Camp Lejeune (MCIEAST-MCB CAMLEJ) Information and Personnel Security Program (IPSP). This Order provides uniform procedures, standards, supporting details, and outlines requirements necessary to support the commander's efforts to protect national security interests.

2. Cancellation. MCIEAST-MCB CAMLEJO 5510.2.

3. Mission

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

APR 12 2019

a. To establish the IPSP and provide policy and guidance to support the commander's efforts to maintain a robust security program, ensuring all personnel are aware of and involved in protecting and applying consistent and appropriate safeguards for the protection of our national security interests.

b. Summary of Revision. This Order has been completely revised to updated policies and procedures and should be reviewed in its entirety.

4. Execution. To be effective, the IPSP must receive attention from all echelons within the chain of command. It is the Commander/Commanding Officer's (CO's) responsibility to ensure the command security posture is accurately and consistently addressed and resources are afforded to execute and support these programs. Marines, Sailors, civilian employees and contractors shall be actively involved and vigilant in the security of U.S. Government and Marine Corps classified assets.

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To enhance information and personnel security awareness at bases and stations within MCIEAST, and provide appropriate safeguards for the protection of Classified Military Information (CMI) and Controlled Unclassified Information (CUI).

(2) Concept of Operations

(a) This Order establishes a formal IPSP within Headquarters MCIEAST-MCB CAMLEJ and applies to all MCIEAST subordinate commands.

(b) Directs subordinate commanders to support the Command Security Manager to ensure the IPSPs are provided adequate command attention and assistance through proper staffing and training, and security resources are appropriate to execute these programs.

(c) The Command Security Manager at each MCIEAST subordinate command is responsible for security matters within their organization. The Command Security Manager shall plan, implement, manage, and direct the organization IPSP in accordance with the CO's guidance, this Order, and references (a) through (w).

b. Tasks

(1) Chief of Staff shall:

(a) Designate the MCIEAST-MCB CAMLEJ Command Security Manager, in writing, to manage the IPSP in accordance with reference (c).

(b) Exercise overall staff cognizance for matters relating to the IPSP.

(c) Ensure the Command Security Manager and other designated security management personnel are appropriately trained and that the command has an effective IPSP.

(2) MCIEAST-MCB CAMLEJ General and Special Staff Section Department Heads shall: Ensure personnel are aware of and involved in protecting and applying consistent and appropriate safeguards for the protection of CMI and CUI.

APR 12 2019

(3) MCIEAST Subordinate Commanders shall:

(a) Appoint a Command Security Manager, in writing, to manage local IPSPs in accordance with reference (c).

(b) Implement, execute, and administer requirements of this Order and publish local command security policy and procedures to ensure security programs encompass the requirements of this Order and references (a) through (w).

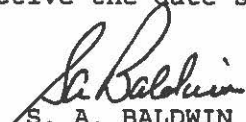
(c) Ensure the Command Security Manager attends the Security Manager Course and completes the required training within 180 days of appointment as the Command Security Manager.

5. Administration and Logistics. Ensure widest dissemination of this Order. Recommendations for changes are encouraged and are to be submitted to the MCIEAST-MCB CAMLEJ Command Security Manager. Some of the procedures in this Order are specific to this Headquarters and may differ from that of MCIEAST subordinate commands. Refer to specific references for policy and procedures.

6. Command and Signal

a. Command. This Order is applicable to this Headquarters, MCIEAST-MCB CAMLEJ General and Special Staff Departments and MCIEAST subordinate commands.

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


S. A. BALDWIN
Deputy Commander

DISTRIBUTION: A/B

APR 12 2019

RECORD OF CHANGES

Log completed action as indicated.

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

APR 12 2019

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
PART I	COMMAND SECURITY PROGRAM	
Chapter 1	COMMAND SECURITY PROGRAM AUTHORITIES AND BASIC POLICY.....	1-1
1.	Purpose.....	1-1
2.	Applicability.....	1-1
3.	Scope.....	1-1
4.	Department of the Navy (DON) Security Program Management....	1-1
5.	Policy Guidance.....	1-2
Chapter 2	COMMAND SECURITY MANAGER PROGRAM MANAGEMENT.....	2-1
1.	Policy.....	2-1
2.	Commander.....	2-1
3.	Command Security Manager.....	2-2
4.	Duties of the Command Security Manager.....	2-2
5.	Assistant Command Security Manager.....	2-4
6.	Top Secret Control Officer (TSCO).....	2-4
7.	Security Officer.....	2-4
8.	Contracting Officer's Representative (COR).....	2-5
9.	Other Security Assistants.....	2-5
10.	General and Special Staff Department Responsibilities.....	2-6
11.	Internal Security Procedures.....	2-6
12.	Security Service Agreements (SSAs).....	2-6
13.	Inspections, Assist Visits, and Reviews.....	2-7
Chapter 3	SECURITY EDUCATION.....	3-1
1.	Policy.....	3-1
2.	Purpose.....	3-1
3.	Responsibility.....	3-1
4.	Scope.....	3-1
5.	Security Briefings.....	3-2
6.	Special Briefings.....	3-3
7.	Debriefings.....	3-3
8.	Continuing Security Awareness.....	3-4
Chapter 4	LOSS, COMPROMISE, AND OTHER SECURITY VIOLATIONS.....	4-1
1.	Policy.....	4-1
2.	Administrative Sanction, Civil Remedies, and Punitive Actions.....	4-1
3.	Incident Reporting Responsibilities.....	4-2
4.	Security Inquiry (SI).....	4-2
5.	JAGMAN Investigations.....	4-3
6.	Investigative Assistance.....	4-3
7.	Reporting Losses or Compromises of Special Types of Classified Information and Equipment.....	4-3
8.	Report of Finding CMI Previously Reported as Lost or Destroyed.....	4-4
9.	Compromise through Public Media.....	4-4

APR 12 2019

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
10.	Unauthorized Disclosure through Spillage.....	4-4
11.	Security Violations.....	4-4
12.	Unsecured Security Containers.....	4-4
13.	Improper Transmission.....	4-5
Chapter 5	COUNTERINTELLIGENCE MATTERS TO BE REPORTED TO THE COMMAND SECURITY MANAGER.....	5-1
1.	Policy.....	5-1
2.	Sabotage, Espionage, International Terrorism, or Deliberate Compromise.....	5-1
3.	Contact Reporting.....	5-1
4.	Special Reporting Situations.....	5-1
5.	Foreign Connections.....	5-2
PART II - INFORMATION SECURITY PROGRAM ELEMENTS		
Chapter 6	CLASSIFICATION MANAGEMENT.....	6-1
1.	Policy.....	6-1
2.	Original Classification Principles and Considerations.....	6-1
3.	Special Classifying Criteria.....	6-1
4.	Classification Designations.....	6-2
5.	Tentative Classification.....	6-2
6.	Limitation of Classifying.....	6-2
7.	Challenges to Classifications.....	6-3
8.	Derivative Classification.....	6-3
9.	Accountability of Classifiers.....	6-4
10.	Foreign Government Information (FGI).....	6-4
Chapter 7	CLASSIFICATION REVIEW.....	7-1
1.	Policy.....	7-1
2.	Marking Requirements.....	7-1
3.	Review Requirements.....	7-1
4.	Mandatory Declassification Reviews.....	7-1
Chapter 8	CMI/CUI CONTROL MEASURES.....	8-1
1.	Policy.....	8-1
2.	Applicability of Control Measures.....	8-1
3.	Top Secret Control Measures.....	8-1
4.	Secret Control Measures.....	8-3
5.	Naval Messages and E-mail.....	8-3
6.	Confidential Control Measures.....	8-4
7.	Working Papers.....	8-4
8.	Inventory of Classified Material.....	8-4
9.	Special Handling Requirements.....	8-4
10.	Control Measures for Special Types of Classified and Controlled Unclassified Information.....	8-5

APR 12 2019

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 9	CMI DISSEMINATION.....	9-1
1.	Policy.....	9-1
2.	Top Secret Dissemination.....	9-1
3.	Secret Dissemination.....	9-1
4.	Confidential Dissemination.....	9-1
5.	Dissemination of Special Types of Classified and Controlled Unclassified Information.....	9-1
6.	Dissemination to Contractors.....	9-2
7.	Disclosure to Foreign Governments and International Organizations.....	9-2
8.	Pre-Publication Review.....	9-2
Chapter 10	CMI SAFEGUARDING.....	10-1
1.	Policy.....	10-1
2.	Responsibility for Safeguarding.....	10-1
3.	Restricted Areas.....	10-1
4.	Protected Distribution System (PDS).....	10-2
5.	Safeguarding Work Spaces.....	10-3
6.	Safeguarding During Working Hours.....	10-4
7.	Safeguarding in Storage.....	10-4
8.	Safeguarding During Visits.....	10-5
9.	Safeguarding During Classified Meetings.....	10-5
10.	Safeguarding CMI while being Hand Carried.....	10-6
11.	Safeguarding CMI while in a Travel Status.....	10-6
Chapter 11	CMI DUPLICATION AND DISTRIBUTION.....	11-1
1.	Policy.....	11-1
2.	Controls on Reproduction.....	11-2
3.	Controls on Copy Devices.....	11-3
4.	Controls on Facsimile (FAX) Devices.....	11-4
5.	Controls on Scanner Devices.....	11-4
6.	Controls on Printed Devices.....	11-5
7.	Controls on Audio Recording Devices.....	11-5
8.	Controls on Visual Recording Devices.....	11-5
9.	Controls on Secondary Storage Media.....	11-5
10.	Clearing and Purging of CMI from Media and Devices.....	11-6
Chapter 12	CMI DESTRUCTION.....	12-1
1.	Policy.....	12-1
2.	Destruction Procedures.....	12-1
3.	Media Destructive Guidance.....	12-2
4.	Emergency Destruction.....	12-3

APR 12 2019

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 13	INDUSTRIAL SECURITY PROGRAM.....	13-1
1.	Policy.....	13-1
2.	Classified and Operationally Sensitive Contracts and the DD 254.....	13-1
3.	Contracting Officer's Representative (COR).....	13-1
4.	Visits by Cleared DoD Contractor Employees.....	13-1
5.	Contractor Badges.....	13-2
6.	Facility Access Determination (FAD).....	13-2
PART III - PERSONNEL SECURITY PROGRAM ELEMENTS		
Chapter 14	PERSONNEL SECURITY POLICY.....	14-1
1.	Policy.....	14-1
2.	Applicability.....	14-1
3.	Commanders.....	14-1
4.	Designation of Civilian Sensitive Positions.....	14-1
Chapter 15	PERSONNEL SECURITY INVESTIGATIONS.....	15-1
1.	Policy.....	15-1
2.	Command Responsibilities.....	15-1
3.	Investigative Request Requirements.....	15-1
4.	JPAS.....	15-2
5.	Office of Personnel Management (OPM).....	15-2
6.	Preparation and Submission of PSI Requests.....	15-2
7.	Follow-Up Actions on PSI Requests.....	15-2
8.	Personnel Security Folders.....	15-2
Chapter 16	PERSONNEL SECURITY ACCESS DETERMINATIONS.....	16-1
1.	Policy.....	16-1
2.	Department of Defense Consolidated Adjudication Facility (DODCAF).....	16-1
3.	JPAS.....	16-1
4.	Eligibility Determination.....	16-1
5.	Unfavorable Determination.....	16-2
6.	Validity and Reciprocal Acceptance of Personnel Security Determinations.....	16-2
Chapter 17	PERSONNEL SECURITY ACCESS.....	17-1
1.	Policy.....	17-1
2.	Requests for Access.....	17-1
3.	Classified Information Non-Disclosure Agreement (SF-312)	17-1
4.	Verbal Attestation.....	17-2
5.	Interim Security Clearance Request (Access).....	17-2
6.	Access, Termination, Withdrawal, or Adjustment.....	17-3
7.	Suspension of Access for Cause.....	17-4

APR 12 2019

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 18	VISITOR CONTROL.....	18-1
1.	Policy.....	18-1
2.	Facilitating Classified Visits.....	18-1
3.	Visits by Foreign Nationals.....	18-1
APPENDICES		
APPENDIX A -	GUIDELINES FOR COMMAND SECURITY INSTRUCTION.....	A-1
APPENDIX B -	PROTECTED DISTRIBUTION SYSTEM (PDS) USER QUICK REFERENCE...	B-1
APPENDIX C -	CLASSIFIED MATERIAL CONTROL CENTER (CMCC).....	C-1
APPENDIX D -	IPSP EMERGENCY ACTION PLAN (EAP).....	D-1

APR 12 2019

Chapter 1

Command Security Program Authorities and Basic Policy1. Purpose. This Order establishes the IPSP.

a. This Order identifies procedures for classification, safeguarding, transmission, and destruction of CMI, as well as regulations and guidance for the IPSP. The term "Classified Military Information" is information originated by or for the Department of Defense (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, Secret, and Confidential, as described in reference (v). CMI may be oral, visual, or material form and has been subdivided further into eight categories per reference (v).

b. This Order implements the IPSP within Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands, and it is in compliance with references (a) through (w) to promote an effective Command Security Program.

c. This Order is also intended to serve as an example for subordinate commands to establish their Command's Security Program; the format of this Order, described in Appendix A, should be followed when developing local Command Security Program Orders.

2. Applicability. This Order applies to all personnel; military, DoD Civilians, DoD Contractors, and subcontractors, assigned to or employed by MCIEAST. Each person who handles CMI is responsible for safeguarding it, and is individually responsible for compliance with this Order and the reference 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 Classified Military Information (CMI). Certain information, referenced in the current edition of reference (b), is controlled by the Assistant Chief of Staff (AC/S) G-3/5 (Attn: Explosive Ordnance Disposal) and AC/S G-6 (Attn: Electronic Key Management System) and corresponding staff sections at subordinate commands. Security Managers whose Command Elements routinely handle special types of CMI should refer to the reference for governing regulations.

b. Controlled Unclassified Information (CUI). Reference (e) 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 (DON) 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 DON security official, while the Assistant for Information and

APR 12 2019

Personnel Security (CNO (N09N2))/Deputy Assistant Director, Information and Personnel Security Programs (NCIS-21) provides staff support for these functions and responsibilities.

b. The Commandant of the Marine Corps (CMC) administers the Marine Corps IPSP within the Marine Corps. CMC (PP&O/PS) is responsible for developing and implementing security related programs and policies Marine Corps wide.

c. The Commanding General (CG) administers the IPSP and is responsible for implementing the IPSP within Headquarters MCIEAST-MCB CAMLEJ and ensuring MCIEAST subordinate commands have implemented an IPSP and are in compliance with the references.

5. Policy Guidance. Reference (a) provides the basic guidance for personnel security matters. Reference (b) provides the basic guidance for the security and safeguarding of CMI, and reference (c) provides Marine Corps specific guidance for IPSP matters. This Order provides specific guidance for IPSP 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 MCIEAST-MCB CAMLEJ Command Security Manager for resolution.

b. The MCIEAST-MCB CAMLEJ Command Security Manager periodically publishes security awareness and training items in various formats. These publications are not directive in nature, but reflect official interpretation of emerging security policies and procedures impacting the IPSP.

c. Waivers and Exceptions. When conditions exist that prevent compliance with a specific safeguarding standard, or costs of compliance exceed available resources, MCIEAST subordinate commands may submit a request for a waiver or exception to this Order, in writing, to the MCIEAST-MCB CAMLEJ Command Security Manager.

APR 12 2019

Chapter 2

Command Security Manager Program Management

1. Policy. The CG is ultimately responsible for compliance and implementation of the MCIEAST-MCB CAMLEJ IPSP. The CG delegates this authority to ensure compliance and implementation to his MCIEAST subordinate commanders.

2. Commander

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

b. Commander's Responsibilities:

(1) Designate a Command Security Manager to implement the IPSP and maintain cognizance of all command information, personnel, and industrial security functions and ensure that the command's total security program is coordinated among other command security professionals, and is inclusive of all requirements in this Order.

(2) Designate a Top Secret Control Officer (TSCO) who reports directly to the Command Security Manager. The Command Security Manager may serve concurrently as the TSCO.

(3) Designate a Security Officer responsible for the Physical Security and Loss Prevention Program. The Command Security Manager may serve concurrently as the Security Officer.

(4) Designate an Information System Security Manager (ISSM) to serve as the point of contact for all Cybersecurity matters relating to all information systems and networks maintained and/or used by Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands.

(5) Issue a written command security instruction.

(6) Issue a written Emergency Action Plan (EAP) for the protection of CMI.

(7) Establish an Industrial Security Program in compliance with reference (f).

(8) Ensure the Command Security Manager and other command security professionals are properly trained, that all command personnel receive required security education, and the command has a robust security awareness program.

(9) Ensure command security inspections, program reviews, and assist visits to subordinate commands are conducted on a biennial basis, or more frequently if necessary. The decision as to what type of visit will be conducted will be dictated by local circumstances.

(10) Ensure the performance rating systems of all Marine Corps military and civilian personnel, whose duties significantly involve the creation, handling, or management of National Security Information (NSI), include a security element on which to be evaluated.

APR 12 2019

3. Command Security Manager. The Command Security Manager will be afforded direct access to the CG/Commander, Deputy Commander, and/or Chief of Staff to ensure effective management of the Command Security Program. The Command Security Manager must:

a. 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. The Command Security Manager must be a U.S. citizen and have been the subject of a favorably adjudicated T5 or T5R within the previous five years.

b. Be designated by name and identified to all members of the command on organization charts, telephone listings, rosters, etc.

c. Attend the Security Manager's Course within 180 days of appointment.

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 Commander 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 has all the necessary requirements to be successful. 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.

b. The Command Security Manager shall:

(1) Serve as the Commander's principal advisor and direct representative in matters pertaining to the classification, safeguarding, transmission, and destruction of CMI.

(2) Serve as the Commander's principal advisor and direct representative in matters regarding the eligibility of personnel to access CMI and to be assigned to sensitive duties.

(3) Develop written command information and personnel security procedures, including an EAP which integrates emergency destruction plans where required.

(4) Formulate and coordinate the command's security awareness and education program.

(5) Ensure security control of visits to and from the command when the visitor requires, and is authorized, access to CMI.

(6) Ensure coordination of staffing Foreign Visit Requests received from the Headquarters, U.S. Marine Corps (HQMC) Foreign Disclosure Officer, to include Extended Foreign Visits, the Foreign Liaison Officer (FLO) Program, and the Marine Corps Foreign Personnel Exchange Program (MCFPEP). Additionally, ensure 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.

APR 12 2019

- (7) Ensure all personnel who will handle CMI or will be assigned to sensitive duties are appropriately cleared through coordination with the Department of the Defense Central Adjudications Facility (DODCAF), and that requests for personnel security investigations are properly prepared, submitted, and monitored.
- (8) Ensure access to CMI is limited to those who are eligible and have a demonstrated need-to-know (NTK).
- (9) Ensure personnel security investigations, clearances, and accesses are properly recorded, with documentation in their Personnel Security File and the Joint Personnel Adjudication System (JPAS).
- (10) Coordinate the command program for continuous evaluation of eligibility for access to CMI, or assignment to sensitive duties.
- (11) Coordinate with the command ISSM on matters of common concern.
- (12) Ensure all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to CMI, with documentation of the event recorded at HQMC, and in JPAS.
- (13) Ensure all personnel granted access to the Secret Internet Protocol Router Network (SIPRNET) receive a North Atlantic Treaty Organization (NATO) SECRET security brief, and a debriefing when their access is rescinded, with documentation of the events recorded in JPAS.
- (14) Ensure all personnel requiring access to CMI (Secret or Top Secret), 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.
- (15) Per reference (g), 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 Military Occupational Specialties 2305 and 2336 in accordance with the current edition of reference (h), with documentation of the event recorded in their Personnel Security File and JPAS.
- (16) Ensure 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, etc.) receive a command debrief, with documentation of the event recorded in their Personnel Security File and JPAS.
- (17) Ensure all personnel who have had their access to CMI terminated as a result of separation, retirement, suspension, or revocation of access for cause have completed a Security Termination Statement, with documentation of the event recorded at HQMC, in JPAS, and in their Personnel Security File.
- (18) Ensure security collaboration with the Staff Judge Advocate (SJA) and Freedom of Information Act (FOIA) Coordinator in reviewing requests received under the FOIA that are, or could possibly be considered for, exemption from release under certain categories described in the current edition of reference (i).

APR 12 2019

(19) Ensure 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.

5. Assistant Command Security Manager. The Assistant Command Security Manager, if assigned, shall:

a. Be either a staff sergeant (E-6) or above, or a civilian employee in the Security Administration Series GS-0080 in the pay grade GS-06 or above.

b. Provide knowledgeable assistance to the Command Security Manager in all facets of the Command Security Program, and be capable of assuming the duties in the absence of the Command Security Manager.

c. Be a U.S. citizen and have been the subject of a favorably adjudicated SSBI or SSBI/PR completed within the previous five years.

d. Attend the Security Manager's Course within 180 days of appointment.

6. TSCO. MCIEAST subordinate commands that handle Top Secret CMI will designate a TSCO in writing. The Security Manager may serve concurrently as the TSCO. The TSCO must:

a. Be a gunnery sergeant (E-7) or above, or a civilian employee in the pay grade of GS-07 or above.

b. Be a U.S. citizen and have been the subject of a favorably adjudicated SSBI or SSBI/PR completed within the previous five years.

c. The TSCO shall:

(1) Be responsible for all Top Secret CMI handled within their command. Top Secret CMI will be controlled per the provisions of the current edition of reference (b) and this Order.

(2) Maintain a system of accountability to record the receipt, reproduction, transfer, transmission, downgrading, declassification, and destruction of Top Secret (TS) information, less Sensitive Compartmented Information (SCI) TS CMI.

(3) With the assistance from the Classified Material Control Center (CMCC) the TSCO shall maintain all records and reports reflecting the processing of Top Secret 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.

(4) Ensure inventories of Top Secret information are conducted at least once annually, with results maintained for five years.

7. Security Officer. The Commander 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 (d).

APR 12 2019

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 shall:

a. Be responsible to the Command Security Manager for coordinating with program managers and technical and procurement officials.

b. Ensure the industrial security functions are accomplished when CMI or controlled unclassified information as defined in reference (e), or operationally sensitive information is provided to industry for performance on a classified or unclassified contract.

c. Be guided by the provisions of the current edition of reference (b).

9. 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 within command element divisions, branches, or General and Special Staff Departments.

b. Those command elements, or the general and special staff departments maintaining billets requiring the processing of CMI, and desiring assignment of a Security Assistant, shall nominate to the Command Security Manager, a Security Assistant. Upon Command Security Manager concurrence, an appointment letter signed by the Command Security Manager shall be forwarded to the Security Assistant through the General or Special Staff Department.

c. Security Assistants shall maintain liaison with the Command Security Manager relative to security matters, and are responsible to their division and branch heads for dissemination of and compliance with security policy and procedures.

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

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

f. Security Assistants may be assigned duties pertaining to Personnel Security, CMCC, Top Secret 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. Each General or Special Staff Department authorized to receive, store, or process CMI shall designate a SCP Custodian. The custodian shall 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

APR 12 2019

responsible to the CMCC for accountability of CMI maintained within their respective SCPs.

(3) Top Secret Control Assistants. If required, each General or Special Staff Department authorized to receive, store, or process TS CMI shall designate a TS Control Assistant. The TS Control Assistant shall be responsible for all TS CMI originated, stored, received, or processed by their respective section. The duties of the Top Secret Control Assistant shall be assigned in writing. The Top Secret Control Assistants are responsible to the TSCO.

10. General and Special Staff Department Responsibilities

a. The AC/S G-3/5 shall manage, advise, and assist the Command Security Manager on operations security and Anti-Terrorism/Force Protection (AT/FP) issues.

b. The AC/S G-4 shall review security equipment procurement requests from the Command Security Manager or other General and Staff Departments Heads, who will submit procurement requests via the Purchase Request (PR) Builder process and manage accountable property held by the Command Security Manager through the Accountable Property System of Record.

c. The AC/S G-6 is responsible to the CG for development, maintenance, and implementation of the Cybersecurity program within the activity. The G-6 advises the CG on all Cybersecurity matters, including identifying the need for additional Cybersecurity staff. The G-6 serves as the command's point of contact for all Cybersecurity matters and implements the command's Cybersecurity program.

d. The Director, Communications Operation Strategy (COMMSTRAT) shall advise and assist the Command Security Manager on security reviews before public release of briefs and articles.

e. The Command Security Manager will manage and advise General and Special Staff Departments Heads and MCIEAST subordinate commands on document and material security administration and control.

11. Internal Security Procedures

a. All MCIEAST subordinate commands, divisions, branches, and MCIEAST-MCB CAMLEJ General and Special Staff Departments 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, requiring and recording clearance and access, security education, and the control of visitors.

12. Security Service Agreements (SSAs)

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.

APR 12 2019

b. The SSAs shall be specific and clearly define the security responsibilities of each participant. All agreements 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 commands Chiefs of Staff or an equivalent command official.

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

a. MCIEAST-MCB CAMLEJ will, on a biennial basis, conduct inspections, assist visits, or reviews to examine the overall security posture of Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands.

b. MCIEAST subordinate commands will, on an annual basis, conduct inspections, assist visits, or reviews to examine overall security posture of their subordinate elements.

c. Internal reviews of Command Security Functions will be conducted as required by this Order, and the Command Security Manager using the Functional Area Checklist available on the Inspector General of the Marine Corps, Inspections Division, web page:
<http://www.hqmc.marines.mil/igmc/Resources/Functional-Area-Checklists/>.

APR 12 2019

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 ensure 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 all personnel (Active, Reserve, DoD (USN) Civilians, Contractors, and Sub-Contractors), who will have access to CMI, receive an orientation briefing and training that includes accountability, proper safeguarding, and storage of CMI at the time of assignment. Thereafter, personnel will participate in a continuous security education program consisting of selected briefings, annual security refresher training, and on-the-job training (OJT) within the scope of information contained in paragraph 3c below.

b. The Command Security Manager is responsible for ensuring all DoD civilians, who are entering employment with the civil service at their command, and who have never held a clearance, receive a security indoctrination brief which is detailed in the current edition of reference (a).

c. General and Special Staff Department Heads, with assistance from the Command Security Manager, are responsible for identifying the security requirements for the functions under their cognizance, and for ensuring personnel under their supervision are familiarized with the security requirements for their particular assignments. The General and Special Staff Department's Security Assistants shall 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 MCIEAST-MCB CAMLEJ and MCIEAST subordinate command personnel, 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.

APR 12 2019

b. Advise personnel of their 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 and access to CMI or assignment to sensitive duties.

e. Familiarize personnel with the principles, criteria and procedures for the 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 the security requirements for their particular assignments and identify restrictions.

g. 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.

h. 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.

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

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

k. 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; or

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

1. 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 which shall include the procedures for the proper safeguarding of CMI; this briefing is normally conducted when processing individuals for security access. Executive level orientation briefs should be made available for principal staff and flag officers; format for the briefs are available on the MCIEAST-MCB CAMLEJ Security Branch website:

<http://www.mcieast.marines.mil/Staff-Offices/Adjutant/Security-Manager/>

APR 12 2019

b. 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. Annual refresher briefings are available online at the MCIEAST-MCB CAMLEJ Security Branch website listed above, or can be provided live onsite upon request.

c. Counterintelligence Briefings. Annually, all personnel who have access to CMI classified Secret or above, must receive a counterintelligence (CI) briefing. 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. All personnel requiring SIPRNET accounts will be briefed to NATO SECRET before SIPRNET access is granted. An example of the NATO security briefing is available online at the MCIEAST-MCB CAMLEJ Security Branch website. NATO debriefs will be conducted in conjunction with the Command Security Debrief (see paragraph 5a), 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. CNWDI. Certain commands are listed as certifying officials for CNWDI, per the provisions of reference (g), for 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, Nuclear, and High Yield Explosives (CBRNE) personnel. For those commands not listed as certifying officials per reference (g), the MCIEAST-MCB CAMLEJ Command Security Manager shall provide CNWDI certification and decertification. Ensure you record RD/CNWDI briefing/debriefing within JPAS.

d. Complete other special briefings as circumstances dictate or directed, e.g., Annual Building 1 and Legal Service Support Section-East personnel security brief.

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.

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 a security clearance is administratively withdrawn;

(4) When a member of the command who possesses no clearance or access, has inadvertently gained access to CMI; and/or

APR 12 2019

(5) When security clearance eligibility is revoked for cause by the DODCAF.

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; and/or

(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 Electronic Service Record (ESR) and Official Personnel File (OPF) 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 CMC (P&PO/PS). The command debriefing form (available on the MCIEAST-MCB CAMLEJ security website identified in paragraph 5a above) will be retained in the individual's Personnel Security Folder.

8. Continuing Security Awareness

a. 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.

b. On-the-job-training (OJT). Supervisors must ensure 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 the security posture of the office is being maintained per this Order.

APR 12 2019

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 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 accounted for or located.

(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 MCIEAST-MCB CAMLEJ 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 notice, reprimand, suspension without pay, removal, or termination. Repetitive security infractions or security violations resulting in the loss or compromise of classified material will also result in the submission of an incident report.

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. Repetitive security infractions or security violations resulting in the loss or compromise of classified material will also result in the submission of an incident report.

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

APR 12 2019

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 shall:

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 Commander to initiate a Security Inquiry (SI).

c. Advise the MCIEAST-MCB CAMLEJ SJA that a SI is being conducted.

4. Security Inquiry (SI). Per the current edition of reference (b), a SI will be initiated when CMI is lost, compromised, or subjected to compromise. The command element's headquarters CO will assign an officer to conduct the SI.

a. SIs will be conducted by an individual assigned external to the Security Branch, and to the General or Special Staff Department requiring the inquiry. At a minimum, the officer conducting the SI will complete the following actions:

(1) Identify incident circumstances in the course of the inquiry as indicated:

(a) Identify the incident CMI completely and accurately. This identification should include the classification of the CMI, all identification or serial numbers, the date, the Original Classification Authority (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.

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

(c) Identify the individual responsible, if possible.

(d) Identify procedural weaknesses, security, and otherwise, what allowed the incident to occur.

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

(2) Establish either:

(a) 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; or

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

(3) Determine overall classification of SI results. Every effort shall be made to keep the SI unclassified and without enclosures. However, if the lost

APR 12 2019

information is beyond the jurisdiction of the U.S., and cannot be recovered, the SI shall be classified commensurate to the security classification level of the lost information to prevent its recovery by unauthorized personnel.

(4) All SI's 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 SI into naval message format addressed to CMC WASHINGTON DC PPO PS, CNO WASHINGTON DC (N09N2), COMMCICOM, the originators of lost or compromised CMI, OCA's if known, NCIS, and or any other commands involved in the SI.

(5) If during the conduct of the SI a compromise, or possible compromise in fact did not occur, the SI shall still continue to completion to determine what security weaknesses existed that permitted the violation to occur. MCIEAST subordinate commands shall provide an info copy of SIs to the MCIEAST-CAMLEJ Command Security Manager. No further reporting of these results external to MCIEAST is required.

(6) If during the conduct of the SI a 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 SI in naval letter format to naval message format, addressed to CMC WASHINGTON DC PPO PS, CNO WASHINGTON DC (N09N2), COMMCICOM, the originator, the OCA, and the local NCIS office. When a SI 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 Judge Advocate General Manual (JAGMAN) investigation 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 SI 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 are included in chapter 12 of the current edition of reference (b). MCIEAST-MCB CAMLEJ subordinate commands will address their completed JAGMAN investigations to CNO WASHINGTON DC (N09N2) via the CG MCIEAST-MCB CAMLEJ, COMMCICOM, and CMC WASHINGTON DC PPO PS. Whenever a violation of criminal law appears to have occurred and criminal prosecution is contemplated, the Security Branch shall notify the Eastern Area Counsel Office.

6. Investigative Assistance. A SI or JAGMAN 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, 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. User's should report losses or compromises to their local Security Managers. MCIEAST subordinate commands will route all correspondence involving losses or compromises via the MCIEAST Command Security Manager. Report losses or compromises involving computer systems to the CNO WASHINGTON DC (N09N2), who will notify the Director, Information Assurance, OASD (C3I).

APR 12 2019

b. Report losses or compromises involving Communications Security (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 SI requirements of this Order, and will be forwarded to the MCIEAST Command Security Manager, CNO WASHINGTON DC (N09N2), National Security Agency (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 MCIEAST-MCB CAMLEJ Command Security Manager, COMMCICOM, CMC WASHINGTON DC PPO PS, and CNO WASHINGTON DC (N09N2) with a copy to the local NCIS office.

d. Immediately report incidents indicating a deliberate compromise of classified information, or indicating possible involvement of a foreign intelligence agency, to the local NCIS office. MCIEAST subordinate commands will inform the MCIEAST-MCB CAMLEJ 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. MCIEAST subordinate commands will inform the MCIEAST-MCB CAMLEJ Command Security Manager on all correspondence involving CMI previously reported as lost or compromised.

9. Compromise through Public Media. If any member of the command becomes aware that CMI may have been compromised as a result of disclosure in the public/social media, i.e., newspaper, magazine, radio, or television, the member must notify the Command Security Manager, who in turn will notify the MCIEAST-MCB CAMLEJ Command Security Manager, COMMCICOM, CMC WASHINGTON DC PPO PS, and CNO WASHINGTON DC (N09N2).

10. Unauthorized Disclosure through Spillage. The term "Spillage" is a Cybersecurity term that refers to any incident where CMI is introduced on an Information Technology (IT) System/Network of a lower classification and/which is not authorized to store, process, or transmit the higher classification 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 ISSM shall be promptly notified and take appropriate action per current IA directives. Paragraph 4 above provides detailed guidance concerning the conduct of a SI.

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 SI must also be vigorously and thoroughly conducted. This gives division, branch, and general and special staff sections a "second chance" to shore up their security program before a compromise does occur. Paragraph 4 above provides detailed guidance concerning the conduct of a SI. 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.

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)/Officer-of-the-Day (OOD). The

APR 12 2019

container will be guarded until the CDO/OOD arrives at the location of the unlocked container. The CDO/OOD will then inspect the CMI involved, lock the container and notify the Command Security Manager immediately for situation awareness and addition guidance. If the CDO believes that CMI may have been compromised, the CDO will immediately notify the Command Security Manager and recall the person responsible for the container to conduct a complete inventory. The Command Security Manager will report incident to the Chief of Staff.

13. Improper Transmission

a. All CMI received at tenant commands 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 General Services Administration (GSA) contract for overnight delivery services (i.e., Federal Express, Airborne Express, etc.), it is possible that MCIEAST and subordinate command division, branch, and MCIEAST-MCB CAMLEJ General and Special Staff Departments 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 either verbally or in writing.

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

d. All instances of mishandling, where compromise cannot be ruled out, must be formally reviewed through a SI, as discussed in paragraph 4 above.

APR 1 2 2019

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/temporary additional duty, the nearest command, any activities described in this chapter involving themselves, their dependents, or others.

2. Sabotage, Espionage, International Terrorism, or Deliberate Compromise

a. An individual who becomes 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 (DIRNAVCRIMINVSERV WASHINGTON DC) by SECRET IMMEDIATE naval message, and info copy the CG MCIEAST-MCB CAMLEJ, CG MCIEAST-MCB CAMLEJ G1, CG MCIEAST-MCB CAMLEJ G3/5, CG MCIEAST-MCB CAMLEJ G6, COMMCICOM, CMC WASHINGTON DC PPO PS, and CNO WASHINGTON DC//N09N2//.

b. The Command Security Manager shall 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 Orders, 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 shall report to the Command Security Manager contacts with any individual, regardless of nationality, whether within or outside 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, email, 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 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, which is verified by a competent medical authority, subordinate Command Security Managers shall immediately report the incident to the local NCIS office, the MCIEAST-MCB CAMLEJ Command Security Manager, and DODCAF. An incident report shall be submitted via JPAS. Additionally, command initiated investigations must be coordinated with the local NCIS office.

APR 12 2019

b. Unauthorized Absentees (UAs). When a member of the command, who currently has, or has had access to CMI, is in a UA status, the subordinate 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 subordinate Command Security Managers will report all information to the local NCIS office, and info the MCIEAST-MCB CAMLEJ Command Security Manager and DODCAF. NCIS will advise whether they will conduct an investigation. An incident report shall be submitted via JPAS, and access will be terminated.

c. Death or Desertion. When a member of the command, who currently has or had access to CMI dies or is declared a deserter, the subordinate Command Security Manager shall 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 subordinate Command Security Manager will report all information to the local NCIS office, info the MCIEAST-MCB CAMLEJ Command Security Manager and DODCAF. NCIS will advise whether they will conduct an investigation. An incident report shall be submitted via JPAS, all access will be terminated; the subject shall be removed from any JPAS owning or servicing relation.

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 United States. 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 DODCAF.

APR 12 2019

Chapter 6

Classification Management1. Policy

a. References (b) and (c) are the only basis for classifying information except as provided in reference (m). It is DON policy 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 Principles and Considerations. MCIEAST-MCB CAMLEJ is not an original classification authority. Specific principles and considerations for original classification are contained in reference (e).

3. 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 paragraphs 3b(1) through 3b(10) 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;
- (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; and/or

APR 12 2019

(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.

4. Classification Designations

a. Information which requires protection against unauthorized disclosure in the interest of national security must be classified in one of three designations: "Top Secret," "Secret," or "Confidential." The markings for Controlled Unclassified Information, as defined in reference (e), 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 reference (n), 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. "Top Secret" 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.

5. Tentative Classification. All command element division, branch, or general and special staff departments 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 the Command Security Manager for review and a security determination.

6. Limitation of 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.

APR 12 2019

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.

7. 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 Headquarters MCIEAST-MCB CAMLEJ, MCIEAST subordinate commands, or from other commands, the matter will be referred to the member's Command Security Manager for review.

8. 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, all of the classified information produced by Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands is derivatively classified, 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 markings that apply to the source. This includes classification of information based on OCA classification guidance (Security Classification Guides).

(1) Security Classification Guides (SCGs) serve both legal and management functions by recording DON original classification determinations made under reference (1).

(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 reference (b) and (c).

APR 12 2019

d. All personnel who create classified informational work products are derivative classifiers and are required to complete derivative classification training annually to maintain certification.

9. 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.

10. Foreign Government Information (FGI). Occasionally, Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands receive CMI 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 reference (b) 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 7 above.

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).

APR 12 2019

Chapter 7

Classification Review

1. Policy. The Command Security Manager must provide for the systematic review of locally produced CMI to ensure correct classification and marking, and to comply with reporting requirements of the Information Security Oversight Office (ISOO).
2. Marking Requirements. All CMI originating within Headquarters MCIEAST-MCB CAMLEJ, MCIEAST subordinate commands, and tenant 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; downgrading and/or declassification instructions; warning notices, intelligence control markings, and other miscellaneous markings. Marking guidance contained in the following documents is to be adhered to:
 - a. The current edition of reference (b), specifically chapter 6;
 - b. Reference (c); and
 - c. Reference (e).
3. Review Requirements. The Command Security Manager is responsible for ensuring all locally produced CMI is reviewed upon completion for appropriate classification and marking. The Command Security Manager may delegate the authority to complete these reviews to the division, branch, or General and Special Staff Department Security Assistants.
 - a. The Command Security Manager shall 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 is responsible for determining final classification and marking.
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 4 of the current edition of reference (b).

APR 12 2019

Chapter 8

CMI/CUI Control Measures1. Policy

a. Commanders shall ensure 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) "Personal notes" taken during classified briefs or training 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) are required to be accounted for in the CMCC. Once the Responsible Officer (RO) signs for their computers that are designated to be connected to the SIPRNET, they will be delivered to the Command Security Manager who will mark the computer with the appropriate magnetic media classification labels, and will then be "buck-tagged" and issue them to the SCPs for local accountability. The HDDs contain classified elements that are the property of the U.S. Government; these local procedures must be followed to ensure 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 encompass all CMI regardless of the media on which it may be represented.

3. Top Secret Control Measures

a. All Top Secret CMI (including copies) received by Headquarters MCIEAST-MCB CAMLEJ or MCIEAST subordinate commands shall be continuously accounted for, individually serialized with a locally developed "buck-tag" and entered into a command Top Secret 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 Top Secret Control Log will be retained for 5 years after the material is transferred, downgraded, or destroyed.

b. In addition to the marking requirements of chapter 6 of reference (b), Top Secret information derivatively classified by Headquarters MCIEAST-MCB CAMLEJ or MCIEAST subordinate commands shall be marked on their "buck-tag" with an individual copy number in the following manner "Copy No. __ of __ copies";

APR 12 2019

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 Top Secret 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 Top Secret information require the applicable Top Secret accounting, control, and marking requirements prescribed for finished product CMI.

e. Top Secret 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 Top Secret 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. Top Secret documents will be physically sighted or accounted for by examination of written evidence of proper disposition, such as certificate of destruction, transfer receipt, etc., at least once annually, and more frequently when circumstances warrant. At the same time, Top Secret records will be audited to determine completeness and accuracy.

h. Retention of Top Secret documents within Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands will be kept to a minimum. When Top Secret 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 5 years.

i. Whenever Top Secret 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 (4 PT), OPNAV 5216/10. TSCOs shall obtain a classified material receipt, which may be documented on a Correspondence/Material Control (4 PT), OPNAV 5216/10, from each recipient for Top Secret information distributed externally.

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

k. When Top Secret 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.

APR 12 2019

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 subordinate commands;

(2) Records of CMI distributed or routed to sub-elements of or activities within the subordinate commands;

(3) Records of CMI disposed of by subordinate commands through transfer of custody or destruction; and

(4) Requirements for annual inventory.

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

c. Correspondence/Material Control Sheets (4 PT), OPNAV 5216/10, or a locally developed "buck-tag" will be attached to all Secret CMI under the control of CMCC; classified removable Hard Disk Drives (HDDs) will have the "buck-tag" affixed with the HDD's serial number printed thereon.

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:

(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:

APR 12 2019

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

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

d. Marking e-mail generated on the SIPRNET: 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.

6. Confidential Control Measures. The control requirements of Confidential information is less stringent than those for Secret: decentralized printing, copying, 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 the CMCC, for copying, accounting, distribution, and destruction.

7. Working Papers

a. Working papers such as classified notes from a training course or conference, research notes, drafts, and similar items that contain classified information and are not finished documents shall be:

(1) Dated when created;

(2) Conspicuously marked "Working Papers" on the first page in letters larger than the text;

(3) Marked centered top and bottom on each page with the highest overall classification level of any information they contain;

(4) Protected per the assigned classification level; and

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

b. All 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 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.

8. Inventory of Classified Material. The MCIEAST-MCB CAMLEJ CMCC/Security Manager will conduct physical inventories of all controlled classified holdings on a monthly basis. The Staff Communications Material Systems Responsible Officer (SCMSRO) shall conduct physical inventories of EKMS material as required by pertinent references and as directed by the Chief of Staff.

9. Special Handling Requirements. MCIEAST subordinate 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

APR 12 2019

Special Category (SPECAT), Limited Distribution (LIMDIS), and "Personal For (P4s)."

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

a. Restricted Data (RD), Formerly Restricted Data (FRD), and Critical Nuclear Weapons Design Information (CNWDI). RD, FRD, and CNWDI are controlled per the current edition of reference (g).

b. Communications Security (COMSEC) Material. Control COMSEC per the current edition of reference (p).

c. For Official Use Only (FOUO). Control FOUO per the current edition of reference (i). Additional guidance in applying the FOUO designation is provided in paragraph 11e(3) below.

d. Sensitive But Unclassified (SBU) Information. Control SBU information per the current edition of reference (i).

e. Controlled Unclassified Information (CUI)

(1) Reference (e), Volume 4, enclosure (3), Identification and Protection of CUI, covers several types of unclassified controlled information, including "DEA Sensitive Information," "Law Enforcement Sensitive," "DoD Unclassified Controlled Nuclear Information," and "Sensitive But Unclassified Information" and provides basic procedures for identification and control.

(2) All material prepared for release into the public domain in any format will be subject to an Intra-Command review for public release per references (o), (q), and (r). The review will be coordinated between a Subject Matter Expert (SME) on the material to be released, the Security Manager, the FOIA Coordinator, and may include a SJA and the Director, COMMSTRAT.

(3) Information that has been determined to be exempt from mandatory disclosure incident to the FOIA, shall be designated "UNCLASSIFIED//FOR OFFICIAL USE ONLY" and marked accordingly. Use overall page markings on UNCLASSIFIED//FOR OFFICIAL USE ONLY documents as follows:

Top of Page in the header and above the letter head if used:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Bottom of Page in the footer and above the page number if used:

UNCLASSIFIED//FOR OFFICIAL USE ONLY
(Exempt from mandatory disclosure under the FOIA,
Exemption (insert #) applies.)

Note 1: Include "(Exempt from mandatory disclosure under the FOIA, Exemption (insert #) applies.)" on the bottom of the first page only of a multi-page U//FOUO document.

Note 2: Exemption #1 is not used for U//FOUO documents since this exemption applies to classified information which is always exempt from disclosure under the FOIA.

APR 12 2019

(4) It is not necessary to use the portion marking (U//FOUO) within the content of an UNCLASSIFIED//FOUO document when all the information contained therein is UNCLASSIFIED//FOUO.

(5) Within an UNCLASSIFIED//FOUO document containing both UNCLASSIFIED//FOUO and public domain UNCLASSIFIED information, use the portion markings (U//FOUO) or (U) as applicable.

(6) When UNCLASSIFIED//FOUO is incorporated into a classified document:

(a) Use the portion marking (U//FOUO) in the same manner as (TS), (S), (C), or (U).

(b) Under the "Derived From" and "Declassify On" statements, insert the statement "U//FOUO information included herein is exempt from mandatory disclosure under the FOIA, Exemption (insert #) applies."

(7) Tips for safeguarding UNCLASSIFIED//FOUO1 information/documents:

(a) Do not post U//FOUO documents on public domain web sites.

(b) Limit Distribution Statements within the US Government domain.

(c) Dispose of U//FOUO documents represented on paper using a cross cut or strip document shredder.

(d) Dispose of electronic copies of U//FOUO documents in the same manner as digital classified documents represented on either magnetic or optical media.

(e) Transmit U//FOUO information within or attached to an encrypted and digitally signed NIPRNET e-mail, always including (U//FOUO) at the beginning of the "SUBJ" line, along with (U//FOUO) portion markings within the body of the e-mail as required. U//FOUO information may also be transmitted as a SIPRNET e-mail with these same "SUBJ" line and portion marking requirements.

(f) As a best business practice within a NIPRNET or SIPRNET e-mail containing U//FOUO information within the body of the e-mail, include the statement "(Exempt from mandatory disclosure under the FOIA, Exemption (insert #) applies.)" above the signature/salutation of the e-mail.

APR 12 2019

Chapter 9

CMI Dissemination1. Policy

a. Within Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands, the dissemination of classified and controlled unclassified material 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 9 of the current edition 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 Top Secret CMI will only be routed from the TSCO to a SCP and returned to the TSCO. Top Secret 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, will not be permanently routed from one SCP to another SCP without being processed via the CMCC for appropriate accountability. 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.

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

a. RD and CNWDI will only be disseminated per the provisions in the current edition of references (a) and (g).

b. Cryptographic and COMSEC Distributed Information. All cryptographic and COMSEC distributed information will be disseminated pursuant to the current edition of reference (p).

c. For Official Use Only (FOUO). FOUO material may be disseminated within DoD components. All requests from non-DoD entities to disseminate FOUO outside Headquarters MCIEAST-MCB CAMLEJ and MCIEAST subordinate commands will be routed through the FOIA Coordinator.

d. Sensitive But Unclassified (SBU). SBU material will be handled in the same manner as FOUO.

e. Sensitive Information. Sensitive information as defined by reference (n) shall be disseminated on a need-to-know basis.

APR 12 2019

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. 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 references (i) and (o).

APR 12 2019

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 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.

APR 12 2019

(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 Commander, Naval Surface Warfare Center Crane, Indiana (Code 4044).

d. All restricted areas require a Physical Security Survey conducted by the servicing Provost Marshal's Office (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. Protected Distribution System (PDS)

a. A PDS is used to transmit unencrypted National Security Information (NSI), in lieu of a National Security Agency approved Type 1 cryptographic device, through an area controlled at a lesser classification level. In as much as the NSI is unencrypted, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation. Since a PDS can be penetrated, given the opportunity and adequate time, a philosophy of detection of attempted penetration is employed. PDS is governed by reference (1).

b. Incidents of tampering, penetration, or unauthorized interception must be reported immediately to the ISSM for assessment and the local Security Manager for review and initiation of an investigation. Subject to law enforcement procedures, which take precedence, the PDS should not be used until the incident is assessed and its security status determined.

c. The PDS terminal equipment shall be installed in a secure room (SR), controlled access area (CAA) or restricted access area (RAA) inside of a GSA approved class five information processing safe (IPS). The command security manager for the PDS shall determine which areas constitute a SR in accordance with reference (b). In addition, the command security manager will designate which areas, through which the PDS will run, are considered CAAs, RAAs or LAAs. The PDS Certification Authority shall validate these determinations.

d. On a daily basis, PDS drop boxes and PDS conduits will be inspected to ensure they are properly secured and that any incidents of tampering, penetration, or unauthorized interception are reported immediately to the Information Assurance Manager for assessment, and the command security manager for review and initiation of an investigation, if necessary.

e. The daily visual inspection shall be performed along the entire length of the PDS. The PDS carrier (e.g., conduit, buried path, etc.), connections, lock boxes, and terminal/pull boxes shall be assessed for signs of penetration, tampering, and any other anomaly causing a deterioration of protection safeguards. Locks and tamper evident seals, if used, will also be inspected. The PDS shall be inspected from a distance no greater than one meter. Adequate lighting must be

APR 12 2019

provided to reveal any attempts at penetration. The person(s) formally appointed by the Security Manager or Executive Staff to accomplish the visual inspection must be trained sufficiently to recognize physical changes in PDS, including attempts at penetration and tampering.

f. A document titled PDS User Quick Reference is included as Appendix B to provide guidance for all personnel working in office spaces that house PDS boxes.

5. Safeguarding Work Spaces

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

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 CMI is 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 collocated with trash receptacles as the subconscious act of discarding waste material could result in CMI being discarded with regular trash.

f. Classified information shall not be discussed over unsecured telephone lines. Secure Telephone Equipment (STE) and 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. Do not download and transfer any unclassified CMI from a classified AIS system to an unclassified AIS without explicit approval and assistance from the ISSM.

h. Current MCIEAST-MCB CAMLEJ 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 ISSM. 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 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.

APR 12 2019

6. 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 as applicable.

c. All NIPRNET computers and cabled peripherals (with the exception of keyboards, mice, and speakers) will be labeled with System Accreditation Labels, NAVMC 11180. All SIPRNET computers and cabled peripherals will be labeled with "SECRET" System Accreditation Labels, NAVMC 11182.

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 an Activity Security Checklist, SF 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. The SF 701 and 702 shall be annotated to reflect after hours, weekend, and holiday activities in secure areas.

7. Safeguarding in Storage

a. Commanders are responsible for the safeguarding of all classified information 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 (e.g., 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 10 of the current edition of reference (b). Additional information relevant to command responsibilities in this reference include:

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

APR 12 2019

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

8. 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 18 of this Order.

9. Safeguarding During Classified Meetings

a. Commanders shall ensure classified discussions at meetings are held only when disclosure of the information serves a specific U.S. Government purpose. Current OSD 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 Level (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 Top Secret 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 ISSM. All PEDs, standard or wireless, such as cell phones, audio recorders, imaging devices, blackberry's, are prohibited within classified conference rooms.

d. Personal Wearable Fitness Devices (PWFD), e.g., Fitbit, Jawbone Up, Nike Fuel Band, Garmin VivoFit with heart monitor, etc., are authorized per reference (t), subject to the capability limitations below:

(1) If commercially available in the U.S. or through a U.S. military exchange, marketed primarily as fitness or sleep device, and designated as Federal Communication Commission (FCC) Class B digital device (denoted as FCC Class B certified, or FCC Class B exempt).

(2) If they have Bluetooth, Global Positioning System or GPS (receive only), accelerometer, altimeter, gyroscope, heart activity, vibration feature, or near field communication capabilities.

(3) If they receive and contain vendor-supplied software updates that do not add any features or capabilities prohibited below.

e. Personal Wearable Fitness Devices are PROHIBITED:

(1) If they contain any external or conflicting hardware or software modifications, including the installation of third party apps. Authorized devices will receive only vendor-supplied software updates that do not add any prohibited features or capabilities.

APR 12 2019

(2) If they contain cellular or Wi-Fi, photographic, video capture/recording, microphone, or audio recording capabilities. Merely disabling the cellular, camera, or video capability is not sufficient.

(3) In conjunction with Universal Serial Bus (USB) accessories, including but not limited to Bluetooth dongles and charging cables.

(4) From being connected to any government information systems.

f. 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 the current edition of reference (b).

10. 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 NTK). 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: SF 705

b. SECRET: SF 704

c. TOP SECRET: SF 703

11. Safeguarding CMI while in a 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 their designated representative, usually the Command Security Manager, must sign the authorization.

b. Couriers traveling Outside the Continental United States, where the courier's mode of travel is other than government conveyance, must receive pre-approval by the MCIEAST-MCB CAMLEJ Command Security Manager prior to embarking.

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 on the following safeguard requirements:

APR 12 2019

(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.

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.

APR 12 2019

Chapter 11

CMI Duplication and Distribution1. Policy

a. The policy within Headquarters MCIEAST-MCB CAMLEJ and MCIEAST 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 are restricted from introduction to any area where CMI is processed, stored, or discussed unless prior approval is obtained from the Command Security Manager.

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

(a) 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.

(b) 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 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.

(c) 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.

(d) 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.

APR 12 2019

(2) Distribution

(a) 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, pen drives, thumb drives, 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.

1. 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, then allow for non-network file transfer when physically introduced to another accredited classified computer's drives and devices. Flash based storage media such as flash drives pose an unacceptable risk to national security and are not authorized unless approved by MCIEAST Cybersecurity division.

2. 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.

(b) A discussion of classified computer HDD primary storage is covered in chapter 8, paragraphs 1(b)(2), and chapter 10, paragraph 6b of this Order.

c. 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 8 of this Order details the procedures to follow for CMCC control.

d. 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 their 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 Top Secret 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 8 of this Order.

APR 12 2019

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:

a. Accountable (finished product) CMI will only be copied by the CMCC/SCP on a "classified copier." Multifunction devices can only be introduced on Marine Corps networks with approval from the C4 Authorizing Official (AO).

b. Top Secret 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. Confidential and Secret messages and working papers may be copied by divisions, branches, and special staff sections under the following conditions:

(1) The division, branch, or General or Special Staff Department has a "classified copier" that has been approved by the Command Security Manager for copying CMI.

(a) 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)."

(b) Copiers not authorized for CMI reproduction will have a warning notice: "THIS DEVICE IS NOT AUTHORIZED FOR PROCESSING CLASSIFIED MILITARY INFORMATION."

(2) The SCP Custodian of the particular division, branch, or General or Special Staff Department will provide local approval authority for all CMI copied within their custodial area of responsibility. SCP's must contact the CMCC when additional finished materials are copied to ensure proper tracking of items.

d. 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.

e. 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.

f. Upon completion of copying, check the copier to ensure the original and all copies have been removed. Users of mixed media machines (those used for multiple classification categories, such as SECRET, CONFIDENTIAL, and UNCLASSIFIED) must purge any latent images of the CMI on copier components immediately after processing CMI on the copier: make copies of a sheet of paper containing unclassified, high-density text, with few blank or black spaces per the following:

(1) To purge CONFIDENTIAL latent images, make one copy of unclassified following the classified copying.

APR 12 2019

(2) To purge SECRET latent images, make three copies of unclassified text following the classified copying.

(3) To purge TOP SECRET latent images, make nine copies of unclassified text following the classified copying.

4. Controls on Facsimile (FAX) Devices

a. Those divisions, branches, and General and Special Staff Departments 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. Divisions, branches, and General and Special Staff Departments 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 Top Secret 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; and
- (5) Description of material sent, e.g., "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 8 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 immediately after processing CMI; see chapter 11, paragraph 3f 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."

5. 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.

APR 12 2019

6. Controls on Printer Devices

a. Classified computers may only be connected to printers accredited to process CMI. Only classified printers may process CMI. Appropriate classification labels will be affixed to each printer.

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 General or Special Staff Departments SCP as required by chapter 8 of this Order.

7. Controls 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 division, branch, or special staff section SCP as required by chapter 8 of this Order.

8. Controls of Visual Recording Devices. Command Security Managers will ensure that only official photography and/or video (when required) is authorized in areas under their cognizance. Normally, such photography/video 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 ISSM.

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 tenant command's Combat Camera, COMMSTRAT, 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 division, branch, or General or Special Staff Department SCP as required by chapter 8 of this Order.

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

a. Only those devices approved jointly by the ISSM and the Command Security Manager are authorized for downloading CMI.

(1) 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 and Cybersecurity Division; as such, these USB flash memory devices should be considered "data transfer" vice "data storage" devices.

APR 12 2019

(2) 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.

(3) Secondary storage media must be labeled properly with a CMCC control number, and the appropriate media classification label must be affixed. If the size of the device precludes such marking, a lanyard and tag system will be permanently attached to the device, and all required markings would be placed thereon.

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 division, branch, or General or Special Staff Department SCP as required by chapter 8 of this Order.

10. Clearing and Purging of CMI from Media and Devices. Detailed instructions for clearing and purging devices and media are contained in reference (s).

a. All candidate media and devices for purging will be turned over to the CMCC for accounting, control, and coordination with the ISSM 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 12 of this Order.

APR 12 2019

Chapter 12

CMI Destruction

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

a. CMI record material may be destroyed only when destruction is the disposition authorized by the current edition of reference (c). 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.

c. MCIEAST-MCB CAMLEJ policy requires unclassified messages and all unclassified controlled information as defined by reference (e), 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 reference (n), 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 COMSEC materials is outside the scope of this Directive and will be accomplished by designated personnel only, in accordance with the current directives governing this program.

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.

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.

APR 12 2019

(3) When authorized by the TSCO, Top Secret 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 Top Secret and accountable "finished product" Secret CMI (does not include Secret "working papers" or Secret messages). Destruction records for Top Secret CMI will be retained for five years; for Secret CMI, two years.

3. Media Destructive 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 <https://www.nsa.gov/resources/everyone/media-destruction> 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 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 1-800-688-6115, and select option 3 to request a faxed copy of the EPL for the particular media.

c. For those MCIEAST subordinate commands temporarily lacking facilities or funding for destruction equipment, or when infrequent need for destruction doesn't justify investment in destruction devices, off-site facilities are available to assist. All CMI, including classified HDDs, to be transferred to an off-site facility will be handled in accordance with the guidance contained in chapter 9 of the current edition of reference (b).

(1) The NSA provides destruction services for all types of media containing CMI and CUI as defined by reference (e). This is particularly helpful when the requirement to destroy non-standard media cannot be met at the tenant command's location.

(2) The NSA's Classified Material Conversion (CMC) facility customer service number is (301) 688-6672, DSN 644-6672. They can fax the required forms, receipts, and mailing instructions upon request.

(3) HDD destruction will be accomplished by degaussing and shredding. When a computer/HDD has reached end-of-life and is designated to be permanently removed from service, the Responsible Officer will remove the hard drive from the chassis and turn it into their SCP who will then turn it into the CMCC. Due to the volume of the materials in the G-6 SCP, the G-6 SCP is authorized to perform their own destruction of classified hard drives, and then turn the destruction report (OPNAV 5510/11) into the CMCC. Once the hard drive is removed from the computer, the secret classification labels and the buck-tag can be removed from the chassis.

(4) Other media that may be destroyed at NSA's CMC is aluminum disks, computer chips, film, floppy disks, magnetic cards, micro circuit units, microfiche, mylar, paper, printed circuit boards, slides, typewriter, ribbons,

APR 12 2019

cartridges, viewgraphs, CDs, diskettes, loose tape, optical tape, reel-to-reel tapes, tape cartridges, and VCR tapes.

4. Emergency Destruction

a. The priorities for emergency destruction are as follows:

- (1) Priority One - Top Secret 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 MCIEAST-MCB CAMLEJ Command Security Manager by SIPRNET e-mail or secure telephone. The MCIEAST-MCB CAMLEJ Command Security Manager will notify CNO (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; and

(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 MCIEAST-MCB CAMLEJ 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; and
- (c) Identify the circumstances under which the emergency destruction was implemented.

APR 12 2019

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 Contracting Officer's Representative (COR) will ensure 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 the control of tenant commands 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. Contracting Officer's Representative (COR). The Command's Contracting Officer shall designate, in writing, the COR when a classified or operationally sensitive contract is proposed, for the purpose of preparing the DD-254, and revisions thereto. The Command Security Manager will sign the DD-254 as the Contracting Officer's Security Representative (COSR).

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 11 of the current edition of reference (b) are accomplished when classified information is provided to industry for performance of a classified contract.

4. Visits by Cleared DoD Contractor Employees. 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 11 of the current edition of reference (b).

a. Per the Under Secretary of Defense, JPAS is the personnel security system of record throughout the DoD, and shall be used to verify the personnel security

APR 12 2019

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 subordinate command's Security Management Office (SMO) number.

b. The Command Security Manager will validate the visitor's access requirement with the division, branch, or General or Special Staff Department 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 NTK 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. Contractor Badges. All contractors, cleared, and those without clearances, working within controlled spaces will wear a security badge. The badges will identify level of access, duration of access, and personal information. Badges will be issued when the prerequisites of paragraph 4 above have been met, and will be returned upon completion of the contract, or upon the contractor's termination of their employee.

6. Facility Access Determination (FAD). Contract 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 reference (b) to request investigations on these persons and to protect persons and property under their command against the actions of untrustworthy persons.

b. Should the Commander exercise this authority, the Regional Contracting Officer will include the FAD program requirements in the contract specifications.

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

d. Alternatively, the Federal Bureau of Investigation 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/station PMO.

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

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

APR 12 2019

Chapter 14

Personnel Security Policy

1. Policy. The Command Security Manager is responsible for administering the IPSP. The Command Security Manager is the Staff Officer for the IPSP, and advises the Commander concerning personnel security matters relative to subordinate elements.

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.

3. Commanders. Every Commander/CO must have a favorably adjudicated SSBI investigation, and a security clearance equivalent to the highest level of CMI maintained at the command.

4. Designation of Civilian Sensitive Positions

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

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

(1) The applicants for employment in a DoD Civilian National Security Position must be able to meet position sensitivity investigation and adjudication requirements. All civilian employees, at a minimum, must have a favorably adjudicated National Agency Check with Inquiries (NACI).

(2) The incumbent in a DoD Civilian National Security Position must be able to maintain the clearance eligibility for the corresponding position sensitivity. Loss of eligibility must be reported to the command's civilian personnel office.

(3) 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.

c. The determination of eligibility to occupy a sensitive position is made by the DODCAF based on the appropriate investigation. The same criteria is applied to both security clearances and sensitive position eligibility

APR 12 2019

determinations. A determination by the DODCAF 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.

APR 12 2019

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 the current version 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.
 - c. Conduct a Local Records Check of all available personnel, medical, legal, security, base/station military police, and other command records to determine if disqualifying information exists.
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/her assistant, acting on behalf of the Commander/CO, are the only officials authorized to request PSIs on individuals within their command.
 - c. The Command Security Manager will ensure that all Marines in the command have been the subject of a National Agency Check, Local Agency Check plus Credit (NACLIC) or Tier 3 investigation.
 - d. 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 1 year service remaining. Exceptions will be granted only for those personnel whose participation in a Special Access Program (SAP) is documented with appropriate orders, and whose assignment is contingent upon completion of the required PR.
 - e. The scope of the PSI requested from OPM will be commensurate with the level of sensitivity of the access required, or position occupied. Only the

APR 12 2019

minimum investigation to satisfy a requirement will be requested. The various types of investigations are described in chapter 6 of the current edition of reference (a).

4. JPAS. The JPAS located at <https://jpasapp.dmdc.osd.mil/JPAS/JPASDisclosure> provides accurate, updated investigation information on personnel from all branches of the service, DoD civilians, and DoD contractors.

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 the Electronic Questionnaires for Investigations Processing (e-QIP) System 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-PRs, will require submission of fingerprints.

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 4-character identifier provided by OPM-FIPC. Each command requesting investigations must have a SON; call the Federal Investigative Processing Center (FIPC) Program Services Office (PSO) at (724) 794-5612, to verify.

(2) To update the SON address or points of contact, submit a "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 60 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. A copy of an individual's completed SF-86, maintained in the Personnel Security File, is not required for retention after the OPM receipt is received. 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.

APR 12 2019

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 divulge the 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 Coordinator 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 Marine's SRB or Official Military Personnel File.

c. The Personnel Security Folder should also be the repository for current clearance, access letters, and endorsements, copies of SF-312s (when submitted from the command), 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.

APR 12 2019

Chapter 16

Personnel Security Access Determinations1. Policy

a. The standard which must be met for security clearance eligibility or assignment to sensitive duties is 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 the current edition of reference (a)).

2. Department of Defense Consolidated Adjudications Facility (DODCAF). The DODCAF will assign clearance eligibility at the highest level supportable by the investigation completed by OPM. DODCAF posts clearance eligibility information directly to JPAS.

3. JPAS

a. JPAS located at <https://jpasapp.dmdc.osd.mil/JPAS/>. JPAS Disclosure 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, or contact the Command Security Manager.

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

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

4. Eligibility Determination

a. The DODCAF 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 DODCAF will communicate the results to the requesting command via JPAS, or in the case of unfavorable determinations, in writing.

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

(2) DODCAF 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.

APR 12 2019

(3) DODCAF 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 DODCAF 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 DODCAF on issues of importance relating to access.

(1) The Command Security Manager must initiate a local records check per chapter 15, paragraph 2 of this Order prior to granting initial command access, reporting any negative findings to DODCAF 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 10 and Appendix G of the most current edition 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 DODCAF in conjunction with the "Incident Report" via JPAS. Chapter 9 of the current version 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); and

(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 7 of the current edition of reference (a).

6. Validity and Reciprocal Acceptance of Personnel Security Determinations

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, or adjusted, or it has been suspended for cause.

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

APR 12 2019

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 chapter 3, paragraph 5 of this Order before granting access to CMI.

2. Requests 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 15 of this Order.

b. The Marine Corps Total Force System is specifically prohibited from making security access determinations, as is the 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 DODCAF. At no time will access be granted based upon the desires of the individual requesting access.

3. Classified Information Non-Disclosure Agreement (SF-312). The SF-312 is a nondisclosure agreement between the United States 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.

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

(2) 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 United States 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.

APR 12 2019

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

b. Reporting the Non-Disclosure Agreement

(1) 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 50 years following its date of execution. Forward the executed, witnessed, and accepted original SF-312 to HQMC (MMSB-20) at the following address:

COMMANDANT OF THE MARINE CORPS
HEADQUARTERS U. S. MARINE CORPS
(MMSB-20)
2008 ELLIOT ROAD
QUANTICO VA 22134-5030

(2) A copy of the SF-312 should be maintained in the individual's personnel security folder maintained at the command where it was executed.

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

4. Verbal Attestation

a. The Deputy SecDef 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/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 National Security Information. I am aware of my obligation to protect classified National Security Information 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 United States 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, SCI Nondisclosure agreement is signed. 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. Interim Security Clearance Request (Access). 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 DODCAF. Interim clearances may be granted by the Commander/CO under the following conditions:

APR 12 2019

a. Interim Top Secret Security Clearance

(1) Either Secret or Confidential security clearance eligibility exists, or a favorable NACLC, ANACI, or Tier 3 investigation (other investigation types may be allowed, refer to the current edition of reference (a)) has been completed within the past 10 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 (10 year scope); and

(4) The T5 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 (10 year scope); and

(3) The appropriate T3 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 DODCAF 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 9 of the current edition of reference (a).

e. Subordinate commands should refer to chapters 6 and 8 of the current edition of reference (a) 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 or permanent change of assignment, or a civilian transfers within the DON, local termination of access, and a debriefing per chapter 3, paragraph 7 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 (OPNAV 5511/14 Rev 9-05) are required per chapter 3, paragraph 7 of this Order.

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

(2) A "Debriefing" 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 for inclusion in the individual's ESR or Civilian Official Personnel File prior to that record's close-out and transfer to a records retention facility.

APR 12 2019

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 DODCAF'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 9 of the current edition of reference (a). All local suspensions will be reported to DODCAF via JPAS with an "Incident Report."

APR 12 2019

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 tenant command's area of responsibility.

d. General visitation by the public will only be allowed on an unclassified basis: no classified areas or information will be shown or divulged. General visitation 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 subordinate 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 National Industrial Security Program (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 Program. It is essential that visit requests be coordinated so that the interests of the U.S. Government and the USMC are adequately served; these

APR 12 2019

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 tenant 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 MCIEAST subordinate commands, will be routed through Headquarters MCIEAST-MCB CAMLEJ. 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 MCIEAST-MCB CAMLEJ. Approved FVRs will detail the level of disclosure authorized for the specified visit.

c. Extended FVRs (FLOs and MCFPEPs) will be supported from HQMC with a Delegated Disclosure Letter (DDL), forwarded to the subordinate command via Headquarters MCIEAST-MCB CAMLEJ, detailing the level of disclosure authorized. Subordinate and some tenant 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.

(1) The original Contact Officer assignment letter should be sent to the Commandant of the Marine Corps (PP&O/PS), via the Commanding General, Marine Corps Installations East-Marine Corps Base, Camp Lejeune (Attn: Security Manager).

(2) Subordinate MCIEAST commands will forward copies of the Foreign Officer Statement of Understanding letters to the MCIEAST-MCB CAMLEJ Command Security Manager.

d. The current edition of references (v) and (w) provides detailed information for Foreign Disclosure Officers (FDO) and Foreign Disclosure Points of Contact (FDPOC), and should be reviewed by Command Security Managers whose commands host foreign visitors.

APR 12 2019

APPENDIX A

GUIDELINES FOR COMMAND SECURITY INSTRUCTION

1. 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. 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.

PART I - Command Security Program Elements

1. Identify purpose, applicability, and relationship to other directives, particularly references (a) and (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, and 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.

PART II - Information Security Program Elements

1. Specify command responsibilities and controls on any special types of classified and controlled unclassified information.
2. 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.
3. 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.
4. Establish reproduction controls to include compliance with reproduction limitations and any special controls placed on information by originators.

APR 12 2019

5. Establish command destruction procedures. Identify destruction facilities or equipment available. Attach a command EAP as a supplement.
6. Develop an Industrial Security program and identify key personnel, such as the COR, if applicable.
7. 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; AIS processing equipment; and residential storage arrangements.

PART III - Personnel Security Program Elements

1. Explain each step of the command's internal administrative procedures leading to access of classified information, or assignment to sensitive duties for command personnel, as well as procedures for safeguarding and maintaining classified information. The text will:
 - 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 the continuous evaluation program. Establish procedures for reporting derogatory information to the DODCAF.
 - 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, foreign liaison officers, and foreign students, and caution command personnel regarding their responsibilities.
 - c. Include in this section a list of areas within the command authorized for general visitation, and clearly identify all areas that are off limits to visitors.

APR 12 2019

APPENDIX B

PROTECTED DISTRIBUTION SYSTEM (PDS) USER QUICK REFERENCE

- Before the PDS box is opened for use:
 - If windows are present, window coverings must be used. Windows must be closed and locked.
 - All office doors must be secured with the UL437 deadbolt lock engaged.
 - All glass panes in doors must be properly covered or made opaque.
 - All un-cleared personnel or personnel without a need to know must exit the workspace.
- All classified material including magnetic media, removable secondary storage media, and removable hard drives will be stored in GSA approved security containers or secure rooms at the end of the day or when the office is unoccupied, even for short periods of time. The cable will be stored in the PDS box when not in use.
- Ensure that office doors are secured at the end of the workday. During working hours the area shall be: 1) occupied; 2) access controlled through use of a cipher or simplex lock, a swipe badge system; or, 3) locked when unoccupied. The workspace must be locked when unoccupied, even if the PDS box is properly secured.
- PEDs must be turned off and secured outside of the office space when the PDS box is open and in use.
- Daily PDS inspection procedures shall be conducted as set forth by the Command Security Manager. At a minimum, users are responsible for identifying and reporting to the Command Security Manager any evidence of tampering, penetration, or any other anomaly causing a deterioration of protection safeguards.

*** Completion of an SF702 form upon opening and closing the PDS box and access rosters for office spaces with PDS boxes are not required unless specifically directed by the Command Security Manager. Please adhere to guidelines set forth by your local Command Security Manager. ***

APR 12 2019

APPENDIX C

CLASSIFIED MATERIAL CONTROL CENTER (CMCC)

1. The term CMCC is not defined in other policy documents though it is typically understood to mean a location through which a command controls classified documents and material. It may be as elaborate as a vault with multiple security specialists to a two drawer GSA approved security container in a corner of an office. Regardless of the size or scope of a command's classified holdings, the term CMCC describes the place from which classified holdings are centrally controlled.

2. The CMCC should be managed by the Command Security Manager. There are no restrictions on "ownership" of the CMCC and there is no conflict of interest in having the Command Security Manager in charge of the CMCC. In fact, there are many positive aspects associated with having the subject matter expert charged with the management of the command's classified holdings.

3. This appendix provides an example of how to establish and manage a CMCC. This is not directive in nature but provides a place to start. The CMCC is effective if it can identify all items of classified material within the command, where it is located and when it is destroyed.

4. Control of secret documents need not be complicated. A simple logbook or spreadsheet with locally generated control numbers for the documents is sufficient. The following is an example of how this might be achieved.

a. Document Control Number. The document control number may be any number that uniquely identifies the document within the command. The example below consists of the unit Reporting Unit Code (RUC), Julian Date and Document Number to read as follows:

Command's RUC	31002
Julian Date Created or entered command	9236
Container Number Letter or Number	(A or 3)
Document Number 01	
Example final number would read:	54008-9236-A-01

The Julian Date is recommended as a simplified manner to enter the date. Rather than attempting to use, 090824 or 24Aug09, the four digit Julian Date is constructed such that the Julian day as shown in Tables T-1 and T-2. Of course, it requires the maintenance of a Julian Date calendar to decipher the number. As stated earlier, this is merely an example.

b. Document Control Spreadsheet. The spreadsheet below is simply an example of how this might be done. Separate spreadsheets can be placed in each container to allow the person logging it into the command to complete the log. Periodically, the spreadsheet could be entered into a computer based database to reduce the need for maintenance of paper logs.

APR 12 2019

APPENDIX D

IPSP EMERGENCY ACTION PLAN (EAP)

NATURAL DISASTERS. Natural disasters include fires, floods, hurricanes, and any phenomena that would result in the inadvertent loss, compromise, or destruction of classified material. When such a situation occurs, the senior Marine or Civilian Employee present will execute the EAP.

1. Fire after duty hours: Should a fire occur around or within Building 1, or any Secondary Control Point (SCP), the Command Security Manager/CMCC Custodian/SCP Custodian will:

a. Notify the Fire Department and Military Police by dialing "911" and report the location and extent of the fire.

b. If the fire occurs during duty hours, secure all classified material in a GSA approved container, vault, or secure room designated as Open Storage Secret (OSS).

c. If the fire occurs after duty hours, ensure the CMCC Vault door, GSA approved container, or SCP is secured before leaving the area.

d. If safe, use all local means to extinguish or control the fire until the fire department arrives. Fire extinguishers are located throughout the building and basement.

e. If after duty hours, and as soon as possible, notify the Command Security Manager, Assistant Security Manager, CMCC Custodian, and/or SCP Custodian.

f. Under no circumstances will anyone subject themselves or their subordinates to possible death or injury to protect classified material from fire.

g. When the Fire Department/Military Police arrive, they will immediately be informed of and admitted to the secure areas. Efforts will be made to get names and identification numbers of all emergency personnel going into secure areas or being exposed to classified material only after the emergency is over.

h. The Security Manager/Assistant, CMCC Custodian, or SCP Custodian will, to the maximum extent possible, ensure that only emergency personnel are allowed into secure areas. When given the "ALL CLEAR" signal from emergency personnel, the vault will be locked or two guards must be placed in the secure area until the Command Security Manager/CMCC Custodian conduct a post-emergency inventory.

i. If the intensity of the fire is such that the area must be abandoned, maintain a surveillance of the general area to prevent unauthorized persons from entering, to the best of your ability.

APR 12 2019

2. Hurricanes, Floods, and other Natural Phenomena. The danger presented by these conditions are not likely to be as sudden as that presented by fire. The primary objective in case of hurricane, flood, etc., is to secure and waterproof classified material and computers to protect them from wind, water, or destruction until the emergency has passed.

a. Prior to Hurricanes (DWC-1C), the Command Security Manager, Security Assistant, CMCC Custodian, and/or SCP Custodian will waterproof all classified material and gear in GSA approved containers or approved OSS areas. All classified computers will be unplugged and waterproofed with plastic as necessary. All other logs, documents, and other important papers, etc., will also be safeguarded accordingly.

b. If there is damage to the CMCC Vault, SCP, or OSS designated area from a hurricane, flood, or other phenomena, the Command Duty Officer (CDO), or other person on the scene, will immediately contact the Command Security Manager, Assistant Security Manager, CMCC Custodian, and/or SCP Custodian and inform them of the extent of damage.

c. Two persons will be posted, if necessary, as a guard force to prevent unauthorized access to classified material until CMCC personnel arrive.

d. The CMCC will coordinate the removal of classified material, if required, to a location pre-determined by the Command Security Manager, that has the ability to safeguard the classified material at the respective level.

e. All SCPs will coordinate the removal of classified material, if required, to the CMCC (primary), or a location pre-determined by the Command Security Manager, that has the ability to safeguard the classified material at the respective level.

3. Loss of Power resulting from a Natural Disaster

a. Per SECNAV M-5510.36, Restricted Areas designated as OSS are required to safeguard SECRET material by one of the following methods:

(1) In the same manner prescribed for Top Secret;

(2) In a GSA approved security container, modular vault, or vault without supplemental controls;

(3) In a non-GSA-approved container having a built-in combination lock. One of the following supplemental controls are required:

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

APR 12 2019

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

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

b. In the event of IDS failure as a result of power loss, the Security Manager, Assistant Security Manager, CMCC Custodian, and/or SCP Custodian will coordinate one of the protection measures to ensure the continuous protection of classified material.

HOSTILE ACTIONS. Hostile Actions include, bomb threats, riots, or civil uprisings. In all cases, the assumption will be made that classified material is a target. All actions must be directed to prevent unauthorized personnel from gaining access to classified material by securing, or evacuating the material as conditions dictate. There are three threat stages of hostile action emergencies. These stages will be carried out by CMCC personnel only.

1. Stage One - (Potential Threat)

- a. Threat source - Operations in high risk environment.
- b. Time frame - Several days to several months.
- c. Action - Precautionary Emergency Protection as outlined under Terrorist Actions below.

2. Stage Two - (Probable Threat)

- a. Threat source - Probability of hostile attack.
- b. Time frame - From one to several days.
- c. Action - Possible Emergency Evacuation as outlined under Emergency Evacuations below.

3. Stage Three - (Imminent Threat)

- a. Threat source - Attack by hostile forces.
- b. Time frame - Imminent.
- c. Action - Immediate Emergency Protection or Evacuation as outlined under Terrorist Actions and Emergency Evacuations below.

4. Bomb Threat. In the event of a bomb threat, the Provost Marshal's Office (PMO) will be notified by dialing "9-1-1". Classified material will be secured in the CMCC vault or SCP. The vault will be locked and all classified material accounting records will be removed from the building. Personnel will wait outside the building at a safe distance

APR 12 2019

until the arrival of the military police and EOD Team. The building will not be re-entered until the "ALL CLEAR" signal is given by EOD personnel.

TERRORIST ACTIONS. Acts of terrorism range from threats of terrorism, assassinations, kidnappings, hijackings, bomb scares and bombings, cyber-attacks (computer-based), to the use of chemical, biological, and nuclear weapons. All actions must be directed to prevent unauthorized personnel from gaining access to classified material by securing, or evacuating the material as conditions dictate. There are five threat stages of terrorist action. These stages will be carried out by CMCC personnel only.

1. Low Condition - Green; low risk of terrorist attacks. The following Protective Measures may be applied:

- a. Refining and exercising preplanned Protective Measures;
- b. Ensuring personnel receive training on departmental, or agency specific Protective Measures; and
- c. Regularly assessing facilities for vulnerabilities and taking measures to reduce them.

2. Guarded Condition - Blue; general risk of terrorist attack. In addition to the previously outlined Protective Measures, the following may be applied:

- a. Checking communications with designated emergency response or command locations;
- b. Reviewing and updating emergency response procedures; and
- c. Providing the public with necessary information.

3. Elevated Condition - Yellow; significant risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- a. Increasing surveillance of critical locations;
- b. Coordinating emergency plans with nearby jurisdictions;
- c. Assessing further refinement of Protective Measures within the context of current threat information; and
- d. Implementing, as appropriate, contingency and emergency response plans.

4. High Condition - Orange; high risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

APR 12 2019

a. Coordinating necessary security efforts with armed forces or law enforcement personnel;

b. Taking additional precaution at public events;

c. Preparing to work at an alternate site or with a dispersed workforce;

d. Restricting access to essential personnel only.

5. Severe Condition - RED; severe risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

a. Assigning emergency response personnel and pre-positioning specially trained teams;

b. Monitoring, redirecting or constraining transportation systems;

c. Closing public and government facilities; and

d. Increasing or redirecting personnel to address critical emergency needs.

EMERGENCY EVACUATION. Emergency evacuation is that action taken to move classified material to a safe place to prevent unauthorized access caused by fire, hurricane, flood, other natural phenomena, hostile action, or terrorist action.

1. Emergency evacuation will only be executed when directed by the Base Commander or Command Security Manager. The Primary Classified Storage area will be the CMCC Vault located in Building 1. During non-working hours and when directed, the Command Duty Officer (CDO) will:

a. Attempt to contact CMCC personnel and the Command Security Manager using the Emergency Recall Roster (located in the CDO Binder) or the CMCC Access Roster (located on the outside of the CMCC door). If CMCC personnel cannot be contacted, the CDO will obtain the combination cards (SF-700) for the CMCC and Vault door from the Emergency Operations Center (EOC), Rm E100, located at Building 1, and will carry out the Evacuation Plan accordingly until they can be reached.

b. The Command Security Manager or Security Assistant must appoint at least two persons to evacuate the classified material, and contact Military Police to provide armed escort for the evacuation.

c. Ensure a Government Vehicle with driver is readily available for pick-up and delivery of classified material during evacuation.

APR 12 2019

d. Post a Military Policeman armed guard at the vault entrance and vehicle until all classified material is loaded onto the Government Vehicle.

e. After all classified material has been gathered and packed, the armed guards will escort and protect the total evacuation of all classified material to include unloading and safeguarding it at the new location.

EMERGENCY PROTECTION. Emergency protection actions include collecting all classified materials not needed for immediate operational use, and securing them in the CMCC Vault or a GSA approved container.

1. Emergency protection procedures will only be executed when directed by the Base Commander, Command Security Manager, or other competent authority.

a. All classified material will be locked up in a GSA approved container, vault, or OSS.

b. All other publications, logs, and correspondence will be packed and prepared for evacuation.

2. Any other protection actions deemed necessary by the Security Manager will also be completed during this time.

EMERGENCY DESTRUCTION. Emergency destruction of classified material may be required due to fire, natural disaster, civil disturbance, terrorist activities, or enemy action. These action may lead to the loss or compromise of classified information, to which emergency destruction is required to minimize the risk of unauthorized disclosure through the recovery of classified information, if necessary, following such events.

1. Emergency destruction will only be executed by the CO, Command Security Manager, Assistant Security Manager, CMCC Custodian, SCP Custodian, classified material originator, and/or personnel identified by the CO or Command Security Manager.

2. Paper-based classified material shall be destroyed utilizing one of the following methods:

- a. Crosscut shredding
- b. Burning
- c. Wet pulping
- d. Chemical decomposition
- e. Pulverizing/disintegrating

APR 12 2019

3. Classified IT equipment and electronic medial shall be destroyed utilizing one of the following methods:

- a. Overwriting;
- b. Degaussing;
- c. Sanding, or
- d. Physical destruction (mutilation).

4. The priority for the destruction of classified material shall be organized by the level of protection against unauthorized disclosure in the interest of national security.

a. The unauthorized disclosure of TOP SECRET material could reasonably be expected to cause exceptionally grave damage to national security and should be destroyed first.

b. The unauthorized disclosure of SECRET material could reasonably be expected to cause serious damage to national security and should be destroyed after all TOP SECRET material has been destroyed. If the command does not possess any TOP SECRET material, SECRET material should be destroyed first.

c. The unauthorized disclosure of CONFIDENTIAL material could reasonably be expected to cause damage to national security and should be destroyed after all TOP SECRET and SECRET material has been destroyed. If the command does not possess any TOP SECRET or SECRET material, CONFIDENTIAL material should be destroyed first.

d. Controlled Unclassified Information (CUI) may be destroyed by any means approved for the destruction of classified information. Destroy paper CUI using cross cut shredders that produce particles that are 1mm by 5mm. Destruction of CUI in the form of electronic media can be performed by clearing, purging, or physical destruction.

e. Foreign Government Information (FGI) shall be destroyed in the same manner as U.S. classified information of the equivalent level, except where otherwise required by international treaty or agreement.

5. Contact the National Security Agency/Central Security Service (NSA/CSS) System and Network Analysis Center at (410)854-6348 or via e-mail at SNAC@radium.ncsc.mil, to obtain technical guidance concerning appropriate methods, equipment, and standards for destroying classified electronic media, IT equipment, electronic components, and other similar or associate materials.

APR 12 2019

SAMPLE DOCUMENT INVENTORY SHEET

Subject	Document Date	Classification	Document Control Number	Disposition	Name/Signature of person taking action
Widgets required for MEU Deployment	18 May 09	SECRET	54008-9236-A-01	Destroyed 9249	Butler, S.
OPORD 3-08	4 Mar 08	SECRET	34708-8064-B-03	Transferred to HQMC	Lejeune, J.
Hard Drive		SECRET		54008-7245-A-06	

Maintaining one spreadsheet per security container allows subsequent document numbers to simply continue with the next number. Documents in different containers are differentiated by separate container numbers. Commands with the same RUC but many different staff agencies with multiple SCPs can simply use a separate command identifier. For example, HQMC can use the commonly known Department, Division, and Branch identifiers. A document controlled by Security Division of Plans, Policies and Operations, controlled on 24 August 2009, in container A, document number 01 would appear like, PS-9236-A-01.

APR 1 2 2019

TABLE-1
JULIAN DATE CALENDAR
(PERPETUAL-NON LEAP YEARS)

DAY	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	DAY
1	001	032	060	091	121	152	182	213	244	274	305	335	1
2	002	033	061	092	122	153	183	214	245	275	306	336	2
3	003	034	062	093	123	154	184	215	246	276	307	337	3
4	004	035	063	094	124	155	185	216	247	277	308	338	4
5	005	036	064	095	125	156	186	217	248	278	309	339	5
6	006	037	065	096	126	157	187	218	249	279	310	340	6
7	007	038	066	097	127	158	188	219	250	280	311	341	7
8	008	039	067	098	128	159	189	220	251	281	312	342	8
9	009	040	068	099	129	160	190	221	252	282	313	343	9
10	010	041	069	100	130	161	191	222	253	283	314	344	10
11	011	042	070	101	131	162	192	223	254	284	315	345	11
12	012	043	071	102	132	163	193	224	255	285	316	346	12
13	013	044	072	103	133	164	194	225	256	286	317	347	13
14	014	045	073	104	134	165	195	226	257	287	318	348	14
15	015	046	074	105	135	166	196	227	258	288	319	349	15
16	016	047	075	106	136	167	197	228	259	289	320	350	16
17	017	048	076	107	137	168	198	229	260	290	321	351	17
18	018	049	077	108	138	169	199	230	261	291	322	352	18
19	019	050	078	109	139	170	200	231	262	292	323	353	19
20	020	051	079	110	140	171	201	232	263	293	324	354	20
21	021	052	080	111	141	172	202	233	264	294	325	355	21
22	022	053	081	112	142	173	203	234	265	295	326	356	22
23	023	054	082	113	143	174	204	235	266	296	327	357	23
24	024	055	083	114	144	175	205	236	267	297	328	358	24
25	025	056	084	115	145	176	206	237	268	298	329	359	25
26	026	057	085	116	146	177	207	238	269	299	330	360	26
27	027	058	086	117	147	178	208	239	270	300	331	361	27
28	028	059	087	118	148	179	209	240	271	301	332	362	28
29	029		088	119	149	180	210	241	272	302	333	363	29
30	030		089	120	150	181	211	242	273	303	334	364	30
31	031		090		151		212	243		304		365	31

APR 12 2019

TABLE-2
JULIAN DATE CALENDAR
(FOR LEAP YEARS ONLY)

DAY	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	DAY
1	001	032	061	092	122	153	183	214	245	275	306	336	1
2	002	033	062	093	123	154	184	215	246	276	307	337	2
3	003	034	063	094	124	155	185	216	247	277	308	338	3
4	004	035	064	095	125	156	186	217	248	278	309	339	4
5	005	036	065	096	126	157	187	218	249	279	310	340	5
6	006	037	066	097	127	158	188	219	250	280	311	341	6
7	007	038	067	098	128	159	189	220	251	281	312	342	7
8	008	039	068	099	129	160	190	221	252	282	313	343	8
9	009	040	069	100	130	161	191	222	253	283	314	344	9
10	010	041	070	101	131	162	192	223	254	284	315	345	10
11	011	042	071	102	132	163	193	224	255	285	316	346	11
12	012	043	072	103	133	164	194	225	256	286	317	347	12
13	013	044	073	104	134	165	195	226	257	287	318	348	13
14	014	045	074	105	135	166	196	227	258	288	319	349	14
15	015	046	075	106	136	167	197	228	259	289	320	350	15
16	016	047	076	107	137	168	198	229	260	290	321	351	16
17	017	048	077	108	138	169	199	230	261	291	322	352	17
18	018	049	078	109	139	170	200	231	262	292	323	353	18
19	019	050	079	110	140	171	201	232	263	293	324	354	19
20	020	051	080	111	141	172	202	233	264	294	325	355	20
21	021	052	081	112	142	173	203	234	265	295	326	356	21
22	022	053	082	113	143	174	204	235	266	296	327	357	22
23	023	054	083	114	144	175	205	236	267	297	328	358	23
24	024	055	084	115	145	176	206	237	268	298	329	359	24
25	025	056	085	116	146	177	207	238	269	299	330	360	25
26	026	057	086	117	147	178	208	239	270	300	331	361	26
27	027	058	087	118	148	179	209	240	271	301	332	362	27
28	028	059	088	119	149	180	210	241	272	302	333	363	28
29	029	060	089	120	150	181	211	242	273	303	334	364	29
30	030		090	121	151	182	212	243	274	304	335	365	30
31	031		091		152		213	244		305		366	31

(USE IN 2004, 2008, 2012, 2016, ETC)