UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
BEAUFORT, SOUTH CAROLINA 29904-5001

IN REPLY REFER TO:
ASO 5510.11K
CMCC
OCT 05 2020

AIR STATION ORDER 5510.11K

From: Commanding Officer, Marine Corps Air Station Beaufort
To: Distribution List

Subj: INFORMATION PERSONNEL AND INDUSTRIAL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.30C
(b) SECNAVINST 5510.36B
(c) MCO 5510.18B
(d) DoDD 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations", June 16, 1992
(e) DoDM 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)", February 24, 2012
(f) DoD 5220.22-M, "National Industrial Security Program Operating Manual(NISPOM)", February 28, 2006
(g) DoDD 5210.2, "Access to and Dissemination of Restricted Data and Formerly Restricted Data", June 3, 2011
(h) MCO 3751.2
(i) SECNAVINST 5720.42
(j) MCO P5530.14
(k) OPNAVINST 5513.1E, DON Security Classification Guides
(l) E.O. 12958, as amended, and E.O. 13292, further amendment to E.O. 12958, Classified National Security Information
(m) Atomic Energy Act of 1954, as amended
(n) Computer Security Act of 1987
(o) DoDM 5200.01, "Volume 2, Marking of Classified Information", February 24, 2012
(p) EKMS-1 Series, Naval Electronic Key Management System
(q) DoDD 5230.9, "Clearance of DoD Information for Public Release", April 9, 1996
(r) DoDI 5230.29, "Security and Policy Review of DoD Information for Public Release", January 8, 2009
(s) DoN Information Assurance Publication 5239-26, May 2000, Remanence Security Guidebook
(t) SECNAV M-5210.1, Department of the Navy Records Management Program Records Management Manual
(u) Internal Security Act of 1950
(v) MCO 5510.20B
(w) MCIEAST-MCB CAMLEJO 5510.3
(x) DoDM 52000.01, Volume 1, "DoD Information Security Program: Overview, Classification and Declassification"

Encl: (1) Information Security Program Procedural Guidance

1. Situation. To promulgate policies and procedures for the effective management, operation, and maintenance of the Marine Corps Air Station (MCAS)

Beaufort Information and Personnel Security Program (IPSP) pursuant to the guidelines established in the references.

2. Cancellation. ASO 5510.11J.

3. Mission. This Order implements local command policy and guidance for the station security manager, station classified material control center, secondary control points (SCPs), and personnel granted access to sensitive material by providing a uniform method for maintenance and control of classified material and the management of an effective IPSP.

4. Execution

a. Department/Division Heads and SCPs shall review and, to the greatest extent applicable, follow the guidance contained in this Order.

b. Recommended changes to this Order are invited and shall be submitted to the Commanding Officer (CO), (Attn: Security Manager) via the appropriate chain of command.

5. Administration and Logistics. Individuals who handle classified material and/or information are responsible for compliance with this Order.

6. Command and Signal

a. Command. This Order is applicable to all personnel aboard MCAS Beaufort.

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

K. R. ARBOGAST

DISTRIBUTION: A

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

Chapter 1

Basic Policy and Applicability

1. Basic Policy. The directives which provide basic guidance for the security of classified information and material are the current editions of references a, b, c, e, o, and x.

a. This Order identifies procedures for classification, safeguarding, transmission, and destruction of CMI, as well as regulations and guidance for the IPSP. The term "CMI" is information originated by or for the DoD, its agencies or is under their jurisdiction, control and that requires protection in the interests of national security. It is designated TS, secret, and confidential as described in E.O. 12356. CMI may be in oral, visual, or material form and has been subdivided further into eight categories per reference (y).

b. This Order implements the IPSP for MCAS Beaufort and is in compliance with the references to promote an effective Command Security Program.

2. Responsibilities. The CO is ultimately responsible for the safeguarding of classified information within the command and for the proper instruction of command personnel in security procedures and practices.

a. Security Manager. The Security Manager is appointed in writing by the CO and is the principal advisor on information, personnel, and industrial security within the Command and must be cognizant of command security functions to ensure the security program has all the necessary requirements to be successful. The Security Manager shall:

(1) Ensure that those in the Command who have security duties are kept abreast of changes in policies and procedures and must provide assistance in resolving security issues.

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

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

(4) Develop a written command IPSP, including an Emergency Action Plan (EAP), which integrates emergency destruction plans where required.

(5) Formulate and coordinate the Command's security awareness and education program.

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

(7) Ensure coordination of staffing foreign visit requests received from the Headquarters 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).

(8) Ensure all personnel who will handle CMI or will be assigned to sensitive duties are appropriately cleared through coordination with the

DoDCAF, and that requests for personnel security investigations are properly prepared, submitted, and monitored.

(9) Ensure access to CMI is limited to those who are eligible and have a demonstrated need-to-know (NTK).

(10) Ensure personnel security investigations, clearances, and accesses are properly recorded with documentation in the personnel security file and JPAS.

(11) Coordinate the command program for continuous evaluation of eligibility for access to CMI or assignment to sensitive duties.

(12) Coordinate with the Command Cyber Security Manager on matters of common concern.

(13) Ensure all personnel execute a Standard Form (SF) 312 prior to granting initial access to CMI, with documentation recorded at HQMC and in JPAS.

(14) Ensure all personnel granted access to the Secret Internet Protocol Router Network (SIPRNET) receive a North Atlantic Treaty Organization (NATO) SECRET security brief and debriefing, with documentation recorded in JPAS.

(15) Ensure all personnel requiring access to CMI (Confidential, Secret, or TS) provide a verbal attestation of their responsibilities to protect that material with documentation recorded in JPAS.

(16) 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 recorded in their personnel security file and JPAS.

(17) 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 for more than 60 days, retiring, reaching the end of their contract, etc.), receive a command debrief with documentation recorded in their personnel security file and JPAS.

(18) Ensure all personnel who 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 recorded at HQMC, in JPAS, and in their personnel security file.

(19) 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).

(20) 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.

b. Top Secret Control Officer (TSCO). If required, the TSCO shall be appointed in writing by the CO to be responsible for the accounting of all command TS information. The Security Manager may concurrently serve as the TSCO. The TSCO shall:

(1) Be responsible for all TS CMI handled within their command. TS CMI shall 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 TS information, and 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 TS material for a period of five years past the date of the event, or in the event of designation or access authorization letters, five years after termination of tenure.

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

c. Assistant Security Manager. The Assistant Security Manager, if assigned, shall:

(1) Be either an E-6 or above, or a civilian employee in the Security administration series GS-0080 in the pay grade GS-09 or above.

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

(3) Be a U.S. citizen and have been the subject of a favorably adjudicated Tier 5 completed within the previous five years.

(4) Attend the Security Manager's Course within 90 days of appointment.

d. Contracting Officer's Security Representative (COSR). When assigned, the COSR will be a Security Specialist, appointed in writing by the Contracting Officer. The Security Manager may serve concurrently as the COSR. The COSR shall:

(1) Be responsible to the Security Manager for coordinating with program managers and technical and procurement officials.

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

e. Security Officer. The Security Officer shall be responsible for the Physical Security and Loss Prevention Program. The Provost Marshal shall serve as the Security Officer and is guided by the provisions of the current edition of reference (j).

f. Cyber Security Manager. The Cyber Security Manager shall serve as the point of contact for all information systems security (INFOSEC) matters

relating to all information systems and networks maintained and/or used by MCAS Beaufort.

g. Special Staff Department Responsibilities

(1) The S-3/5/7 Director shall advise and assist the Security Manager on operations security and anti-terrorism/force protection issues.

(2) The S-4 shall manage, advise, and assist the Security Manager on security equipment procurement matters.

(3) The S-6 shall manage, advise, and assist the Security Manager on INFOSEC, information assurance, and COMSEC.

(4) The Security Officer shall advise and assist the Security Manager on physical security and loss prevention.

(5) The Director of Communication Strategy and Operations shall advise and assist the Security Manager on security reviews before public release of briefs, photography, and articles.

3. Special Types of CMI and CUI

a. Special Types of CMI. Certain information, referenced in the current edition of reference (b), is controlled by EOD and the CMCC and corresponding staff sections. Staff sections and departments who routinely handle special types of CMI shall refer to the references for governing regulations.

b. CUI. Reference (e) covers several types of unclassified controlled information including: "For Official Use Only (FOUO)" information, "Sensitive But Unclassified" (formerly "limited official use") information, "Drug Enforcement Administration 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 identification and control.

4. Definitions

a. Access. The ability and opportunity to obtain knowledge or possession of classified information. An individual does not have access to classified information merely by being in a place where such information is kept. There are provided security measures that are in effect to preclude the individual from gaining knowledge or possession of such classified material. Access is granted based on the individual's NTK.

b. Classified Information. Official information that in the interest of national security has been determined to require protection against unauthorized disclosure.

c. Classified Material. Any material, document, or equipment assigned a classification.

d. Clearance. An administrative determination by designated authority that an individual is eligible for access to classified information in a specific classification category.

e. Compromise. A security violation that has resulted in the confirmed or suspected exposure of an unauthorized person to classified information or material.

f. Counterintelligence. The aspect of intelligence activity that is devoted to discovering, neutralizing, or destroying the effectiveness of hostile foreign intelligence activities and to protecting information against espionage, individuals against subversion, and installations or material against sabotage.

g. Marking. The physical act of indicating, on classified material, the assigned classification, changes in classification, downgrading, and declassification instructions, and any limitations on the use of the classified information.

h. Need-to-Know. The necessity for access to, knowledge of, or possession of classified information in order to execute official military or governmental duties. Responsibility for determining if a person's duties require access to classified material rests with the Security Manager.

i. Security Violation. Any failure to comply with regulations or procedures relative to the security of classified material.

j. COMSEC. COMSEC ensures the security of telecommunications, confidentiality, and integrity. Generally, COMSEC may refer to the security of any information that is transmitted, transferred, or communicated.

Chapter 2

Program Management

1. Inspection Program. The CO Inspection Program has established a requirement for review and inspection procedures to evaluate the effectiveness of the IPSP. These inspections shall be conducted by qualified personnel and will inquire into the security procedures and practices including, but not limited to, classification, issue, transmission, control and accounting, storage, review for downgrading and declassification, personnel security, and security education and training.

2. Management Official. The Security Manager shall be appointed in writing. He or she assists the CO in fulfilling the latter's responsibilities for the protection of classified information being guided by the references. The Security Manager shall:

a. Serve as the CO's advisor and direct representative in matters pertaining to the security of classified information.

b. Develop written command security procedures, including an emergency plan, and when required, include emergency destruction procedures.

c. Ensure formulation and compliance with accounting and security control requirements for classified material, including receipt, distribution, inventory, reproduction, and disposition.

d. Ensure that all personnel who are to handle classified information are cleared and that all requests for personnel security investigations are properly prepared, submitted, and monitored.

e. Ensure that clearance statuses and accesses granted are recorded and accessible for verification.

f. Administer the Command's classification management requirements by maintaining a program for the proper classification, declassification, and downgrading of information.

g. Coordinate the preparation and use of classification guides and the development of advance security planning for the Installation.

h. Ensure compliance with provisions of the industrial security program for classified contracts with DoD contractors.

i. Ensure security control over installation visitors.

j. Manage the security education program for installation personnel.

k. Ensure that compromises and other security violations are reported and investigated.

3. Inventory of Classified Material

a. General. An inventory of all classified material shall be conducted annually by the material custodian. Such inventories will involve a reconciliation to ensure that all material received by the Command is on hand and administrative records are current and accurate. This inventory shall

also serve as "Clean-Out day" in which material no longer required will be identified. However, COMSEC material shall be inventoried on a more frequent basis.

b. Frequency of Inventory. Inventories shall be held on the following occasions:

(1) When there is a change of personnel.

(2) When a security container is found open, unattended, and compromise or suspected compromise has occurred.

(3) When a member of the Command having access to the classified material commits suicide, attempts suicide, or is in an unauthorized absence (UA) status for over 48 hours.

(4) COMSEC shall be inventoried bi-annually (February and August), or after the change of CO or Key Management Infrastructure (KMI) Manager.

4. Dissemination of Classified and Controlled Information. Dissemination of classified information outside of the Command must be approved by the CO or Security Manager. Classified information originated in a non-DoD department or agency cannot be disseminated outside the DoD without the consent of the originator, except where specifically permitted. Authority for disclosure of classified information to a foreign government is the responsibility of the Director, Navy International Programs Office. At times we will have officials of a foreign government visiting the Command for official business. At no time will foreign nationals be given access to classified information without the approval of the CO or Security Manager.

5. Internal Security Procedures

a. All MCAS Beaufort divisions, branches, 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 shall 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.

6. Inspections, Assist Visits, and Reviews. The Security Manager will be responsible for evaluating the security posture of the Command.

a. The Security Manager shall, on an annual basis, conduct inspections or reviews to examine the overall security posture of MCAS Beaufort.

b. The Security Manager shall, on an annual basis, conduct inspections, assist visits, or reviews to examine overall security posture of their subordinate elements.

c. The Command Security Manager shall use the Automated Inspection Reporting System Checklist, which is available on the Inspector General of the Marine Corps, Inspections Division, web page.

Chapter 3

Security Education

1. Basic Policy and Responsibilities. The Security Manager is responsible for establishing and maintaining an active security education program to instruct personnel on security policies and procedures, regardless of their position, rank, or grade.

2. Scope. The principal guide for the security education programs is contained in the current edition of reference (a).

3. Principles. The security education program shall be designed to:

a. Familiarize personnel with security requirements applicable to their duties and assignments.

b. Remind personnel of their responsibility to ensure that classified material is safeguarded effectively and economically.

c. Ensure conscientious compliance with security regulations and procedures.

d. Make personnel aware of their responsibilities in the classification management program.

e. Inform personnel of techniques and devices employed by foreign intelligence agencies in attempting to obtain classified information and their individual responsibility to report any attempts or suspected attempts.

f. Advise personnel having access to classified information of the hazards of unauthorized disclosure to any person not authorized to receive such information.

4. Types of Briefings. The Security Manager shall ensure that the following briefings are conducted:

a. Orientation Briefing. Every new employee, military and civilian, shall receive a new employee orientation.

b. Initial Security Brief. An initial security brief shall be given to all individuals when they are granted access.

c. Annual Refresher Briefing. Personnel having access to classified information will be given an annual refresher briefing. In most cases the supervisor will give the briefing with written guidance from the Security Manager.

d. Naval Criminal Investigative Service (NCIS) Briefing. All personnel who have access to secret information and above shall receive an NCIS counterespionage briefing at least every two years. Individuals holding a Secret clearance for the purpose of frequent travel or periodic access to restrictive areas do not require the brief. The Security Manager shall arrange for the briefing with the servicing NCIS Office.

e. Supervisors must ensure that subordinates know the security requirements impacting on their duties. Assuming is what precipitates compromise of information. OJT training by supervisor and leaders will cover

such aspects as to the proper use of Standard Format (SF) 701, SF 702, local access procedures for the work area, and protection of classified information when not secured.

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

a. NATO Briefings. All personnel requiring SIPRNET accounts will be briefed to NATO SECRET before SIPRNET access is granted. NATO debriefs will be conducted in conjunction with the Security Debrief (see paragraph 6a).

b. Courier Responsibilities Brief. All couriers will be informed of and acknowledge their security responsibilities when escorting or hand-carrying CMI. All courier briefs will be records will be maintained at the Security Manager's Office.

c. Critical Nuclear Weapon Design Information. 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 explosives personnel. The Security Manager will record RD/CNWDI briefing/debriefing within JPAS.

d. Foreign Travel

(1) Command personnel requesting foreign travel for annual leave will report to the Security Manager 60 days prior to receive applicable training for the foreign country being visited.

(2) All personnel possessing security clearance eligibility are required to list all personal foreign travel as part of the required periodic reinvestigation.

e. Complete other special briefings as circumstances dictate.

6. Debriefings. Under pre-defined conditions, the 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 termination statement will be executed and a command debriefing will be given under any of the following conditions:

a. Prior to termination of active military service or civilian employment.

b. At the conclusion of the access period when a Limited Access Authorization has been granted.

c. When a security clearance is administratively withdrawn.

d. When a member of the Command who possesses no clearance or access, has inadvertently gained access to CMI.

e. When security clearance eligibility is revoked for cause by the DoDCAF.

f. When a member of the Command, who possesses a clearance and access, inadvertently has substantive access to information which the individual is not eligible to receive;

g. When a member of the Command transfers out of the Command; and/or

h. Temporary separation for a period of 60 days or more including sabbaticals and leave without pay.

i. The original termination statement must be placed in the Marine's official military personnel file (OMPF) or 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 shall be forwarded to HQMC, Plans, Policies and Operations/Security Division (PP&O/PS).

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

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

Chapter 4

Loss, Compromise, and Other Security Violations

1. Policy. The loss/compromise of CMI represents a threat to national security and must be determined, properly investigated, and necessary actions taken to negate or minimize the adverse effects of the loss/compromise and preclude recurrence. The following are definitions of security violations and must be immediately brought to the attention of the Security Manager:

a. A loss of CMI occurs when it cannot be physically accounted for or located.

b. A compromise is the unauthorized disclosure of CMI to a person who does not have a valid clearance, authorized access, or a NTK. 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.

c. 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.

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

e. 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, including contractors, 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, forfeiture of pay, removal, or termination.

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

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

3. Incident Reporting Responsibilities. Any individual or custodian of CMI with knowledge of a loss/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 CO to initiate a PI.

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

a. PIs will be conducted by an individual assigned external to the department, division, or section requiring the inquiry. At a minimum, the officer conducting the PI 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) (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 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 PI results. Every effort shall be made to keep the PI unclassified and without enclosures. If lost information is beyond the jurisdiction of the U.S. and cannot be recovered, the PI shall be classified commensurate to the security classification level of the lost information to prevent its recovery by unauthorized personnel.

(4) All PI's will be initially completed within three working days and reported via naval letter format to the appointing officer via the Security Manager. The Security Manager will then transcribe the PI into naval

message format addressed to HQMC PP&O/PS, Commander, Marine Corps Installations Command (COMMCICOM), the originators of lost or compromised CMI, OCA's if known, NCIS, and any other commands involved in the PI.

(5) If during the conduct of the PI it is determined that a compromise or possible compromise in fact did not occur, the PI shall still continue to completion to determine what security weaknesses existed that permitted the violation to occur. The CO, via the Security Manager, shall provide an info copy of PIs to the Marine Corps Installations East-Marine Corps Base Camp Lejeune (MCIEAST-MCB CAMLEJ) Security Manager. No further reporting of these results external to MCIEAST-MCB CAMLEJ is required.

(6) If during the conduction of the PI a compromise is confirmed, probability of damage to national security cannot be discounted, a significant security weakness is revealed, or punitive action is appropriate the Security Manager shall verify and a formal 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 required corrective or disciplinary actions when a PI confirms a compromise, 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). The Command will address the completed JAGMAN investigations to MCIEAST-MCB CAMLEJ COMMCICOM, and HQMC PP&O/PS.

6. Investigative Assistance. A PI 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 Security Manager, the SJA, or NCIS. All requests for assistance will be coordinated through the Security Manager.

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

a. Report losses/compromises involving computer systems to the Cyber Security Manager and Security Manager. The Security Manager will route all correspondence involving losses/compromises via the MCIEAST Security Manager.

b. Report losses/compromises involving COMSEC via an initial report, per the procedures contained in the current edition of electronic key management system 1 series. This initial report will suffice for the PI requirements of this Order, and will be forwarded to the MCIEAST Security Manager, MCIEAST KMI Manager, and the local NCIS office. No other deviations from the reporting procedures of this chapter are authorized.

c. Report losses/compromises involving RD/CNWDI to the MCIEAST-MCB CAMLEJ Security Manager, COMMCICOM, HQMC PP&O/PS, and 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. The Security Manager will inform the MCIEAST-MCB CAMLEJ Security Manager on all correspondence involving losses/compromises.

8. Report of Finding CMI Previously Reported as Lost or Destroyed. When CMI previously reported as lost or destroyed is subsequently found, the Security Manager will be notified. The Security Manager will inform the MCIEAST-MCB CAMLEJ 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 media, i.e., newspaper, magazine, radio, or television, the member must notify the Security Manager, who in turn will notify the MCIEAST Security Manager, COMMCICOM, and HQMC PP&O/PS.

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

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 Security Manager. Normally, security violations demonstrate a weakness in the security program. For this purpose, a PI must also be vigorously and thoroughly conducted. This gives the division, department, or section a "second chance" to shore up their security program before a compromise does occur. 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 compromised 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 Station Duty Officer (SDO). The container will be guarded until the SDO arrives at the location of the unlocked container. The SDO will then inspect the CMI involved, lock the container, and notify the Security Manager. If the SDO believes that CMI may have been compromised, the SDO will immediately notify the Security Manager and recall the person responsible for the container to conduct a complete inventory.

13. Improper Transmission. All CMI received at the Command is normally received via the CMCC. However, because confidential and secret CMI can be sent through either the U.S. Postal Service (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 a department, division, or section could receive CMI directly from the mailroom or the overnight delivery carrier.

a. 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 the CMCC, it should be immediately delivered to the Security Manager with all wrappings and labels received, accompanied by a brief statement of circumstances either verbally or in writing.

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

c. All instances of mishandling where compromise cannot be ruled out must be formally reviewed through a PI, as discussed in paragraph four.

Chapter 5

Counterintelligence Matters to be Reported to the Command Security Manager

1. Policy. Certain matters affecting national security must be reported to the Security Manager, who will report the matter to NCIS. All military and civilian personnel, regardless of access to CMI or not, will report any activities described in this chapter involving themselves, their dependents, or others to the Security Manager or to the nearest DoD component if on leave/temporary additional duty where access to the Security Manager is not feasable.

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 call 9-1-1 and subsequently notify the 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 Security Manager shall 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, COMMCICOM, HQMC PP&O/PS.

b. The 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 NTK, regardless of nationality. The 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, or information about the designation, strength, mission, and combat posture of any command. The Security Manager will notify the local NCIS office of these requests.

3. Contact Reporting

a. All command personnel, regardless of security clearance, shall report 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 to the Security Manager. 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 Security Manager if they are concerned they may be the target of exploitation. The 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, the Security Manager shall immediately report the incident to the DoDCAF, and the local NCIS office if applicable. An incident report shall be submitted via JPAS.

b. Unauthorized Absence (UA). When a member of the Command, who has/had access to CMI is in a UA status, the Security Manager 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 Security Manager will report all information to the local NCIS office, 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 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 Security Manager will report all information to the local NCIS office and DoDCAF. NCIS will advise whether they will conduct an investigation. An incident report shall be submitted via JPAS, all access will be terminated, and the subject shall be removed from any JPAS owning or servicing relation.

5. Foreign Connections

a. A security risk may exist when:

(1) 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.

(2) An individual has financial interest(s) in a foreign country.

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.

Chapter 6

CMI/CUI Control Measures

1. Policy

a. 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) residing in SIPRNET computers will be marked with appropriate magnetic media classification labels, and will be entered into the network operations accounting system by serial number. The HDDs contain classified elements that are the property of the U.S. Government; local procedures must be established 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. This must be completed 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 classified information regardless of the media on which it may be represented.

3. Top Secret Control Measures

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

b. In addition to the marking requirements of chapter six of reference (b), TS information derivatively classified by MCAS Beaufort shall be marked on their "buck-tag" with an individual copy number in the following manner "Copy No.__ of __ copies"; exceptions to this rule are allowed for publications containing a distribution list by copy number. In this case, adequate and readily available documentation shall be maintained indicating the total copies produced and the recipients of the copies.

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

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

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

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

h. Retention of TS documents within MCAS Beaufort will be kept to a minimum. When TS CMI is destroyed, the CMCC section will prepare a classified material destruction report OPNAV 5511/12 identifying the material destroyed and the two officials who witnessed its destruction. The TSCO will retain these destruction records for a period of five years.

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

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

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

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

4. Secret Control Measures

a. The Security Manager Office 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 departments, divisions, or sections.

(2) Records of CMI distributed or routed to departments, divisions, or sections.

(3) Records of CMI disposed of by departments, divisions, or sections through transfer of custody or destruction.

(4) Requirements for an annual inventory.

b. Signed receipts are required for accountable secret CMI distributed or routed within departments, divisions, or sections. All Secret CMI transferred from one section to another within the command will be routed through the Security Manager Office.

c. Correspondence/material control sheets or a locally developed "buck-tag" will be attached to all Secret CMI under the control of CMCC; classified removable HDDs will have the "buck-tag" affixed with the HDD's serial number printed thereon.

d. When transmitting secret CMI to another command, the Security Manager Office 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; where one of the following procedures apply:

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

(b) Mark as "working papers."

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

d. Marking e-mail generated on the SIPRNET:

(1) All SIPRNET generated e-mail must be marked, prior to transmission, with appropriate security classification and associated

markings, including UNCLASSIFIED; this applies to all elements of the e-mail: subject, body, portions, and attachments.

(2) Departments, divisions, or sections are encouraged to use commercial off-the-shelf software on their SIPRNET computers, requiring SIPRNET e-mail users to select the appropriate classification and associated markings prior to sending the e-mail.

6. 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, rough drafts, and similar items that contain secret or confidential information shall:

(1) Be dated when created.

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

(3) Be protected per the assigned classification level.

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

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

c. All confidential working papers, retained for more than 180 days from the date of creation, will be entered into the departments, divisions, or sections SCP accounting system prescribed for finished product CMI.

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

e. All confidential working papers to be transferred from the Command within 180 days of creation will be entered into the Security Manager Office accounting system prescribed for finished product CMI, prior to its transfer via the Security Manager Office.

8. Special Handling Requirements. Departments, divisions, or sections, with the advice of the Security Manager, must establish security rules and procedures for the control of "special handling" messages and material, such as special category, limited distribution, and "Personal For".

9. Control Measures for Special Types of Classified and CUI

a. RD and Formerly Restricted Data. RD and CNWDI are controlled per the current edition of reference (g).

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

c. FOUO. Control FOUO per the current edition of reference (i). Additional guidance in applying the FOUO designation is provided in paragraph 10e (3) below.

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

e. CUI.

(1) Reference (e), 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 "SBU 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 (1), (q), (r), and (s). The review will be coordinated between a subject matter expert on the material to be released, the Security Manager, the Privacy Act Coordinator, the FOIA Coordinator, and may include the SJA and the Communications strategy Office (CSO).

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

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

UNCLASSIFIED//FOUO

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

UNLCASSIFIED//FOUO

(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.

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

(5) Within a U//FOUO document containing both U//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//FOUO information/documents:

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

(b) Limit Distribution Statements within the U.S. 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 Non-classified Internet Protocol Router Network (NIPRNET) e-mail, always including U//FOUO at the beginning of the subject 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 subject 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.

Chapter 7

CMI Dissemination

1. Policy. Within MCAS Beaufort, the dissemination of classified and controlled unclassified material will be kept to a minimum with operational requirements considered based on the NTK principle. All CMI dissemination external to the command will be conducted in accordance with the guidance contained in this chapter and of the current edition of reference (b). Non-DoD originated classified materials will not be distributed outside of the DoD without the approval of the originating department or agency.

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

3. Secret Dissemination. Internal to the Command, Secret CMI shall not be permanently routed from one SCP to another SCP without being processed via the Security Manager Office for accountability with the exception of working papers, e-mails, and naval messages.

4. Confidential Dissemination. The same procedures for secret CMI applies to Confidential CMI.

5. Dissemination of Special Types of Classified and CUI. RD and CNWDI shall only be disseminated per the provisions of references (a) and (g).

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

b. FOUO. FOUO material may be disseminated within DoD components. All requests from non-DoD entities to disseminate FOUO outside MCAS Beaufort shall be routed through the FOIA Officer/Privacy Act Officer.

c. SBU. SBU material shall be handled in the same manner as FOUO.

d. Sensitive Information. Sensitive information as defined by reference (n) shall be disseminated on a NTK basis.

6. Dissemination to Contractors. Cleared personnel, to include cleared contractors, are prohibited from discussing or releasing classified information and documents with other contractors regardless of their level of clearance. Dissemination is only authorized when the visit has been approved through the Security Manager and the contractor has NTK as defined in their 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 Security Manager. At no time will classified or unclassified documents be released to representatives of foreign governments or international organizations without Security Manager's approval.

8. Pre-Publication Review. All material prepared for public release in any format will be subject to Security Manager Review per the current edition of references (i) and (s).

Chapter 8

CMI Safeguarding

1. Policy. CMI shall 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. 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 shall not be discussed with or in the presence of unauthorized persons. Individuals shall 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. 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. 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:

a. 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.

b. 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 be admitted to the area with appropriate approval, but must be controlled by an escort, attendant, or other security procedures to prevent access to CMI.

c. 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.

(1) 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."

(2) All restricted areas require a physical security survey conducted by the Provost Marshal Office on an annual basis or in accordance with reference (j).

4. Safeguarding Work Spaces

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

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

c. Ensure adequate controls are established to prevent unauthorized individuals gaining access to areas where classified material 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 co-located with trash receptacles as the subconscious act of discarding waste material could result in classified material being discarded with regular trash.

f. Classified information shall not be discussed over unsecured telephone lines. Secure telephone equipment is the telephonic equipment 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 to an unclassified AIS without explicit approval and assistance from the Cyber Security Manager.

h. Cameras, photo-capable cell phones or wireless Personal Electronic Devices (PEDs), to include "cordless phones" in areas where classified material is stored or processed is prohibited unless jointly approved by the Security Manager and the Cyber Security Manager. The use of these devices poses a serious threat to national security.

i. Technical surveillance countermeasure (TSCM) services are available 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 TS CMI will be processed or discussed; requests will be forwarded to the servicing NCIS resident agent.

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

a. After removing classified documents from storage, maintain constant surveillance and keep face down or covered when not in use. Classified material cover sheets 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, which includes classified HDD and excludes 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 "UNCLASSIFIED" 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 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.

6. Safeguarding in Storage

a. Departments, divisions, and sections are responsible for the safeguarding of all classified information within their area of responsibility. This 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 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.

(3) Records of security container combinations.

c. Departments, divisions, and sections must submit the SF 700s for their security containers to the Security Manager. Each department, division,

or section with security containers shall select representative to conduct monthly check of SF 700s that have been turned into the Security Manager Office. These monthly checks shall be record and kept annually.

d. In the event that emergency access is required the perspective department, division or section will coordinate with the Security Manager for assistance.

7. Safeguarding During Visits. Only visitors with an appropriate clearance level and "need-to-know" are granted access to classified information. Prior to any visits occurring the Security Manager will be contacted for guidance and approval.

8. Safeguarding During Classified Meetings

a. Classified discussions at meetings are held only when disclosure of the information serves a specific U.S. Government purpose. Current office of the Secretary of Defense (SecDef) 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 where adequate physical security and procedural controls have been approved.

b. TSCM services are available for the purpose of detecting any attempts to obtain classified information from meeting venues through the use of clandestine listening devices. All TSCM service requests will be classified at the secret level and will support surveys of meeting venues where TS CMI will be processed or discussed; requests will be forwarded to the 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 Cyber Security Manager. All PEDs, standard or wireless, such as cell phones, audio recorders, imaging devices, Blackberrys, and smart watches are prohibited within classified conference rooms.

d. Note taking during the classified session of the meeting will be permitted only if such action is necessary. Classified information created, used, or distributed during the meeting shall be safeguarded, transmitted, and transported per the procedures contained in this Order and reference (b).

9. Safeguarding CMI while being Hand Carried. Internal to the Command, classified cover sheets are required on all classified documents when they are not secured in a safe (when visual access is available to persons not having the proper clearance or 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

10. 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 CO or the 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 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 public areas.

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:

(1) The CMI shall 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 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 shall 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.

Chapter 9

CMI Duplication and Distribution

1. Policy

a. The policy for MCAS Beaufort is to keep the duplication and distribution of classified material to the absolute minimum while maintaining operational effectiveness. 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) Universal Serial Bus (USB) pen drives, flash drives, and 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 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 desktop or standalone computer either directly 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.

(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, compact disks (CDs), pen drives, thumb drives, fire-wire hard drives, personal computer memory card international association hard drives, flash media, memory cards, compact flash drives, 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. Certain secondary storage media pose a substantially high risk to national security, particularly the USB pen and thumb drives.

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.

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

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

a. The Security Manager Office is the only section that can approve the reproduction of CMI at locally authorized reproduction facilities.

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

c. 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 shall only be copied on a classified copier. The Security Manager must be consulted for additional guidance.

b. TS CMI shall not be copied except by the Security Manager, 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 departments, divisions, and sections under the following conditions:

(1) The department, division or section has a classified copier that has been approved by the 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 SECURITY MANAGER. USE OF THIS DEVICE TO PROCESS CMI MUST BE APPROVED BY SCP."

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

(2) The SCP Custodian of the particular department, division, or section will provide local approval authority for all CMI copied within their custodial area of responsibility.

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. Copies of paper containing unclassified, high-density text, with few blank or black spaces shall be made per the following:

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

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

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

4. Controls on FAX Devices

a. Those departments, divisions, or sections with an approved secure fax device connected to phone lines via an approved secure activated encryption device may send CMI via fax providing the equipment is appropriately marked: "THIS DEVICE IS AUTHORIZED FOR PROCESSING CLASSIFIED MILITARY INFORMATION UP

TO AND INCLUDING (classification), BY DIRECTION OF THE COMMAND SECURITY MANAGER. USE OF THIS DEVICE TO PROCESS CMI MUST BE APPROVED BY SCP."

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

(1) Receiving fax number.

(2) Person receiving fax.

(3) Date material sent.

(4) Authorizing official.

(5) Description of material sent. (e.g., "Encl (1) of DIAM 5813, Vol II.")

c. 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.

d. 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.

e. Fax devices connected to unsecured phone lines shall 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 shall 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.

6. Controls on Printer Devices. Classified computers may only print to printers accredited to process CMI. Any computer not configured to print to a printer accredited to process CMI is not authorized to print CMI regardless of the computer's accreditation. Appropriate accreditation labels shall be affixed.

7. Controls of Audio Recording Devices. 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 Security Manager.

8. Controls of Visual Recording Devices. 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 Security Manager, in consultation with the Cyber Security Manager and CSO.

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

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 Cyber Security Manager and the 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. 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 Security Manager. As such, these USB flash memory devices should be considered "data transfer" vice "data storage" devices.

(a) The Security Manager and the Cyber Security Manager will only consider government purchased devices for CMI storage or transfer approval; personally owned devices are strictly prohibited under any circumstance.

(b) The USB flash memory device must be etched with a Security Manager Office 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 shall 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.

10. Clearing and Purging of CMI from Media and Devices. Detailed instructions for clearing and purging devices and media are contained in reference (t). All candidate media and devices for purging shall be turned over to the Security Manager Office for accounting, control, and coordination with the Cyber Security Manager for purge processing.

Chapter 10

CMI Destruction

1. Policy. CMI record material may be destroyed only when destruction is the disposition authorized by the current edition of reference (u). Classified information that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center. All other CMI, including "finished product," "working papers," and DMS messages will be destroyed when no longer required. Early destruction of unnecessary CMI assists in reducing security costs, preparing for emergency situations and better protecting necessary CMI. CMI over five years old will not be retained without proper justification being provided to the Security Manager.

a. MCAS Beaufort policy requires unclassified messages and all unclassified controlled information as defined by reference (e), including those defined in reference (n), and technical documents with limited distribution statements be destroyed via 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.

b. Destruction of COMSEC materials is outside the scope of this Order and shall be accomplished by designated personnel only per the current directives governing this program.

c. The annual clean out day shall be conducted during annual inventory.

2. Destruction Procedures

a. CMI shall 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 Security Manager is responsible for the destruction of all accountable CMI entered into the Command's accountability system.

(1) Secret "working papers" and secret messages that 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 under the guidance of the Security Manager.

(2) The physical task of destroying accountable secret and confidential CMI may be delegated to the SCPs. Secret and Confidential CMI will be destroyed by two cleared command personnel: 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 Security Manager Office.

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

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

3. Media Destructive Guidance. Various methods and equipment may be used to destroy or purge CMI including cross-cut shredding, degaussing, and disintegrating.

a. Evaluated product listings provided by the National Security Agency 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. Command personnel requiring destruction of hard drives, CDs and digital video disks will contact the Security Manager for access to the degasser and hard drive shredder. Other media such as computer chips, film, floppy disks, magnetic cards, micro circuit units, microfiche, mylar, paper, printed circuit boards, slides, typewriter, ribbons, cartridges, viewgraphs, CDs, diskettes, loose tape, optical tape, reel-to-reel tapes, tape cartridges, and videocassette recorder tapes will be turned into the Security Manager's Office for destruction.

4. Emergency Destruction

a. The priorities for emergency destruction are:

(1) Priority one - TS CMI

(2) Priority two - Secret CMI

(3) Priority three - Confidential CMI

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

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

(a) Items of CMI that may not have been destroyed.

(b) CMI presumed to have been destroyed.

(c) Classification of CMI destroyed.

(d) Method of destruction.

(e) 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 the following additional information:

(a) Character of the records destroyed.

(b) When and where the destruction was accomplished.

(c) Circumstances under which the emergency destruction was implemented.

Chapter 11

Industrial Security Program

1. Policy. All approved DoD contractors that operate within MCAS Beaufort areas shall fall under the direct security oversight of MCAS Beaufort. The Security Manager has been delegated to provide the security oversight for this Command.

2. Classified and Operationally Sensitive Contracts and the DD 254

a. All classified or operationally sensitive contracts, the Contracting Officer and the 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. 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.

a. The COR is responsible to the 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, all cleared DoD contractors shall be classified as either short-term or long-term visitors under the Command's Visitor Control Program. Contract employees shall conform to this IPSP and will be included in applicable portions of the Command's Security Education Program, per reference (b).

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

b. The Security Manager office shall validate the visitor's access requirement with the department, division, or section's 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 shall disclose classified information during the visit.

5. Contractor Identification Cards. All cleared contractors, and contractors without clearance, working within controlled spaces shall wear an identification card. Cards shall be generated using the Authorized Personnel Automated Clearance System or locally issued Marine Corps Electronic Security Systems.

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

a. The CO reserves the authority and responsibility under reference (v) to request investigations on these persons and to protect persons and property under their command against the actions of untrustworthy persons.

b. Should the CO exercise this authority, the Contracting Officer shall include the FAD program requirements in the contract specifications.

c. The Security Manager shall coordinate the submission of Tier 1, "Questionnaire for Public Trust Positions".

d. Alternatively, the Federal Bureau of Investigations 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). The Security Manager Office is authorized to perform such background checks as required.

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."

Chapter 12

Personnel Security Policy

1. Policy. The Security Manager is responsible for administering the IPSP and is the Staff Officer for the IPSP. The Security Manager shall advise the CO 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 Services level or assignment to sensitive duties.

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

3. Commanders and Executive Officers. The COs of MCAS Beaufort and Headquarters and Headquarters Squadron, and their Executive Officers must possess a favorably adjudicated Tier 5 investigation.

4. Designation of Civilian Sensitive Positions

a. The Security Manager shall assist the CO in completing a survey of all National Security Positions within their commands for DoD civilian personnel. Category designations of Special Sensitive "SS", Critical Sensitive "CS", and Non-Critical Sensitive "NCS" shall be applied to each position; any position not meeting the criteria for a National Security position shall be referred to as "Non-Sensitive."

b. It is imperative the civilian position description accurately reflects the required duties and corresponding position sensitivity requirements. The Security Manager shall make liaison with the Command's Station S-1 and Human Resources Office (HRO) 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 Tier 1 or its equivalent.

(2) The incumbent in a DoD civilian National Security position must be able to obtain and maintain the clearance eligibility for the corresponding position sensitivity. Loss of eligibility must be reported to the Command's Station S-1, Human Resources Office Department Head and the MCAS Beaufort Executive Officer.

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 determinations. A determination by the DoDCAF that an individual is not eligible for assignment to sensitive duties, or a clearance, shall also result in the corresponding removal of duties and/or clearances.

Chapter 13

Personnel Security Investigations

1. Policy. No individual shall be granted access to CMI or be assigned to sensitive duties unless the individual possess a favorably adjudicated background investigation that grants a security clearance eligibility commensurate to the classification level of the CMI or access to sensitive duties.

2. Command Responsibilities. Prior to submission of a Personnel Security Investigation (PSI), the Security Manager shall 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 shall be granted clearances and access to classified information or assigned sensitive duties.

(2) Citizenship shall be verified per Appendix I of the current version of reference (a).

(3) Immigrant aliens shall 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 Security Manager.

c. Conduct a local records check of all available personnel, medical, legal, security, base/military police, and other command records to determine if disqualifying information exists.

3. Investigative Request Requirements

a. All PSI requests shall be prepared following guidance found in reference (a).

b. The Security Manager or Assistant Security Manager, acting on behalf of the CO, are the only officials authorized to request PSIs on individuals within the Command.

c. The Security Manager shall ensure that all Marines in the Command have been the subject of a Tier 3 or equivalent.

d. PSIs and PRs shall not be requested for any civilian or military personnel who shall retire, resign, or separate with less than one year service remaining. Exceptions shall be granted only for those personnel whose participation in a Special Access Program is documented with appropriate orders and whose assignment is contingent upon completion of the required PR.

e. The scope of the PSI requested from the OPM shall be commensurate with the level of sensitivity of the access required or position occupied. Only the minimum investigation to satisfy a requirement shall be requested.

The various types of investigations are described in chapter six of reference (a).

4. Defense Information System for Security (DISS). DISS provides accurate, updated investigation information on personnel from all branches of the service, DoD civilians, and DoD contractors.

5. OPM. The OPM conducts all PSIs for the Marine Corps. The Security Manager and the assistant Security Manager are prohibited from conducting their own PSIs.

6. Preparation and Submission of PSI Requests

a. Each individual approved for submission of a PSI shall forward their completed SF-86, Questionnaire for National Security Positions, to the Command Security Manager via the Electronic Questionnaires for Investigations Processing System for validation and processing.

b. All PSI requests shall require certification and investigation release forms signed by the individual submitting the PSI; and all investigation requests, Tier less than 5R or equivalent, shall 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).

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/her 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 shall 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 Security Manager Office.

a. The file copy of an individual's completed SF-86, maintained electronically in the personnel security file, is not required for retention after the background investigation has been adjudicated by the DoDCAF. While it is maintained in the personnel security folder it should be afforded FOUO level protection, at a minimum.

b. In rare instances, the Security Manager 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 shall 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 Security Manager is limited to assisting in identifying the name and address of the FOIA Officer at the investigating agency. The 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 may be stored in a vault, safe or in an appropriate manner to protect the investigative materials or report. Under no circumstances shall the investigation material or reports be placed in a Marine's Officer Qualification Record, OMPF, or a DoD Civilian's OPF.

Chapter 14

Personnel Security Access Determinations

1. 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. 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. DISS

a. All personnel with authorizations to access to CMI, or any special program, must annotate that access in DISS.

b. The DISS enables security personnel to communicate eligibility/access issues with DoDCAF.

4. Eligibility Determination

a. The DoDCAF shall 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 shall communicate the results to the requesting command via DISS.

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

(2) DoDCAF can issue a Memorandum of Intent to Deny or Revoke security clearance eligibility to an individual for whom an unfavorable personnel security determination is being contemplated.

(3) DoDCAF can issue a Memorandum of Denial or Revocation 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 CO via the Security Manager shall 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 Security Manager shall initiate a local records check per chapter 13, paragraph two of this Order prior to granting initial command access, reporting any negative findings to DoDCAF via an "Incident Report" in JPAS.

(2) The Security Manager must continuously evaluate command personnel with regard to their eligibility for access to CMI. Enclosure (12) of the most current edition of reference (a), provides excellent guidance on the "Continuous Evaluation Program."

(3) The Security Manager must advise the CO 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 DISS, and to the subject of the suspension in a letter from the Security Manager. The current version of reference (a) provides excellent guidance.

5. Unfavorable Determination

a. An unfavorable personnel security determination shall 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 Requests for Information or Letters of Notification) are sufficiently addressed in chapter seven 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 shall 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 Security Manager shall be the determining authority for validating and accepting other government agency issued security clearances.

Chapter 15

Personnel Security Access

1. Policy

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

b. Access to classified information shall be limited to the minimum number of individuals necessary to accomplish the mission and shall be based on NTK.

c. The CO via the Security Manager shall ensure that personnel under their command are briefed in accordance with chapter three, paragraph five of this Order before granting access to CMI.

2. Requests for Access. All requests for access shall be provided to the 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 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 Defense Clearance and Investigation Index 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 shall not be used as proof of eligibility for access.

c. Access authorization is a local command responsibility and is based on NTK established by the CO; 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 shall access be granted based upon the desires of the individual requesting access.

3. 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 shall be witnessed, with the witness' entry affixed at the time of execution.

(2) The Security Manager and his assistants accept and witness the signing of 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.

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 shall be retained at HQMC for 50 years following its date of execution. Forward the executed, witnessed, and accepted original SF-312 to MMSB-20 at the following address:

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

(2) 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 Secretary of Defense determined that additional measures were warranted to increase the awareness of individuals who were entrusted with access to CMI at all levels of eligibility and/or indoctrinated into Special Access Programs. In compliance, the statement below shall 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 shall not be sworn to. Attestation administration is required only one time, usually when the original SF-312 or 1879-1, SCI Nondisclosure agreement is signed. Reporting the attestation shall be accomplished via JPAS on the individual's "Personal Summary" screen.

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

5. Temporary Security Clearance Request (Access) (formerly known as Interim). Temporary security clearance and access may be granted (except for SCI access) pending completion of full investigative requirements and pending establishment of a final security clearance by DoDCAF. Temporary clearances may be granted by the Commander via the Security Manager under the following conditions:

a. Temporary TS Security Clearance

(1) Either Secret security clearance eligibility exists, or a favorable National Agency Check, Local Agency Check and Credit, Tier 3, or Access National Agency Check with Written Inquiries and Credit Check (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).

(4) The Tier five has been submitted to the OPM.

b. Temporary Secret or Confidential Security Clearance

(1) A favorable review of local records.

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

(3) The Tier three investigation has been submitted to OPM.

c. The Security Manager will record interim security clearances in JPAS.

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

6. Access, Termination, Withdrawal, or Adjustment

a. A "debrief" and an "out-process" action is required in JPAS on the individual's Person Summary screen upon departure of the Command. Local termination of access and a debriefing per chapter three, paragraph seven of this Order, is required when:

(1) When a Marine executes a Permanent Change of Station/Assignment orders.

(2) When a civilian transfers within the DON.

(3) When a Marine or civilian retires or terminates service. Additional requirements for this occasion are:

(a) A debriefing and a Security Termination Statement (OPNAV 5511/14 Rev 9-05) are required.

(b) DoDCAF shall be notified via JPAS of the reasons for termination.

(c) The completed Security Termination Statement shall be immediately forwarded for inclusion in the individual's OQR, OMPF, or OPF prior to close-out and transfer to a records retention facility.

b. 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 shall 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 CO may suspend access locally. Details regarding such

suspensions are adequately addressed in chapter nine of reference (a). All local suspensions will be reported to DoDCAF via JPAS with an "Incident Report".

8. Continuous Evaluation

a. Individuals must report to their supervisor or appropriate official any incident or situation that could affect their continued eligibility for access to classified information or assignment to sensitive duties. Supervisors or appropriate officials having received notification from their employees shall immediately report the incident or situation to the Security Manager. Co-workers have an obligation to advise their supervisor or appropriate official when they become aware of adverse information concerning an individual who has access to CMI or assignment to a sensitive position. Supervisors and leaders play a critical role in early detection of an individual's problems. Supervisors and leaders are in a unique position to recognize problems early and must react appropriately to ensure balance is maintained regarding the individual's needs and national security requirements. Confidentiality and personnel assistance is the key to the continuous evaluation process.

b. Legal Officer. The Legal Officer shall provide the Security Manager a copy of the weekly legal brief.

c. Substance Abuse Control Officer (SACO). The SACO shall provide the Security Manager a copy of the weekly substance abuse report.

d. Government Travel Charge Card (GTCC) Coordinator. The GTCC Coordinator shall provide the Security Manager a copy of the monthly Hierarchy Delinquency Report.

e. Provost Marshal. The Provost Marshal shall ensure that the Security Manager is placed on the Military Blotters disposition list.

f. Cyber Security Manager. The Cyber Security Manager shall provide the Security Manager with any reports of spillage or misuse of government computer systems.

g. Director, HRO. The Director of HRO shall notify the Security Manager of any administration action taking on an employee as a result of an incident or situation that could affect their continued eligibility for access to classified information or assignment to sensitive duties.

Chapter 16

Visitor Control

1. Policy. For security purposes, the term "visitor" applies to all individuals who are not permanently assigned to the Command. All visitors must be subject to approval prior to gaining Installation access. 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.

2. Facilitating Classified Visits

a. DISS 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. DISS shall be used to request and verify the personnel security clearance level for visitors requiring access to CMI.

(1) Visit Authorization Letters (VALs) are no longer required for civilian, military, and contractor personnel whose access level and affiliation are accurately reflected in DISS.

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

c. The responsibility for establishing the positive identification of visitors and determining NTK prior to the disclosure of any classified information will be validated by the Security Manager prior to disclosing the classified information.

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

a. Requests for official visits conducted by foreign governments or representatives to this Command's 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 MCAS Beaufort, will be routed through 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 & MCFPEPs) will be supported from HQMC with a Delegated Disclosure Letter, forwarded to the command via MCIEAST-MCB CAMLEJ, detailing the level of disclosure authorized. 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) All forward copies of the Foreign Officer Statement of Understanding letters to the MCIEAST-MCB CAMLEJ Command Security Manager.

d. The current editions of references (v), (w), and (x) provide detailed information for Foreign Disclosure Officers and Foreign Disclosure Points of Contact.

Chapter 17

Emergency Action Plan

1. Natural Disasters. Natural disasters includes 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 present will execute the Emergency Action Plan.

a. Fire after duty hours. Should a fire occur around or within the building where classified or COMSEC is stored, the custodian of the classified or COMSEC will:

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

(2) If the fire occurs during duty hours, secure all classified and COMSEC material in the safe and secure the vault door.

(3) If the fire occurs after duty hours, ensure the vault or secure room door which stores classified or COMSEC is secured before leaving the area.

(4) If safe, use all local means to extinguish or control the fire until the fire department arrives. Fire extinguishers are located throughout the building.

(5) If after duty hours, and as soon as possible, notify the Security Manager.

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

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

(8) The Security Manager/Assistant or Classified Custodian shall, 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 shall be locked and two guards shall be placed in the secure area until the Security/Assistant Manager performs a post-emergency inventory.

(9) If the intensity of the fire is such that the area must be abandoned, maintain adequate surveillance of the general area to prevent unauthorized persons from entering.

b. 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.

(1) Prior to hurricanes the Security Manager, Security Assistant, or Classified Custodian shall waterproof all classified or COMSEC material and gear in safes. All classified computers will be unplugged and waterproofed with plastic as necessary. All other logs, documents, and other important papers shall also be secured in waterproof containers.

(2) If there is damage to the CMCC Vault from a hurricane, flood, or other phenomena the SDO, or other person on the scene, will immediately contact the Security Manager or Security Assistant to inform them of the extent of damage.

(3) Two persons shall be posted, if necessary, as a guard force to prevent unauthorized access to classified material until CMCC personnel arrive.

(4) The CMCC will coordinate the removal of classified material, if required, to a location designated utilizing the Emergency Evacuation Cards located on the inside left wall of the CMCC Vault.

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

a. Stage One - Force Protection Condition - Bravo

(1) Threat source - Operations in high risk environment.

(2) Time frame - Several days to several months.

(3) Action - Precautionary Emergency Protection as outlined under Terrorist Actions below.

b. Stage Two - Force Protection Condition - Charlie

(1) Threat source - Probability of hostile attack.

(2) Time frame - From one to several days.

(3) Action - Possible Emergency Evacuation as outlined under Emergency Evacuations below.

c. Stage Three - Force Protection Condition - Delta

(1) Threat source - Attack by hostile forces.

(2) Time frame - Imminent.

(3) Action - Immediate Emergency Protection or Evacuation as outlined under Terrorist Actions and Emergency Evacuations below.

d. Bomb Threat. In the event of a bomb threat, the Provost Marshal's Office shall be notified by dialing "9-1-1". Classified and COMSEC material will be secured in the CMCC safe. The safe shall be locked and all

classified/COMSEC material accounting records shall be removed from the building. Personnel shall wait outside the building at a safe distance until the arrival of the military police and EOD Team. The building shall not be re-entered until the "ALL CLEAR" signal is given by EOD personnel.

3. 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.

a. Force Protection Condition (FPCON) Normal. FPCON NORMAL applies at all times as a general threat of terrorist attacks, hostile acts, or other security threats always exists in the world.

(1) Educate command personnel on the terrorist and hostile adversary threats, deterring and detecting these threats, and reporting indications of these and other suspicious activities, to maintain a level of protection the Secretary of Defense requires for all DoD elements and personnel against terrorist attacks and hostile acts.

(2) Ensure personnel are knowledgeable on terrorist and hostile actor threats; understand the individual actions they can take to protect themselves and others from terrorist attack; know procedures for reporting suspicious activities and incidents; deter and detect general, non-specific threats of terrorist attacks and hostile acts; and prepare to implement additional FPCON measures designed to delay, deny, and defend against these threats.

(3) Regularly assessing facilities for vulnerabilities and taking measures to reduce them.

b. FPCON ALPHA. FPCON ALPHA applies to a non-specific threat of a terrorist attack or hostile act directed against DoD elements and personnel.

(1) Checking communications with designated emergency response or command locations.

(2) Reviewing and updating emergency response procedures.

(3) Providing the public with necessary information.

c. FPCON BRAVO. FPCON BRAVO applies when an increased or more predictable threat of a terrorist attack or hostile act exists and is directed against DoD elements and personnel. In addition to the previously outlined protective measures, the following may be applied:

(1) Increasing surveillance of critical locations.

(2) Coordinating emergency plans with nearby jurisdictions.

(3) Assessing further refinement of protective measures within the context of current threat information.

(4) Implementing, as appropriate, contingency and emergency response plans.

d. FPCON CHARLIE. FPCON CHARLIE applies when a terrorist or hostile act incident occurs within the commander's area of interest, or intelligence is received indicating a hostile act or some form of terrorist action or targeting against DoD elements, personnel, or facilities is likely. In addition to the previously outlined Protective Measures, the following may be applied:

(1) Coordinating necessary security efforts with armed forces or law enforcement agencies.

(2) Taking additional precaution at public events.

(3) Preparing to work at an alternate site or with a dispersed workforce.

(4) Restricting access to essential personnel only.

e. FPCON DELTA. FPCON DELTA applies when a terrorist attack or hostile act has occurred or is anticipated against specific installations or operating areas. In addition to the previously outlined protective measures, the following may be applied:

(1) Assigning emergency response personnel and pre-positioning specially trained teams.

(2) Monitoring, redirecting, or constraining transportation systems.

(3) Closing public and government facilities.

4. 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. Emergency evacuation shall only be executed when directed by the CO or Security Manager. The Primary Classified Storage area shall be the CMCC Vault located in Building 601. During non-working hours and when directed, the SDO shall:

a. Attempt to contact CMCC personnel and the Security Manager using the Emergency Recall Roster (located in the SDO Binder).

b. The Security Manager or Assistant Security Manager 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.

d. Post a military police 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.

5. Emergency Protection. Emergency protection actions include collecting all classified material not needed for immediate operational use and securing them in the CMCC Vault and safe. Emergency protection procedures will only be

executed when directed by the CO, Security Manager, or other competent authority.

a. All classified material shall be locked up in the safe.

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

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

6. Emergency Destruction Plan for COMSEC. When a hostile action occurs, the decision to enact the complete emergency destruction plan shall be made by the CO, Security Manager, SDO, or senior officer present. Utilizing the CMS Accountable Items Summary (located in the Chronological file), account for all material prior to destruction. Once all material has been accounted for destroy the following material, in the order listed below, using the shredder located in the CMS vault. Depending on the situation and present location of classified COMSEC material involved, the CMCC shredder is the most expeditious and complete method of ensuring destruction. Destruction priorities begin with CMCC safe 1.

a. COMSEC Keying Material Marked "CRYPTO"

(1) All primary keying material designated "CRYPTO" except tactical operations and authentication codes classified SECRET or below.

(2) Current effective keying material designated "CRYPTO" including key stored electronically in crypto equipment and fill devices.

(3) Superseded tactical operations codes classified SECRET or below.

(4) SECRET and CONFIDENTIAL multi-holder keying material marked "CRYPTO" which will become effective within the next 30 days.

(5) All remaining classified keying material, authentication systems, and maintenance or sample keys.

b. COMSEC Aids

(1) Complete crypto-maintenance manuals or their sensitive pages. When there is insufficient time to completely destroy these manuals, make every reasonable effort to destroy their sensitive pages, which are either marked or tabbed. Otherwise the complete manual is to be destroyed.

(2) National, department, agency, and service general doctrinal guidance publications.

(3) Keying material holder lists and directories.

(4) Remaining classified documents.

c. Equipment

(1) Make a reasonable effort to evacuate equipment, but the immediate goal is to render it unusable and unrepairable.

(2) If the keying element on crypto equipment cannot be physically withdrawn by turning the knob or pressing the zerorize button.

(3) Remove and destroy readily removable classified elements (e.g. printed circuit boards).

(4) STE phones will be zerorize and evacuated if possible.

(5) The Management Client Node (MGC) computer and all data contained on the hard drives is classified. If the computer cannot be evacuated then the hard drives are removed and rendered useless by a hammer.

(6) If Advance Key Processor (AKP) is not capable of being evacuated, you must zerorize AKP. Never zerorize during a drill!