



UNITED STATES MARINE CORPS

MARINE CORPS AIR STATION
BEAUFORT, SOUTH CAROLINA 29904-5001

ASO 5510.11J
CMCC
12 APR 2012

AIR STATION ORDER 5510.11J

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

Subj: INFORMATION, PERSONNEL AND INDUSTRIAL SECURITY PROGRAM

Ref: (a) SECNAV M-5510.36
(b) SECNAV M-5510.30
(c) OPNAVINST C5510.101D
(d) MCO P5510.18A
(e) National Industrial Security Program Operating Manual
(f) MARADMIN 624/08

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 Security Program pursuant to the guidelines established in references (a) through (d).

2. Cancellation. ASO 5510.11H.

3. Mission

a. This Order implements local command policy and guidance for the Station Security Manager, Station Classified Material Control Center, Secondary Control Points (SCP), and personnel granted access to classified material, by providing a uniform method for maintenance and control of classified material, and the management of an effective information and personnel security program.

b. This Order has been completely revised and should be reviewed in its entirety.

4. Execution

a. Department/Division Heads, and Secondary Control Points will review and, to the greatest extent applicable, follow the guidance contained in this Order.

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

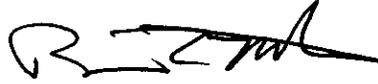
5. Administration and Logistics. Not applicable.

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

12 APR 2012

6. Command and Signal

- a. Command. This Order is applicable to the Marine Corps Reserve.
- b. Signal. This Order is effective the date signed.



B. C. MURTHA

DISTRIBUTION: A

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 1	BASIC POLICY AND APPLICABILITY.....	1-1
1.	BASIC POLICY.....	1-1
2.	RESPONSIBILITIES.....	1-1
3.	APPLICABILITY.....	1-1
4.	DEFINITIONS.....	1-1
Chapter 2	PROGRAM MANAGEMENT.....	2-1
1.	INSPECTION PROGRAM.....	2-1
2.	MANAGEMENT OFFICIALS.....	2-1
3.	INVENTORY OF CLASSIFIED MATERIAL.....	2-1
4.	DISSEMINATION OF CLASSIFIED MATERIAL AND CONTROLLED INFORMATION.....	2-2
Chapter 3	SECURITY EDUCATION.....	3-1
1.	BASIC POLICY AND RESPONSIBILITIES.....	3-1
2.	SCOPE.....	3-1
3.	PRINCIPLES.....	3-1
4.	TYPES OF BRIEFINGS.....	3-1
Chapter 4	THREATS TO SECURITY.....	4-1
1.	GENERAL.....	4-1
2.	PRELIMINARY INQUIRY.....	4-1
3.	INVESTIGATION.....	4-1
4.	REPORT OF FINDING OF CLASSIFIED MATERIAL PREVIOUSLY REPORTED AS LOST.....	4-1
5.	SECURITY VIOLATIONS.....	4-1
Chapter 5	CONTROL, PRODUCTION, ISSUE, AND DESTRUCTION OF CLASSIFIED MATETERIAL.....	5-1
1.	GENERAL.....	5-1
2.	RESPONSIBILITY.....	5-1
3.	REPRODUCTION AND PHOTOGRAPHY OF CLASSIFIED MATERIAL...	5-1
Chapter 6	PHYSICAL SECURITY OF CLASSIFIED MATERIAL.....	6-1
1.	GENERAL.....	6-1
2.	USER RESPONSIBILITY.....	6-1
3.	PHYSICAL SECURITY MEASURES.....	6-1
4.	STORAGE OF CLASSIFIED MATERIAL.....	6-2
5.	COMBINATION CHANGES AND REPAIRS TO SECURITY CONTAINERS	6-2
6.	REPAIRS OF DAMAGED SECURITY CONTAINERS.....	6-2
7.	PHYSICAL SECURITY INSPECTIONS, EVALUATIONS, AND SURVEY	6-2

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 7	TRANSMISSION OF CLASSIFIED MATERIAL.....	7-1
1.	GENERAL.....	7-1
2.	TRANSMISSION.....	7-1
Chapter 8	VISITOR CONTROL.....	8-1
1.	VISITOR CONTROL.....	8-1
2.	IDENTIFICATION.....	8-1
3.	VISITOR RECORDS.....	8-1
Chapter 9	PERSONNEL SECURITY INVESTIGATION, CLEARANCE, AND ACCESS PROGRAM.....	9-1
1.	GENERAL.....	9-1
2.	PERSONNEL SECURITY INVESTIGATION.....	9-1
3.	REQUESTS FOR PERSONNEL SECURITY CLEARANCE AND ACCESS.....	9-1
4.	VERIFICATION OF SECURITY INVESTIGATIONS.....	9-1
5.	ACCESS.....	9-1
6.	ADMINISTRATIVE TERMINATION OF CLEARANCES.....	9-1
7.	CONTINUOUS EVALUATION.....	9-2
Chapter 10	EMERGENCY ACTION PLAN.....	10-1
1.	NATURAL DISASTER.....	10-1
2.	HOSTILE ACTIONS.....	10-2
3.	TERRORIST ACTIONS.....	10-3
4.	EMERGENCY EVACUATION.....	10-4
5.	EMERGENCY PROTECTION.....	10-7
6.	EMERGENCY DESTRUCTION PLAN FOR COMSEC.....	10-8

12 APR 2012

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 SECNAV M-5510.30A and SECNAV M-5510.36. The references can be viewed or downloaded at www.navysecurity.navy.mil.

2. Responsibilities

a. The Commanding Officer and department heads are directly responsible for the safeguarding of classified information within their commands and for the proper instruction of their personnel in security procedures and practices.

b. Each individual on the Air Station, military or civilian, is responsible for the security of classified information to which access has been granted. Each individual is responsible for reporting any violations of security regulations or security weaknesses to the Commanding Officer, Security Manager, or supervisor.

3. Applicability. This Order establishes the procedures of policies of the current editions of the references and will be implemented at MCAS Beaufort.

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 preclude the individual from gaining knowledge or possession of such classified material. Access is granted based on the individual's "NEED-TO-KNOW."

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.

ENCLOSURE (1)

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 Installation Security Manager.

i. Security Manager. A person designated, in writing, by the Commanding Officer, MCAS Beaufort as the principal staff advisor on information security. The Security Manager serves as the Commanding Officer's direct representative in matters pertaining to the security of classified information.

j. Assistant Security Manager or Security Assistant. A person designated, in writing, by the Commanding Officer to assist the Security Manager in matters pertaining to the security of classified information.

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

l. Communications Security (COMSEC). Communications security (COMSEC) ensures the security of telecommunications, confidentiality, and integrity - two information assurance (IA) pillars. Generally, COMSEC may refer to the security of any information that is transmitted, transferred, or communicated.

Chapter 2

Program Management

1. Inspection Program. The Commanding Officer's Inspection Program (COIP) has established a requirement for review and inspection procedures to evaluate the effectiveness of the Information Security Program. These inspections will 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 Officials. The Security Manager will be appointed in writing. He or she assists the Commanding Officer in fulfilling the latter's responsibilities for the protection of classified information being guided by the references. The Security Manager will:

a. Serve as the Commanding Officer'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 Department of Defense (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 will be conducted annually by the Security Manager. Such inventories will involve a reconciliation to ensure that all material received by the command is actually on hand and administrative records are current and accurate. This inventory will also serve as "Clean up day" in which material no longer

ENCLOSURE (1)

12 APR 2012

required will be identified. However, COMSEC material will be inventoried on a more frequent basis.

b. Frequency of Inventory. Inventories will 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 absences (UA) status for 48 hours.
- (4) COMSEC will be inventoried bi-annually (February and August), or after the change of Commanding Officer or Electronic Key Management System (EKMS) Manager.

4. Dissemination of Classified and Controlled Information. Dissemination of classified information outside of the command must be approved by the Commanding Officer 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 (IPO). At times we will have officials of a foreign government visiting the command to inspect surplus equipment or monitor the repair process of equipment. At no time will foreign nationals be given access to classified information without the approval of the Commanding Officer or Security Manager.

ENCLOSURE (1)

12 APR 2012

Chapter 3

Security Education

1. Basic Policy and Responsibilities. The Security Manager will be responsible for establishing and maintaining an active security education program to instruct personnel in 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 SECAVINST M-5510.30.

3. Principles. The security education program will 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 will ensure that the following briefings are conducted:

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

b. Initial Security Brief. An initial security brief will 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 Naval Criminal Investigative Services Office.

e. Debriefing. Debriefing will be conducted on those occasions listed in reference (b).

ENCLOSURE (1)

ASO 5510.11J
38 APR 2012

f. Supervisors must assure themselves that subordinates know the security requirements impacting on their duties. Just "assuming" they know is what precipitates compromise of information. On-the-job training by supervisor and leaders will cover such aspects as to the proper use of SF 701, SF 702, local access procedures for the work area, and protection of classified information when not secured.

ENCLOSURE (1)

12 APR 2012

Chapter 4

Threats to Security

1. General. The compromise of classified information presents a threat to national security. The seriousness of that threat must be determined and measures taken to negate or minimize the adverse effect of the compromise. Any member of this Installation becoming aware of the compromise of classified information or material will immediately notify the Security Manager. When classified material has been reported as compromised, or subjected to compromise, action shall be initiated to accomplish the following objectives:

a. Regain custody of the material, if feasible, and afford it proper protection.

b. Evaluate the information compromised, or subjected to compromise, to determine the extent of potential damage to national security and take action as necessary to minimize the effects of the damage.

c. Discover the weakness in security procedures that caused or permitted the compromise, or susceptibility to compromise, and revise procedures as necessary to prevent recurrence.

2. Preliminary Inquiry. Upon receipt of a report of a compromise or suspected compromise, the Security Manager will immediately take those actions required by reference (a).

3. Investigation

a. If determination is made that a compromise took place or that the probability of identifiable damage to national security cannot be discounted, significant security weakness is revealed, or punitive action is appropriate, a JAG Order investigation will be initiated per reference (a).

b. The results of a JAG Order investigation will be delivered to the Commanding Officer (Attention: Security Manager) within 30 days after notification of the preliminary inquiry that identified the need for additional investigation.

4. Report of Finding of Classified Material Previously Reported as Lost. When classified material previously reported as lost is later found and the circumstances show that there has been no compromise, this fact shall be reported to all who had been notified of the loss. If, when the material is found, indications are that damage to the national security cannot be discounted, the requirements outlined in reference (a) apply.

5. Security Violations

a. The definition of a security violation is the violation of regulations pertaining to the safeguarding of classified information that do not result in compromise or probable compromise.

b. If a container in which classified material is stored is found unlocked and unattended, or if classified material is found adrift in the absence of custodial personnel, the person making the discovery will:

ENCLOSURE (1)

12 APR 2012

(1) Assure protection of the classified material. If a security container is found open and unattended, contact the persons listed on the inside locking drawer. The person discovering the unattended material will afford the classified material proper protection.

(2) If found after normal working hours, notify the Station Duty Officer (SDO) at (843) 228-7121 who will then notify the Security Manager.

c. All cases of security violations, known or suspected, will be reported to the Security Manager for appropriate investigation.

ENCLOSURE (1)

12 APR 2012

Chapter 5

Control, Reproduction, Issue and Destruction of Classified Material

1. General. Official information classified under the provisions of this Order and the current edition of SECNAV M-5510.36 shall be afforded a level of accounting or control commensurate with the assigned classification. Accounting and control procedures must be established to ensure access is granted on "need-to know."

2. Responsibility

a. The Security Manager is responsible for ensuring the proper accounting and control of classified material within the jurisdiction of the Commanding Officer in accordance with current directives.

b. The Classified Material Control Center (CMCC) is the central office of record for classified material retained at the Air Station. The CMCC Custodian directs the operation of the CMCC. The custodian will assign control numbers to classified documents and equipment that is issued out for use from the CMCC.

c. Only the Security Manager can receipt for, transfer, or destroy classified material aboard the Installation. All users will turn in classified material to CMCC for disposal. Destruction of Secret material requires two signatures to document the destruction. Classified Naval messages retained at the Local Communications Center (LCC) are exempt from this provision.

3. Reproduction and Photography of Classified Material. Reproduction of classified material will be strictly controlled, accounted for, and afforded protection commensurate with its classification. Only the Commanding Officer or the Security Manager can authorize reproduction of classified material. Photography in areas where classified material is used or stored is prohibited.

ENCLOSURE (1)

12 APR 2012

Chapter 6

Physical Security of Classified Material

1. General. Classified information or material may be used or stored only where there are facilities and conditions adequate to prevent unauthorized persons from gaining access. The exact nature and extent of security requirements will depend on a thorough security evaluation conducted by the Security Manager.

2. User Responsibility. Users of classified material are responsible for safeguarding the material at all times and particularly for securing classified material in appropriate security containers whenever it is not in use or under supervision of authorized personnel. Users will not allow:

a. Classified material to be hidden from view in desks, cabinets, or files when not in use.

b. Discussion or viewing of classified material by unauthorized personnel.

c. Classified material to be removed from officially designated office spaces at any time for the purpose of working with such material at home.

d. Classified information to be discussed over un-secure telephone circuits.

e. Classified material to be discarded in trash receptacles.

f. Security containers, authorized for storage of classified material, to be used for the safekeeping of coffee mess funds, jewelry, narcotics, precious metals, or any other items of monetary value.

3. Physical Security Measures

a. Security Containers. The term "security container" is used herein for those safes specifically designed and approved by the General Services Administration (GSA) for the storage of classified material. A security container can readily be identified by a label on the face of the locking drawer that specifies "General Services Administration Approved."

b. Security containers specifically designated for the storage of classified material will not be used for storing unclassified items or "For Official Use Only" material.

c. Security containers that are not being used for the storage of classified material will have a statement posted on the container that reads: **"THIS CONTAINER IS NOT USED FOR THE STORAGE OF CLASSIFIED MATERIAL."**

d. Each security container will have an Optional Form 89 (OF 89) inside the locking drawer that will be filled in by the user and used to record any repairs. Any remarks on this form will be made by the Installation locksmith or Security Manager.

e. OPEN/CLOSED or OPEN/LOCKED (GSA Form or equivalent) signs will be

ENCLOSURE (1)

displayed on each security container, vault, or strong room to indicate the status of the container.

f. Security Container Check Sheet. Each security container used for storing classified material will have a Standard Form 702 (SF 702) Security Container Check Sheet posted which will be completed each time the container is opened and closed. Additionally, a second person will initial the sheet each time the container is opened or closed.

4. Storage of Classified Material

a. Storage of Secret information and material outside the CMCC is not authorized unless specifically approved by the Security Manager and is subject to physical security evaluation.

b. It is recognized that classified material may be received by a department/division without being channeled through the CMCC. When such an incident occurs, the department/division will ensure control and safeguarding of the item and immediately deliver the item to the CMCC for assignment of a control number and proper issuance.

5. Combination Changes and Repairs to Security Containers

a. Combination changes to security equipment containing classified material will be conducted by the Security Manager. Combinations will be changed when the container is first put in use, when an individual knowing the combination no longer requires access to it, unless sufficient controls exist to prevent access to the lock, and when the combination has been compromised.

b. The Standard Form 700 (SF 700) will be used to record combination changes. The CMCC will store the combination envelopes for the Local Communications Center (LCC) and Explosives Ordnance Disposal (EOD). The Local Communications Center will store the combination envelopes for the CMCC. Personnel having access to the combination must have a security clearance that is equal to the classification of the combinations.

c. The SF 700 will list all personnel who have access to the combination. The detachable portion of the combination envelope will be attached to the inside locking drawer.

6. Repair of Damaged Security Containers. The Installation locksmith is authorized to repair and replace parts on all security equipment and should be called upon when required. Under no circumstances will repairs be made or attempted by untrained personnel. All repairs or modifications must be recorded on an OF 89. A properly cleared individual will be present at all times when maintenance is performed on security containers storing classified material.

7. Physical Security Inspections, Evaluations, and Surveys

a. Security Manager Inspections. The Security Manager will conduct both announced and unannounced security inspections of activities issued classified material.

b. A security survey consists of a detailed and comprehensive examination of all facets of security, ranging from the guard force and physical security, to the internal handling and control of classified

12 APR 2012

material. The Security Manager, along with the PMO's Physical Security Section, are the only individuals who will conduct the security survey.

c. Holders of classified material will utilize the Standard Form 701 (Activity Security Checklist) to conduct a security inspection of the work area at the end of each workday.

ENCLOSURE (1)

Chapter 7

Transmission of Classified Material

1. General. Classified information shall be transmitted either in the custody of an appropriately cleared individual, or by an approved system or courier, and in accordance with reference (a).

2. Transmission. When classified material is to be transported, the following steps must be followed:

a. Only appropriately cleared personnel may act as couriers. Special handling instructions will be provided to couriers before departure. Forwarding the material via approved means is the preferred method.

b. Approval to remove classified material from the physical confines of the installation must be obtained from the Security Manager; however, should travel require an overnight stopover where there is no available government facility to store the material, the hand carrying of classified material will not be authorized.

c. The CMCC is the only place where material may be prepared for such transportation or travel. This requires the users to bring the material held by them to the CMCC for preparation to be transmitted.

d. All material being transported shall be enclosed in a suitable container such as a briefcase, courier pouch, or sealed envelope. Markings other than unit designations should not appear on the outside of the container.

e. Classified material being transported between offices aboard the installation will be enclosed within an appropriate classified material folder. The material will then be placed in an additional container to prevent others from identifying that you are carrying classified information.

12 APR 2012

Chapter 8

Visitor Control

1. Visitor Control. The activities requiring individuals to visit the Installation for a classified visit will advise the visitors to have their Security Official submit a visit request to the Security Manager for approval. The Security Manager will take appropriate steps to verify the visitor's clearance and access level through the Joint Personnel Adjudication System (JPAS) and will then approve or deny the visit. A visit request is not required for unclassified visits. If the visitor's clearance and access level cannot be verified, the Security Manager will disapprove the access request. Departments, divisions, and sections are responsible for maintaining coordination with the Installation Security Manager for the duration of the visit.

2. Identification

a. Any visitor who is authorized access to classified information must present adequate identification at the time of the visit. Users of classified material will not permit access thereto until they are satisfied as to the identity, security clearance, and "need-to-know" status of the visitor as established by the Security Manager. In no case will the CMCC or users issue classified material to a visitor without having received the verbal or written authorization of the Security Manager.

b. Access to classified material will not be permitted to foreign visitors unless specifically authorized by the Security Manager.

c. If doubt exists about granting access to any visitor, the Security Manager will be contacted for a decision.

3. Visitor Records. When personnel from the Installation are required to travel to another installation for a classified visit, the individual traveling will forward a draft copy of the OPNAV 5521/27 to the Security Manager. The Security Manager will verify the information and forward a completed visit request to the command to be visited either through JPAS or by fax.

ENCLOSURE (1)

Chapter 9

Personnel Security Investigation, Clearance, and Access Program

1. General. The Security Manager has staff responsibility for administering the Personnel Security Investigation, Clearance, and Access Program.

2. Personnel Security Investigation. No person will be given access to classified information or be assigned to sensitive duties unless a determination has been made of trustworthiness. The determination will be based on an investigation appropriate to the access required and results of a local records check that is conducted by the Security Manager.

3. Requests for Personnel Security Clearance and Access

a. Requests for personnel security clearance and access for military and civilian personnel, will be forwarded by department/division heads to the Installation Security Manager.

b. Temporary or interim clearances may be granted locally pending adjudication by the Department of the Navy Central Adjudication Facility (DONCAF). The Security Manager is authorized to grant temporary or interim clearances up to and including Top Secret.

4. Verification of Security Investigations. Verification of personnel security investigations will be conducted using the Joint Personnel Adjudication System (JPAS).

5. Access

a. Access Authority. The Security Manager may grant access up to, and including, Top Secret to military and civilian personnel provided they possess appropriate clearance eligibility.

b. The Security Manager may deny or terminate all levels of access for cause in the case of military or civilian personnel.

c. Adjudication of derogatory information concerning civilian employees and active duty military personnel falls within the responsibility of the Department of the Navy Central Adjudication Facility (DONCAF).

d. Should an allegation be so severe as to question the individual's immediate or continued access to classified material; e.g., felony charges, the Security Manager may immediately terminate the individual's access and conduct a review to terminate the individual's clearance.

e. A memorandum will be forwarded by the Security Manager to the appropriate department/division head terminating that individual's access to classified material.

6. Administrative Termination of Clearances

a. When an employee is removed, terminated, resigns, retires, or is reassigned to a position not requiring access or clearance, the Security Manager will ensure that a Security Termination Statement, OPNAV 5511/14, is executed and debriefings are conducted.

ENCLOSURE (1)

12 APR 2012

b. Individuals who transfer will be given a Security debriefing.

7. 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. 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 classified information 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 employee assistance is the key to the continuous evaluation process.

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

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

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

ENCLOSURE (1)

12 APR 2012

Chapter 10

Emergency Action Plan (EAP)

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 (EAP).

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 will immediately be informed of and admitted to the secure areas. Efforts will be made to get names and identification numbers of all emergency personnel going into secure areas or being exposed to classified or COMSEC material only after the emergency is over.

(8) The Security Manager/Assistant or Classified Custodian will, to the maximum extent possible, ensure that only emergency personnel are allowed into secure areas. When given the "ALL CLEAR" signal from emergency personnel, the vault will be locked and two guards will 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 a surveillance of the general area to prevent unauthorized persons from entering, to the best of your ability.

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.

ENCLOSURE (1)

building. Personnel will wait outside the building at a safe distance until the arrival of the military police and Explosive Ordnance Disposal (EOD) Team. The building will not be re-entered until the "ALL CLEAR" signal is given by EOD personnel.

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

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

- (1) Refining and exercising preplanned protective measures.
- (2) Ensuring personnel receive training on departmental, or agency specific protective measures.
- (3) Regularly assessing facilities for vulnerabilities and taking measures to reduce them.

b. Guarded Condition - Blue. General risk of terrorist attack. In addition to the previously outlined protective measures, the following may be applied:

- (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. Elevated Condition - Yellow. Significant risk of terrorist attacks. 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. High Condition - Orange. High risk of terrorist attacks. 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.

ENCLOSURE (1)

(1) Prior to hurricanes the Security Manager, Security Assistant, or Classified Custodian will 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 will also be secured in waterproof containers.

(2) If there is damage to the CMCC Vault from a hurricane, flood, or other phenomena, the Station Duty Officer (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 will 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 will 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 will be carried out by CMCC personnel only.

a. Stage One - Potential Threat

- (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 - Probable Threat

- (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 - Imminent Threat

- (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 (PMO) will be notified by dialing "9-1-1". Classified and COMSEC material will be secured in the CMCC safe. The safe will be locked and all classified/COMSEC material accounting records will be removed from the

ENCLOSURE (1)

12 APR 2022

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

(4) Restricting access to essential personnel only.

e. Severe Condition - RED. Severe risk of terrorist attacks. In addition to the previously outlined protective measures, the following may be applied:

(1) Assigning emergency response personnel and pre-positioning especially 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 will only be executed when directed by the Installation Commander or Security Manager. The Primary Classified Storage area will be the CMCC Vault located in Building 601. During non-working hours and when directed, the Command Duty Officer (CDO) will:

a. Attempt to contact CMCC personnel and the Security Manager using the Emergency Recall Roster (located in the CDO Binder) or the CMCC Access Roster (located on the outside of the CMCC door).

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 policeman armed guard at the vault entrance and vehicle until all classified material is loaded onto the government vehicle.

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

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 Commanding Officer, Security Manager, or other competent authority.

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

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

c. Any other protection actions deemed necessary by the Security Manager will 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 will be made by the

ENCLOSURE (1)

12 APR 2012

CO, Security Manager, or SDO (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.

a. Destruction priorities begin with CMCC safe 1 and safe 2.

b. Keying Material. (COMSEC 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.

c. 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.

d. Equipment

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

(2) Cryptographic equipment if the keying element 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 LCMS computer and all data contained on the hard drive is classified. If the computer cannot be evacuated, then at the DOS prompt type format C:. For example "c:\format c:" and answer yes to the computer prompted questions that follow.

ENCLOSURE (1)

ASO 5510.11J

12 APR 2012

(6) If KP is not capable of being evacuated, you must **Zerorize** KP.
(Never during a drill!)

ENCLOSURE (1)