



UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
POSTAL SERVICE CENTER BOX 8003
CHERRY POINT, NORTH CAROLINA 28533-0003

ASO 5510.2
MPR
10 Jan 12

AIR STATION ORDER 5510.2

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

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.36A
(b) SECNAVINST 5510.30B
(c) OPNAVINST C5510.101D
(d) MCO P5510.18A

Encl: (1) Information and Personnel Security Program Guidelines

1. Situation. To promulgate policies and procedures for the effective management, operation, and maintenance of the Marine Corps Air Station (MCAS), Cherry Point, NC, Information and Personal Security Program (IPSP) pursuant to the guidelines established in references (a) through (d).
2. Cancellation. AirStaO P5510.2A.
3. Summary of Revision. This Order has been completely revised and should be reviewed in its entirety.
4. Mission. This Order implements local command policy and guidance for the Security Manager, Classified Material Control Center (CMCC), 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.
5. Execution
 - a. Department/Division Heads, and Secondary Control Point Custodians 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, Marine Corps Air Station,

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


(Attn: Security Manager) via the appropriate chain of command for evaluation.

6. Administration and Logistics. The Security Manager is responsible for the management of the Command IPSP.

5. Command and Signal

a. Command. This Order is applicable to the Marine Corps Reserve.

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


E. S. WEISSBERGER
Executive Officer

DISTRIBUTION: A

INFORMATION AND PERSONNEL SECURITY PROGRAM

1. BASIC POLICY. The directives which provide basic guidance for the security of classified information and material are the current editions of SECNAVINST 5510.30B and 5510.36A. The references can be viewed or downloaded at www.navysecurity.navy.mil.

2. RESPONSIBILITY

a. Commanding Officer's 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 aboard MCAS Cherry Point, military or civilian, is responsible for the security of classified information to which access had been granted. Each individual is responsible for reporting to the Commanding Officer, Security Manager, or supervisor any violation of security regulations or security weaknesses.

3. APPLICABILITY. This Order establishes the procedures by which the policies of the current editions of SECNAVINST 5510.30B, SECNAVINST 5510.36A, and references (c) and (d) will be implemented aboard MCAS Cherry Point.

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 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. Classified Material Control Center (CMCC) Custodian. The individual who is designated by the Commanding Officer, MCAS Cherry Point as having the custodial responsibility for safeguarding and accounting of classified documents. This individual provides primary administrative and supervisory control over the CMCC.

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

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

g. Counterintelligence. That 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.

h. 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.

i. 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.

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

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

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

PROGRAM MANAGEMENT

1. INSPECTION PROGRAM. The Commanding Officer's Inspection Program 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 OFFICIAL. The Security Manager will be appointed in writing by the Commanding Officer and is responsible for the protection of classified information per SECNAVINST 5510.30B and SECNAVINST 5510.36A. The Security Manager will:
 - a. Serve as the Commanding Officer's advisor and direct representative in matters pertaining to 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 required to handle classified information are cleared and that all requests for personnel security investigations are properly prepared, submitted, and monitored.

 - e. Ensure that clearance status and access 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.

h. Ensure compliance with provisions of the industrial security program for classified contracts with Department of Defense (DOD) contractors.

i. Ensure security control over visitors to classified areas.

j. Manage the security education program.

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 within the command will be conducted annually by the CMCC Custodian. 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 required will be identified and properly destroyed.

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

(1) When there is a change of the CMCC Custodian.

(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 UA for 48 hours.

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 no time will foreign nationals be given access to classified information without the approval of the Commanding Officer or Security Manager.

SECURITY EDUCATION

1. BASIC POLICY AND RESPONSIBILITY. 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 security education programs is contained in the current edition of SECAVINST 5510.30B.
3. PRINCIPALS. 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 properly safeguarded.
 - 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

- a. The Security Manager will ensure that the following briefings are conducted:

- (1) Initial Security Brief. An initial security brief will be given to all individuals when they are granted access to classified information.

(2) 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. During the brief, the supervisor will address specific security requirements unique to the work area. The annual refresher briefing/training can be completed online. The training course takes approximately three hours to complete and satisfies the annual refresher briefing requirement. Once the course is completed, the individual will be prompted to create a certificate of completion. This certificate will be signed by the supervisor and forwarded to the Security Manager for retention.

(3) Naval Criminal Investigative Service (NCIS) Briefing. All personnel who have access to classified information shall receive an NCIS counterespionage briefing at least every two years. The Security Manager shall arrange for the briefing with the servicing Naval Criminal Investigative Services Office.

(4) Debriefing. Debriefing will be conducted on those occasions listed in SECNAVINST 5510.30B.

b. The supervisor must take the lead and train their subordinate personnel in the proper use and control of classified material. 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 when not secured.

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 Command 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 the 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 the national security cannot be discounted, significant security weakness is revealed, or punitive action is appropriate, a Judge Advocate General (JAG) Manual investigation will be initiated. Reference (a) outlines the requirements of the investigation.

b. The results of a JAG Manual investigation will be delivered to the Commanding Officer, Marine Corps Air Station (Attn: 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. All violations of regulations pertaining to the safeguarding of classified information that result in compromise or probable compromise must be reported to the Security Manager.

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:

(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 during nonworking hours, notify the Command Duty Officer (CDO) 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.

CONTROL, REPRODUCTION, ISSUE AND DESTRUCTION OF CLASSIFIED MATERIAL

1. GENERAL. Official information classified under the provisions of this Order and the current edition of SECNAVINST 5510.36A shall be afforded a level of accounting or control commensurate with the assigned classification. Accounting and control procedures must be established to ensure issue is based on "need-to know."

2. RESPONSIBILITY

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

b. The CMCC is the central office of record for classified material retained at MCAS Cherry Point. The CMCC Custodian directs the operation of the CMCC. The custodian will assign control numbers to classified documents and equipment that are issued out from the CMCC.

c. Only the Security Manager or CMCC Custodian can receipt for, transfer or destroy classified material. All users will turn in classified material to CMCC for disposal.

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.

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

a. 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.

b. Users will not allow:

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

(2) Discussion or viewing of classified material by unauthorized personnel.

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

(4) Classified information to be discussed over unsecure telephone lines.

(5) Classified material to be discarded in trash receptacles.

(6) Security containers, authorized for storage of classified material, to be used for the safekeeping of coffee mess funds, jewelry, narcotics, precious metals, or any item 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 (GSA) approved."

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

(2) 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."

(3) Each security container will have an Optional Form 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 Command Locksmith or Security Manager.

(4) OPEN/CLOSED or OPEN/SECURED (GSA Form or equivalent) signs will be displayed on each security container, vault, or strong room to indicate the status of the container.

b. 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.

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 without being channeled through the CMCC. When such an incident occurs, the department 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 & REPAIRS TO SECURITY CONTAINERS

a. Combination changes to security containers will be conducted by qualified personnel or the Command Locksmith. 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 all Secondary Control Points and any additional sites that may have classified storage containers (i.e., safes). The Station CMCC combination envelopes will be stored at TISD. 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 the personnel who have access to the combination and the detachable portion of the combination envelope will be attached to the inside locking drawer.

6. REPAIR OF DAMAGED SECURITY CONTAINERS. The Command 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 announced and unannounced security inspections of activities issued classified material. 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 material. The Security Manager with assistance from the Physical Security Manager in the Provost Marshall's Office (PMO) are the only individuals authorized to conduct the security survey.

b. 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.

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 SECNAVINST 5510.36A.

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 base 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 designated area where classified material may be prepared for such transportation or travel. Only cleared personnel in proper possession of classified material approved for transportation or travel will bring material to the CMCC for processing.

d. All material being transported shall be enclosed in a suitable container such as a briefcase, courier pouch, or sealed envelope. No markings other than unit designations should appear on the outside of the container.

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

VISITOR CONTROL

1. VISITOR CONTROL. Activities requiring individuals to visit MCAS Cherry Point, 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 steps to verify the visitor's clearance and access level through the Joint Personnel Adjudication System (JPAS) and will

then approve the visit. If the visitor's clearance and access level cannot be verified, the Security Manger will disapprove the access request. Departments and sections are responsible for maintaining coordination with the 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. Command authorized 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 custodian 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 Station are required to travel to another installation for a classified visit, the individual traveling will forward a draft copy of 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 by JPAS or fax.

PERSONNEL SECURITY INVESTIGATION, CLEARANCE, AND ACCESS PROGRAM

1. GENERAL. The Security Manager has staff responsibility for administering the Joint Personnel and Adjudication System (JPAS) 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 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.

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.

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

7. CONTINUOUS EVALUATION

a. Individuals. 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 play a critical role in early detection of an individual's problems. Supervisors 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 Joint Law Center (JLC) will provide the Security Manager a copy of the weekly legal report.

c. Substance Abuse Control Officer (SACO). The SACO will provide the Security Manager assistance with regards to Local Records Checks (LRC's).