

MASTER DIRECTIVES



UNITED STATES MARINE CORPS
MARINE AIRCRAFT GROUP 12
1ST MARINE AIRCRAFT WING, MARFORPAC
UNIT 37150
FPO AP 96603-7161

GruO P5510.6D
S-2
NOV 03 1999

GROUP ORDER P5510.6D

From: Commanding Officer
To: Distribution List

Subj: COMMAND SECURITY INSTRUCTION

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) Command Security Education Program
(d) CMS-21

1. Purpose. To establish security procedures within Marine Aircraft Group 12 (MAG-12) for personnel security and information security. The Command security instruction shall supplement the references, not replace them.

2. Cancellation. GruO P5510.6C.

3. Applicability

a. This order establishes policies for the security of classified material/information. This order, in conjunction with the references, will enable the user to implement and maintain an effective security program.

b. The policies and procedures in this order and its references represent the minimum security requirements for all elements of MAG-12. Commanding Officers who feel that more stringent requirements are needed to meet their unique situation will publish their own internal security directives. Those directives will only address areas where additional security is needed and will avoid duplication of effort by referencing this order.

c. This Headquarters will publish, as circumstances dictate, memoranda that interpret official policy. These memoranda will be based on questions within MAG-12 subordinate units concerning information security directives issued by higher headquarters.

d. All MAG-12 personnel are individually responsible for compliance with this order.

NOV 03 1999

3. Chain of Command

a. The Commanding Officer, MAG-12 has designated in writing all personnel responsible for the management of the information and personnel security programs within the command. The Executive Officer of MAG-12, as the Security Manager, is responsible for the overall management of both programs. Figures 1.1 shows the security chain of command and their national security positions within the headquarters of MAG-12.

Billet	Position	NSP
Commanding Officer MAG-12	Commanding Officer MAG-12	Special-Sensitive
Security Manager	Executive Officer MAG-12	Special-Sensitive
Assistant Security Manager	Intelligence Officer/Chief	Special-Sensitive
CMCC Officer	Adjutant	Critical-Sensitive
Information Systems Security Officer	Information Systems Center Officer	Critical-Sensitive
Information Systems Security Manager	Information Systems Center Officer	Critical-Sensitive
Network Security Officer	Information Systems Center Chief	Critical-Sensitive
Special Security Officer	Special Security Communications Team SNCOIC	Special-Sensitive
Top Secret Control Officer	Special Security Communications Team SNCOIC	Special-Sensitive
NBCD	NBC Officer/SNCO	Noncritical-Sensitive

Fig 1.1

4. Security Reviews and Inspections

a. MAG-12 and its subordinate units will receive an annual Functional Area Inspection (FAI) for security conducted by the Assitant Security Manager, 1ST MAW G-2. UDP squadrons will not be inspected by the MAG-12 Security Mangager due to thier short deployment period. However, UDP squadron security managers are responsible for ensuring that their respective squadrons maintain an

effective security program in compliance with the references.

b. MAG-12 Security Manager and Assistant Security Manager will conduct security inspections/reviews as stated in reference (c).

5. Counterintelligence Procedures

a. Individuals who are aware of sabotage, international terrorism, espionage, deliberate compromise or other subversive activities will report all available information concerning such activities immediately to the Security Manager or Commanding Officer at their command. NCIS will be notified immediately of any requests through other than official channels for classified or national defense information from anyone without an official need to know, regardless of nationality.

b. All personnel who possess a security clearance are to report to their Commanding Officer or Security Manager any contacts with any individual, regardless of nationality, whether within or outside the scope of the Marine's official duties, where possible activities involved illegal or unauthorized access to classified or otherwise sensitive information.

6. Security Education Program

a. The purpose of the security education program is to ensure that all personnel understand the need and procedures for protecting classified information. The goal is to develop fundamental security habits as a natural element for each task.

b. Security education must be provided to all personnel. The education effort must be tailored to meet the needs of the command as well as those of different groups within the command.

c. Commanding Officers will ensure that all personnel receive security education training semi-annually, and that adequate records are maintained indicating classes given and personnel in attendance.

d. All newly joined personnel will receive a command security orientation brief. For PSD-12, the brief will be given when the Marine checks in with the intelligence section. Marines from a subordinate command within MAG-12 will also receive the orientation brief.

7. Classification Authority

NOV 03 1999

a. The Commanding General is the only person within 1st MAW with original classification authority. MAG-12 has derivative authority to create classified material based on the inclusion of material from other classified material.

b. Any person within MAG-12 who believes that the information contained in a document is classified may assign a tentative classification to the document, mark it appropriately, and forward it up the chain of command for a determination of the appropriate classification.

8. Classifications and Marking

a. All classified material generated within MAG-12 will be properly marked or annotated in the manner specified in ref (b). Classified material refers to any product that contains classified information regardless of form.

b. Since MAG-12 does not have original classification authority, the majority of any classified information that the command uses will come from the CMCC to individuals or designated SCPs. Any working papers must be marked as such and have a "created date" and "destroy date" on them. Such documents must be protected in the same manner as information classified at the same level.

c. The command will publish a group bulletin at the beginning of November for an annual "clean out" day. On "clean out" day all classified material no longer required will be destroyed and the destruction reports turned into the Group CMCC within five working days.

d. Classified information provided to MAG-12 by foreign governments and international organizations will be assigned a classification that assures equivalent protection in English.

9. For Official Use Only (FOUO) Information. All official unclassified material such as rosters, letters, messages and reports, will be shredded or burned. Under no circumstances will FOUO material be placed in trashcans. Trashcans will hold only trash items such as soda cans, gum wrappers, food wrappers etc.

10. Reproduction

a. Classified material will only be reproduced when

NOV 03 1999

operationally necessary. Reproduction of classified material up to secret will only be done in designated sections on approved copiers. Within the MAG headquarters the approved location is the S-2 section. Reproduction of classified information higher than secret must have the approval of the Top Secret Control Officer and Special Security Officer prior to the reproduction.

b. For TS or higher classification, the Special Security Communications Team Detachment is the only approved reproduction facility. All reproduction facilities must have a logbook that will be filled out prior to reproducing any classified information. For electronic "soft copies" of classified material, the computer being used must be designated for the appropriate level of classification. Due to the magnitude of the security risks involved when dealing with electronic media, copies will only be made when deemed absolutely necessary. Prior arrangements should be made with the MAG-12 S-2, SSCT, or CMCC, which have computers designated for the handling of classified material.

11. Safeguarding Classified. In addition to the basic policy set forth in the references, the following additional procedures shall be adhered to within MAG-12:

a. All sections that store, use or disseminate classified information will do a security sweep of their area at the end of each workday utilizing an activity security checklist (SF 701). This checklist can be locally generated to meet individual command requirements; however, a copy must be turned in to CMCC.

b. A security container check sheet (SF 702) will be utilized on every entry/exit point where classified information or system is stored.

c. All workspaces that use classified material will ensure that red "message handling boxes" are used exclusively for classified material and that those boxes are emptied at the end of each work day.

d. All STU-III phones are maintained and managed by the EKMS manager as per ref (d), chapter 16. This also includes STU-III keying material.

e. The only two facilities within PSD-12 that are authorized to fax classified material are the intelligence section and Special Security Communications Team (SSCT)

buildings. Each subordinate command can designate their own classified faxes per ref (b).

f. Only authorized personnel may change combinations on any container holding classified information. The CMCC will maintain a copy of all classified container combinations, with the exception of all CMS and SSCT containers. CMS classified container combinations will be maintained in the SSCT facility. SSCT combinations are maintained within the SCIF of 3D SSCT, Camp Foster, Okinawa, Japan. Combinations will be changed within 24 hours upon transfer of personnel with access to the container, or annually.

g. When unrecognized personnel enter a classified facility, all classified material will be secured to avoid accidental disclosure.

h. Destruction of secret classified material will be annotated with a destruction report which will be maintained for two years. A copy of all destruction reports will be turned in to the Group CMCC. All destruction of classified material will be done by the CMCC.

12. Hand Carrying Classified Material

a. Any personnel who are hand carrying classified material will have a courier card. The courier will not transport any classified materials with a higher classification than what his courier card states. Couriers are not authorized to open, inspect, or read any classified material in their possession. Limited viewing is authorized when accounting for material. All classified material will be double wrapped with the inner envelope stamped with the highest classification of the document. Transportation of classified material aboard commercial transportation is prohibited unless approved by the Commanding Officer.

b. Only those indoctrinated by Special Security Officer, MAG-12 and possessing an ONI 5510/7 (4-98) Sensitive Compartmented Information courier card may courier SCI.

13. Protection of Classified While in a Travel Status. Any personnel that carry classified material during travel status must be authorized recipients of a courier card with a classification commensurate (or higher) to the material they are carrying. Material must remain in the couriers possession at

all times. Material should only be exposed for accountability purposes only. In the event the courier must stay somewhere overnight, the classified material will be placed in a safe authorized to safeguard classified information. This safe must be located on a military reservation.

14. Key Control Program. Keys to areas that maintain classified material are to be maintained by that area. In the event that a squadron is vacating an office area, the keys will be given to CMCC at MAG-12 for control until the new squadron is on board.

15. Procedures for Emergency Access to Locked Security Containers

a. In the event that combinations are needed to a workspace that falls under MAG-12, excluding spaces that contain Top Secret material, they are held in the CMCC office of MAG-12. These combinations can be given to personnel who are listed on the SF 700.

b. In the event that Emergency Access is required to Det SSCT spaces and Det SSCT Marines are unavailable, contact will be made to 3D SSCT in Okinawa, Japan.

16. Conduct of Classified Meeting. MAG-12 personnel who sponsor classified meetings must comply with the requirements in references (a) and (b). The section hosting the meeting has the responsibility for security and will ensure the following:

a. All attendees will be checked at the door to ensure that they are on the meeting clearance roster. The roster must be maintained for at least one year.

b. All personnel who plan on attending the meeting must fax their clearance information with the signature of their Security Manager or Assistant Security Manager. No one is authorized to hand carry their own clearance information.

c. The room in which the meeting is to be held shall be cleared of all personnel who lack the appropriate security clearance for the level of classified information to be discussed or who do not have a need to know.

d. The room in which the meeting is to be held must have has been cleared for use as a classified meeting area.

NOV 03 1999

e. All classified notes and handouts will be controlled per their level of classification. Any classified notes, handouts or briefs leaving the command must be processed through CMCC.

17. Automated Information Systems

a. All automated information system users must exercise extreme care to ensure that classified material is never processed on an unclassified system.

b. All SIPRNET users must receive a mandatory security briefing prior to being issued an account. In order to have a SIPRNET account setup within MAG-12 each individual must fill out and sign the SIPRNET LAN account request form, MAG-12 S-2 and S-6 have the necessary forms. SIPRNET users can only access the network on the designated machines in the SSCT, S-2 and S-3 buildings. Commands that utilize the AT&T 1910 SDD for access to the SIPRNET must have:

(1) An access list for all personnel who are authorized to use the 1910. This list will include individual security clearance information. A copy must be provided to MAG-12 S-2.

(2) A letter that designates the computer, which is to be used in conjunction with the 1910, as authorized to process classified information. A copy of the letter must be provided to MAG-12 S-2.

(3) Both computer and 1910 must be located in a secure area per ref (b).

c. For systems processing SCI, only SSO DIA is the approving authority. See the SSO for specific details.

18. Command Visitor Control

a. Commanding Officers are authorized to approve requests for official visits to their commands. Copies of visit requests to squadrons will be forwarded to the MAG-12 Security Manager at least five days prior to the visit.

b. Requests for visits to the MAG-12 headquarters will be coordinated by that staff section, the Assistant Security Manager and the intelligence section for security clearance verification.

c. The intelligence section will maintain a visitor control logbook which will include, at the minimum, the following:

Full Name
SSN/Nationality
Clearance Info
Parent Unit/Organization
Purpose of Visit
Hosting Unit/Section
Visit Dates

d. All unofficial visits to MAG-12 will be on an unclassified basis only. Commanding Officers and individual sections will ensure that visitors do not enter into restricted areas and are not exposed to classified information.

e. All visitors who require access to restricted areas must be escorted by appropriately cleared personnel.

19. Reporting and Investigating Loss or Compromise. The basic policy for loss or compromise of classified information is that it presents a threat to the national security of the United States.

a. Reports of loss or compromise ensure that such incidents are properly investigated and proper actions are taken to negate or minimize any adverse effects of the loss or compromise and to preclude recurrence of similar incidents. The definitions of loss and compromise are:

(1) A loss of classified information occurs when classified items cannot be physically located or accounted for.

(2) A compromise is the unauthorized disclosure of classified information to a person who does not have a valid clearance, authorization access or need-to-know.

b. The individual who becomes aware that classified information is lost or compromised shall immediately notify the Assistant Security Manager, Security Manager or Commanding Officer.

20. Personal Security

a. All personnel who require a security clearance must check in with the intelligence section. At that time,

GruO P5510.6D
NOV 03 1999

procedures to grant access to classified information will be initiated.

b. Personnel who are preparing to execute PCS or PCA orders, must check out with the intelligence section. At that time, the intelligence section will provide a copy of the person(s) adjudicative message.

21. Continuous Evaluation Program. All personnel with access to classified information are automatically on the Command's continuous evaluation program.


J. F. FLOCK

DISTRIBUTION: A