



UNITED STATES MARINE CORPS  
1ST MARINE AIRCRAFT WING, FMF PACIFIC  
APO SAN FRANCISCO 96307-0701

WgO 2230.1F  
18  
27 JAN 1992

WING ORDER 2230.1F

From: Commanding General  
To: Distribution List

Subj: COMMUNICATIONS SECURITY (COMSEC)

Ref: (a) ACP-122  
(b) CINCPACFLT OPORD 201 Annex K  
(c) FMFPacO 2230.1E  
(d) JANAP 119  
(e) CSP-1  
(f) OPNAVINST C5510.93B  
(g) OPNAVINST 5510.1E  
(h) Pacific Fleet Radiotelephone Users Manual (ROM)  
(i) MCO 2231.3  
(j) PNFPM 3-30

Encl: (1) COMSEC Definitions and Terms  
(2) Essential Elements of Friendly Information (EEFI)  
(3) COMSEC Programs  
(4) Communications Security Inspections/Checklist  
(5) Secure Telephone Unit (STU)-III Usage

1. Purpose. To establish COMSEC policy and objectives for the 1st Marine Aircraft Wing (MAW), provide guidance for planning, and assign responsibilities necessary to accomplish COMSEC.

2. Cancellation. WgO 2230.1E.

3. Summary of Revision. This Order has been thoroughly revised and should be reviewed in its entirety.

4. General. Communications Security is a responsibility of command at all echelons. References (a) through (j) set forth policy, objectives and guidance for planning and executing communications security programs. Enclosure (1) provides applicable definitions and terms.

a. Discussion of classified and sensitive unclassified information over unsecure circuits is prohibited. Encryption is the best defense against hostile communication intelligence efforts. Other COMSEC measures include authentication systems, transmission security techniques, TEMPEST inspections (reference (f)), and operator discipline.

b. Telephone conversations are a particularly lucrative source of information. The Secure Telephone Unit, Type III (STU-III), when properly keyed, enhances communications security by protecting

27 JAN 1992

classified and sensitive communications through the Defense Switched Network (DSN) and commercial telephone networks. Conventional telephones offer no such protection. All government-owned or leased administrative telephone systems are subject to COMSEC monitoring.

#### 5. Policy

a. Communications security measures shall be continuously reviewed and evaluated to identify weaknesses which can be exploited.

b. Communications security shall be an integral part of planning, unit training, and daily operations at all echelons of command.

c. Commanders shall periodically analyze their COMSEC postures to ensure that the highest level of communications security awareness is maintained.

d. All communications users shall have a thorough knowledge of the various measures required to ensure COMSEC. The guidance contained in references (a) through (c) pertains and its application is required for effective security.

e. Caution and diligence shall be exercised by all personnel to ensure that classified or sensitive information is not discussed over radios, telephones, or other electrical means unless protected by cryptographic devices (see enclosure (2)).

f. Where secure communications are not available, authorized manual codes and authentication systems shall be used to the maximum extent practicable.

g. Use of unprotected tactical teletypewriter circuits is prohibited; on-line cryptographic equipment is available.

h. Callwords are allocated by reference (d) and assigned by CG, 1st MAW (G-6). Neither unit nicknames nor locally fabricated callwords are authorized. Unit Deployment Program squadrons may continue to use their parent MAW or Brigade JANAP-119 assigned callwords.

6. Objective. Achieve the highest degree of COMSEC possible. The ultimate goal is to provide total security for all information transmitted electrically by the means outlined in enclosure (3).

#### 7. Action

a. Assistant Chief of Staff, G-2. Conduct annual inspections of cryptographic facilities per reference (c).

b. Assistant Chief of Staff, G-6

(1) Assigned duties as COMSEC Officer, 1st MAW.

(2) Coordinate with the AC/S, G-2 and AC/S, G-3 regarding command, control, and communications countermeasures (C3CM).

(3) Conduct COMSEC inspections using enclosure (4).

(4) Coordinate all communications monitoring requirements.

c. Commanding Officers

(1) Comply with the policy and guidance provided by this Order, and references (a) through (j).

(2) Ensure subordinate units are cognizant of all COMSEC material for which they are designated as "controlling authorities."

(3) Promulgate a unit COMSEC order outlining policy and procedures.

(4) Establish an effective COMSEC indoctrination and training program, incorporating the guidance in enclosures (3) and (4).

(5) State formal COMSEC requirements as an integral part of all operations plans, orders, and procedures.

(6) Appoint, in writing, an organizational COMSEC Officer who will monitor COMSEC operations and requirements.

(7) Ensure that communications operators are trained in electronic counter-countermeasures and the use of authorized codes and authentication systems per reference (h).

(8) Ensure that all personnel answering telephones include in their initial response the phrase, "...THIS IS NOT A SECURE LINE..." Personnel should not attempt to "talk around" classified matters.

(9) Ensure that available COMSEC equipment is used to the maximum extent possible during both training and operations.

(10) Ensure that STU-III's are used to the maximum extent and always in the secure voice mode. Reallocate STU's as necessary to ensure ready accessibility by those who need to discuss operational matters on a daily basis (see enclosure (5)).

(11) Ensure that only authorized call signs, codes, and authentication systems are used.

(12) Provide physical security for COMSEC material per references (e) and (g).

(13) Report COMSEC violations and practices dangerous to security which involve COMSEC material per reference (g).

WgO 2238.1P

27 JAN 1992

(14) Ensure Emergency Action Plans are established and training conducted.

  
J. R. MURRAY  
Chief of Staff

DISTRIBUTION: LIST 1/3

COMSEC DEFINITIONS AND TERMS

1. Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JCS Pub 1-82)
2. Crypto-Security. The component of communications security which results from the provision of technically sound crypto-systems and their proper use. (JCS Pub 1-82)
3. Transmission Security. The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (JCS Pub 1-82)
4. Emission Security. The component of communications security which results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. (JCS Pub 1-82)
5. Physical Security. The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JCS Pub 1-82)
6. Beadwindow/Gingerbread. Procedures used to maintain security on voice circuits. Beadwindow procedures are defined and explained in CINCPACFLTPOPOD 281 Annex K. The term "Gingerbread" is used to alert stations that imitative deception or intrusion is suspected on a voice circuit (Pacific Fleet Radiotelephone Users Manual pertains).
7. Meaconing. A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (JCS Pub 1-82)
8. Electromagnetic Intrusion. The intentional insertion of electromagnetic energy into transmission paths in any manner with the objective of deceiving operators or causing confusion. (JCS Pub 1-82)
9. Electronic Jamming. The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment, or systems. (JCS Pub 1-82)

ENCLOSURE (1)

27 JAN 1992

10. Electromagnetic Interference. Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like. Also called EMI. (JCS Pub 1-82)

11. TEMPEST. An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanation," (e.g., TEMPEST tests, TEMPEST inspections). (OPNAVINST C5518.93)

12. Electronic Warfare (EW). Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. (JCS Pub 1-82)

13. Electronic Countermeasures (ECM). That division of electronic warfare involving actions taken to prevent or reduce an enemy's effectiveness of the electromagnetic spectrum. Measures include jamming and deception. (JCS Pub 1-82)

14. Electronic Counter-Countermeasures (ECCM). That division of electronic warfare involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of electronic warfare. (JCS Pub 1-82)

15. Command, Control, and Communications Countermeasures (C3CM). Command, control, and communications countermeasures is the integrated use of operations security, military deception, jamming, and physical destruction supported by intelligence to deny information to, influence, degrade, or destroy adversary C3 capabilities and to protect friendly C3 against such actions. There are two divisions within C3CM:

a. Counter-C3. Measures taken to deny adversary commanders and other decision makers the ability to command and control their forces effectively.

b. C3-Protection. Measures taken to maintain the effectiveness of friendly C3 despite both adversary and friendly counter-C3 actions. C3-Protection includes, but is not limited to, ECCM, Signals Security (SIGSEC), emission control, signature reduction, physical security, and terrain masking. C3-Protection incorporates no new techniques or programs, but emphasizes the requirement to focus increased attention on the protection of friendly C3. (JCS Pub 1-82)

ENCLOSURE (1)

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI)

1. The EEFI identifies specific items of information which, if acquired by an enemy, would degrade the security of military operations. Secure telephones are not always available; consequently, the administrative telephone system and DSN are used. Routine conversations are lucrative sources of information to an enemy. When using a nonsecure telephone, ensure these EEFI are not discussed:

<u>Number</u>	<u>Description</u>
#1 POSITION	Friendly or enemy position, movement or intended movement: position, course, speed, altitude or destination of any air, sea, or ground element unit or force.
#2 CAPABILITIES	Friendly or enemy capabilities or limitations: force composition or identity, capabilities, limitations or significant casualties to special equipment, weapon systems, sensors, units or personnel. Percentage of fuel or ammunition remaining.
#3 OPERATIONS	Friendly or enemy operations, intentions, progress or results: operational or logistic intentions, assault objectives, mission participants, flying programs, mission situation reports, or results of friendly or enemy operations.
#4 ELECTRONIC WARFARE	Friendly or enemy EW/EMCON intentions, progress or results: intention to employ ECM, results of friendly or enemy ECM, objectives of ECM, results of friendly or enemy ECCM, results of ESM, present or intended EMCON policy, equipment affected by EMCON policy.
#5 PERSONNEL	Friendly or enemy key personnel: movement or identity of friendly or enemy flag officers, distinguished visitors, unit commanders, or movement of key maintenance personnel indicating equipment limitations.
#6 COMMUNICATION SECURITY	Friendly or enemy COMSEC locations: linkage of codes or codewords with plain languages, compromise of changing frequencies or linkage of changing call signs with previous call signs or units. Compromise of encrypted/classified call signs, incorrect authentication procedures.

ENCLOSURE (2)

COMSEC PROGRAMS

1. General. The key to achieving an adequate COMSEC posture is establishing aggressive COMSEC programs for all communication users.

a. The goal is to provide an understanding of the COMSEC threat, how to counter it, and the consequences of poor COMSEC.

b. Programs shall include: Physical Security, Transmission Security, Crypto Security, and Emission Security.

2. Indoctrination Program. All Marines shall be educated regarding the necessity for security measures through organizational indoctrination programs. Previous COMSEC training shall be supplemented and reemphasized continually to maintain a high state of awareness. All Marines shall be indoctrinated on the vulnerabilities of electrical transmissions, especially voice transmissions.

3. Training Program

a. COMSEC training programs shall support the following objectives:

(1) Providing, through transmission security practices, effective defenses against imitative communications deception.

(2) Protecting COMSEC material/systems from compromise.

(3) Emphasizing COMSEC training and awareness.

(4) Conducting COMSEC indoctrination for all personnel.

(5) Monitoring and evaluating communications for weaknesses and deficiencies and applying corrective action. This includes:

(a) Emission security analysis.

(b) Inspections of telecommunication and crypto-center facilities.

(c) Communications security critiques listed in exercise and operation after-action reports.

(6) Using communications equipment with authorized crypto systems.

(7) Promptly disseminating COMSEC guidance furnished by higher authority.

ENCLOSURE (3)

(8) Identifying and providing encryption devices to secure telecommunications circuits, especially voice, that are particularly vulnerable to COMSEC violations.

(9) Adhering to approved installation criteria to limit interaction between classified and unclassified signal lines, grounds, equipment and systems.

(10) Using low-level keying and signalling for all equipment and systems when practicable.

(11) Installing equipment/systems within shielded enclosures.

b. Communication Users Training Program. As a minimum, this program shall:

(1) Identify the types of information that require protection.

(2) Describe and identify various COMSEC measures available.

(3) Identify the types of threats and initiate applicable countermeasures.

(4) Describe reportable security violations and methods for reporting possible compromises and practices dangerous to security.

c. Occupational Field 25 Training Program. As a minimum, the program shall:

(1) Ensure proficiency in installing, operating and maintaining COMSEC equipments and systems.

(2) Stress the need for transmission security and how to take definitive actions such as adhering to proper operation and security procedures, reduction of transmission time, circuit discipline, etc..

(3) Train operators to properly safeguard COMSEC equipment and material. Proper accounting will also be explained.

(4) Include completion of Pacific Fleet Radiotelephone Users Manual by each student.

(5) Ensure proficiency is maintained in the operation of over-the-air-rekeying (OTAR).

ENCLOSURE (3)

27 JAN 1992

COMMUNICATIONS SECURITY INSPECTIONS/CHECKLIST

1. Inspections. Inspections provide one of the best means of follow-up on COMSEC programs to determine progress and to identify weaknesses. As a minimum, the following command inspections are required:

- a. An annual inspection of cryptographic facilities.
- b. A semiannual inspection of cryptographic equipment/material users' training records to ensure COMSEC training is being conducted.
- c. A quarterly proficiency test by unit COMSEC officers in which applicable communications nets are established using personnel and equipment selected at random.
- d. A quarterly inspection by unit COMSEC officers of COMSEC equipment records to ensure authorized modifications are completed and preventive maintenance records are current.
- e. A quarterly inspection of CMS vaults, conducted by both the unit COMSEC officer and CMS custodian, to ensure equipment and software on hand is actually required, properly reported, and maintained.

2. Checklist

- a. Is the COMSEC Officer appointed in writing?
- b. Does the COMSEC Officer have a turnover folder and/or desk top procedures?
- c. Does the unit have a COMSEC order or SOP?
- d. Does the order/SOP:
  - (1) Identify training goals/objectives for each functional area of communications security?
  - (2) Provide guidance and direction related to TEMPEST?
  - (3) Provide guidance and direction related to methods of conducting communications security training?
- e. Are procedures in effect to indoctrinate newly joined Marines regarding:
  - (1) The type of information which must be protected.
  - (2) The consequences of inadequate COMSEC.

ENCLOSURE (4)

27 JAN 1992

(3) The techniques and means available to protect information during electrical transmission.

(4) The location and operation of secure voice communications terminals (i.e., STU-III), within their unit and/or higher headquarters.

f. Does the COMSEC Officer review COMSEC equipment modification control records to ensure modifications have been applied to all existing equipment?

g. Does the COMSEC Officer review all exercise COMM PLANS to ensure COMSEC established procedures are addressed and identified for physical security, transmission security, emission security and crypto security?

h. During exercises, does the training schedule reflect training in the area of COMSEC?

i. What VHF/UHF/HF nets are not covered by cipher devices? Why not?

j. Are operators familiar with instructions for the use of manual authentication?

k. Has the unit requested training visits from NIS, NAVSECGRU, or radio battalion?

l. Does the COMSEC Officer review and assist in the revising of all emergency action plans held within the unit?

m. Is the COMSEC Officer knowledgeable in all reporting procedures related to security violations and compromises?

n. Does the COMSEC Officer review monthly and quarterly unit training plans to ensure adequate COMSEC training is both scheduled and conducted in communications security?

(1) Is a COMSEC required reading program in effect within the unit?

(2) Is a review of proficiency/qualification tests conducted on crypto maintenance personnel?

(3) Is a review conducted of crypto operators' qualifications records?

o. Does the COMSEC Officer review all lesson plans prepared for communications security training?

p. Has the unit established an active COMSEC monitoring program on unsecure voice radio circuits? Are logs maintained?

ENCLOSURE (4)

27 JAN 1992

g. Are procedures established in all areas handling keying material to conduct watch-to-watch inventories?

(1) Do sections maintain an emergency action plan?

(2) Do sections have instructions on reporting suspected violations or compromises?

(3) Do sections have detailed instructions for the proper destruction/reporting of destruction of keying material or equipment?

ENCLOSURE (4)

SECURE TELEPHONE UNIT (STU)-III USAGE

1. Purpose. To promulgate the policy and procedures for the use of STU-III telephones within the 1st MAW.

2. Background

a. The STU-III program was initiated in 1985 by the Secretary of Defense to protect classified and sensitive unclassified information involving operations, plans, systems acquisition, logistic support, and personnel.

b. The advent of the STU-III affords a reliable, secure means of passing classified information; however, recent assessments of telephone monitoring reports indicate less than ten percent of calls made on STU-III units in PACFLT actually use the secure mode. Examples of information passed on a routine basis over unsecure telephones include:

- (1) Flag officer movements
- (2) Troop movements and flight schedules
- (3) Classified operational information

3. Action. In view of the telephone intercept/exploitation vulnerability and fiscal constraints that preclude replacing all telephones with STU-III units, the following policy is effective:

a. When the STU-III is available to both parties, users will go secure when discussing classified and sensitive unclassified info.

b. Personnel without immediate access to a STU-III will move to or transfer calls to a STU-III or other secure communications equipment when discussing classified or sensitive information.

c. Commanders will make crypto ignition keys (CIKs) readily available to each STU-III user. (CIKs are not classified items unless left unattended with the corresponding STU-III; MCO 2231.3 pertains).

d. Implement training/indoctrination programs ensuring the widest use of the STU-III in the secure mode.

e. Review requirements and improve the availability of STU-III's. The STU-III's are user friendly. Making a secure call is as easy as pushing a button, provided the CIK is in the phone. Commanding officers and supervisors must educate and enforce the routine use of the STU-III in the secure mode. The number of STU-III's fielded doesn't matter if the secure feature of the unit is not employed.

ENCLOSURE (5)