



UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CA 92055-5300

IN REPLY REFER TO:
2201
SSO
6 Mar 12

POLICY LETTER 1-12

From: Commanding General, I Marine Expeditionary Force
To: Distribution List

Subj: FOCAL POINT COMMUNICATION PROCEDURES

Ref: (a) CJCSM 3213.02C, The Joint Staff Focal Point Program
(b) DoD 5200.1-R, Information Security Program
(c) JCS SM 769-89, Focal Point Communication Procedures Manual
(d) DoD 5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual
(e) CJCSM 5760.01A Vol I & II, Joint Staff and Combatant Command Records Management Manual

Encl: (1) I MEF Standing OPT Manning Document
(2) I MEF Need to Know (NTK) Billet Matrix

1. Purpose. To establish administrative policies and procedures for I Marine Expeditionary Force's (I MEF) use of Joint Chiefs of Staff (JCS) Focal Point communication systems.

2. Applicability. This policy applies to all I MEF personnel and security assistance organizations (SAO) participating in any Focal Point Program(s). Where procedures are not addressed in this policy letter or conflict exists between this policy and reference (a), reference (a) will take precedence. Any questions regarding Focal Point communications systems procedures should be addressed to the Focal Point Program Control Officer (FPPCO).

3. General Responsibilities and duties. The I MEF Focal Point (FP) Program falls under the purview of the Special Security Officer (SSO) and Assistant Chief of Staff G-2 (AC/S G-2). Individual need to know (NTK) determination for each Focal Point Program (FPP) in which I MEF is a participant is the responsibility of the Assistant Chief of Staff G-5 (AC/S G-5).

a. Focal Point Control Officer. The Focal Point Control Officer has the primary management responsibility for the

Subj: FOCAL POINT COMMUNICATION PROCEDURES

specific assigned Focal Point Program(s) handled at I MEF. He is required to coordinate with the US Marine Corps Central Command (MARCENT) and US Marine Corps Pacific Command (MARFORPAC) command FPPCO regarding any administrative changes to his assigned program.

(1) Ensures required indoctrination and training is conducted in accordance with governing directives.

(2) Maintain and update an internal list of briefed personnel in each section with access to specific FPPs. Notify MARCENT FPPCO when personnel are departing the command or no longer require access to FPP material.

(3) In-Brief (Read-On) personnel. The briefing/debriefing statement (Nomination Form/CC Form 9) for a particular program must be signed by personnel who are given access to the system. The FPPCO will maintain the signed statement for the I MEF for the duration of the program.

(4) Provide MARCENT or MARFORPAC FPPCO with the NTK list of briefed personnel in their section/office and submit nominations for briefing to the MARCENT or MARFORPAC FPPCO.

(5) Ensure briefed personnel complete require annual training (per ref a).

(6) Establish and maintain a list of briefed personnel requiring access to the FPP folders. Provide the aforementioned list to the MARCENT or MARFORPAC FPPCO to ensure requested personnel are granted access to the FP folders on JWICS WAN.

(7) Access to folders is limited to personnel that are "Read-On" to specific programs, plans and/or information covered in the specific folder(s).

(8) Termination Briefing Procedures

(a) Debriefings (Read-Off) are required for the following reasons.

1. When an individual leaves the command, he/she will be read-off of all Focal Point Programs currently read on.

2. When an individual no longer has a need to know, he/she will be removed from the specific program(s) Access Control List (ACL).

Subj: FOCAL POINT COMMUNICATION PROCEDURES

(b) The Focal Point Program Control Officer will conduct the termination briefing with the individual departing. The FPPCO will monitor the outbound roster to cross reference the briefed personnel list in order to ensure individuals are debriefed prior to departing the command. The individual will be advised of the following requirements: "Understand that I am no longer authorized to the special category of information indicated. Further affirm that I have been advised of my continuing responsibility for not disclosing information concerning the programs."

(c) Once the individual has been read-off, the FPPCO will make the appropriate notation in the Focal Point Program Access Control Log. The FP Program Access Log will be managed and controlled by the FPPCO.

b. Briefed Personnel

(1) Individuals briefed and given access to a Focal Point Program are responsible for security of both Focal Point material and information.

(2) It is the individual's responsibility to notify the FPPCO when they are out-processing from the command.

c. Contractor Participation. If contractors participate in any Focal Point program, a DD Form 254, "Contract Security Classification Specification" must be modified as follows

(1) Mark "Yes" in block 10.k, "Other," and add note to "See Item 13."

(2) Mark "Yes" in block 11.a when access to ACCM/FPP information is not required at the contractor's facility (i.e. ACC/FPP work will be done "onsite" at government facility).

(3) In block 13 describe the information (ACCM) the contractor will need in performance of the contract and cite applicable wording from CJCSM 3213.02B as the security guidance for protection of the FPP information.

(4) If the contract will require handling of ACCM/FPP information at the contractor's facility, select the appropriate block(s) in section 11 and list specific security requirements (i.e. separate filing cabinets, special AIS configuration, etc.) in section 14.

Subj: FOCAL POINT COMMUNICATION PROCEDURES

(5) Since DD Form 254 addresses the type of information vice specific programs, the DD 524 will not require modification after program name changes.

4. General Focal Point Security

a. Personnel Security. A minimum of a final SECRET clearance, granted by a competent authority based on a National Agency Check (NAC) is required for FPP access. Personnel approved for access to FPP information DO NOT require Single Scope Background Investigation (SSBI).

b. Requesting access. Assistant Chiefs of Staff (AC/S) will request FPP access for personnel within their staff sections through the SSO for validation by the AC/S G-5 to determine NTK. The SSO will deliver Nomination/CC Form 9 for processing to the MARCENT FPPCO. The USCENTCOM Nomination/CC Form 9 will include (at a minimum) the following data:

(1) Individual's Name, Rank, SSN, Organization, and Security Clearance/Date Granted.

(2) Sufficient justification (describe how the individual's duties require FPP access).

(3) Unclassified Focal Point Communication System Nicknames for which access is required.

(4) After verification of security clearance information through the I MEF SSO, the FPPCO and AC/S G-5 will review requests for FPP access. Individuals approved for access will be contacted (via email or phoncon) and a security briefing scheduled. Access requests with insufficient data/justification will be returned to the sponsoring AC/S for corrective action.

5. Access Control List

a. Control Measures - Section 4.1 of Executive Order 12958 mandates organizations electronically processing FP information must have a control measure system in place to ensure access is limited to those with a NTK based upon a lawful and authorized purpose.

b. The FPPCO will coordinate identification of authorized users for each FP program processed by I MEF. Access will be

Subj: FOCAL POINT COMMUNICATION PROCEDURES

limited to those with a specific association in accordance with AC/S G-5 vetting (Encl 1 or 2).

c. FPPCO will review and update on a regular basis the access authorizations and/or restrictions for each FP protected folder.

d. A list of authorized users shall be maintained as an Access Control List (ACL), which will define the individuals granted access to FP information. ACLs will be maintained at the program level.

e. The ACL will be used to grant access to information, establish protected electronic files folders, identify authorized e-mail senders and/or recipients, and identify authorized DMS message senders and/or recipients.

f. The FPPCO and AC/S G-5 will audit the ACL quarterly to ensure no unauthorized modifications or duplications have been made.

g. A record of each ACL shall be maintained during the duration of the FP program. These records will be archived with other program records upon termination of the program.

6. Safe Keeping/Storage

a. FP information must be positively controlled at all times in a manner appropriate with the classification, warning notices, or control markings on the original material. FP information may be stored in either paper or electronic format. The program information must be stored in separate containers (paper or electronic) at the appropriate classification level. This controls NTK access and co-mingling with non-program information and materials.

b. Combinations to storage containers containing FP information will be limited to those personnel granted access. The Focal Point custodian will complete Standard Form 700 and section 2A. The FP custodian will be assigned in writing. The front page of the SF 700 will be placed in a visible location inside the safe to document contact information for personnel responsible for the safe. The safe combination will be recorded on Section 2A of SF 700, placed inside the envelope portion and sealed. The SF 700 envelope will be delivered to the I MEF SSO who is responsible for maintaining I MEF security container information.

Subj: FOCAL POINT COMMUNICATION PROCEDURES

c. Safe custodians are responsible for changing combinations as indicated below:

(1) When the container is initially used to store FP materials.

(2) Whenever an individual knowing the combination no longer requires access, unless the individual is no longer assigned to I MEF.

(3) When the combination has been subject to possible compromise.

(4) When the container is subject to maintenance by persons other than the custodian/FPPCO.

(5) When the container is take out of service.

d. Sensitive Compartmented Information Controls. FP material containing SCI will be handled per SCI regulations and restrictions. Access will only be granted to FP SCI material to those indoctrinated into SCI and the FP program. FP material contained within SCI controls will be stored in separate files and folders from other SCI material.

e. Archiving of FP Material. Documents and information protected within a FP system are Federal records subject to the regulations of the National Archives and Records Administration. Program sponsors will ensure that FP programs have a record management plan in place for economic and efficient management of all records of the program.

f. Reproduction of Focal Point material classified Secret and below is authorized.

i. Top Secret material requires approval of the Focal Point Top Secret Control Officer (FPTSCO).

7. Accountability and Control

a. Marking

(1) Printed Material. Standard cover sheets for TOP SECRET, SECRET, and CONFIDENTIAL are to be used with the word "Focal Point", written or stamped below the classification

Subj: FOCAL POINT COMMUNICATION PROCEDURES

marking and "ACCM" with the "Program Nickname" written or stamped on the center of the cover sheet.

(2) Within a given document, each paragraph containing FP protected information will be marked in addition to the normal classification marking with a Focal Point designation. For example, a paragraph containing SECRET/Focal Point information will be marked (S/Program Name).

(3) Electronic Marking. Electronically created Focal Point material will be marked in the following manner. In accordance with the classification of the material. "ACCM//Program Name" following the classification marking.

b. Transportation

(1) Written Material. Hand-carry - There are occasions when classified FP information is hand-carried in the normal work area or couriered outside the normal work area between geographic locations or aboard commercial aircraft.

(2) Within the normal work area - When hand-carrying classified FP information within the I MEF perimeter, the document or material will have a Focal Point cover sheet (FP classified cover sheet) attached to prevent inadvertent disclosure by non-briefed personnel (AF Form 310 or equivalent) is required for hand-to-hand transfer of Top Secret material.

(3) Outside the normal work area - When hand-carrying FP material outside the I MEF perimeter, FP material must be double wrapped with a classification and point of contact information on the inner container and enclosed in an outer container (e.g., sealed envelope, pouch, or locking briefcase). This will provide secure protection while in transit, prevent the material from breaking out of the container, and facilitate the detection of any tampering with container.

(4) Aboard Commercial Aircraft - When hand-carrying FP classified information aboard commercial aircraft, the individual must be authorized and designated as an official US Government Courier. The courier designation can be in the form of official travel orders, Courier Designation Letter, or

Courier Identification Card (DD Form 2501 MAR 88). The courier authorization and exemption notice should allow the individual to pass through passenger control points without subjecting the information to inspection. If stopped, inform authorities that

Subj: FOCAL POINT COMMUNICATION PROCEDURES

you are an official U.S. Government Courier. If necessary, contact I MEF SSO to verify courier status.

(5) Mailing. When Courier/ mailing FP information, double wrap the package. Inner envelope shall be marked with appropriate nickname and addressed to attention FPPCO. Outer envelope shall be marked with the addressee's mailing address; no classification, handling or other restrictive markings.

(6) Facsimile Transmissions. Facsimile transmission used in association with STE is authorized. Prior to sending, FPPCO/designee must call recipient, confirm program access, transmission system classification authorized and advise number of pages in facsimile. The cover sheet must be annotated with the appropriate caveats to document FP information:

(a) Contains "classification" (as appropriate)//ACCM "Program Nickname" material. Deliver immediately [or during normal duty hours] to "Program Nickname" Focal Point Program control Officer - [insert name if known] - only. **If you receive this FAX in error, notify the sender immediately. Do not copy or further disseminate without explicit permission from the sender or your local Focal Point Program Control Officer!**

(b) Sender must remain with facsimile machine until transmission complete and voice confirmation receipt of the complete document.

(7) Visual Aids. Visual Aids containing FP information will be annotated as follows: Classification//ACCM "Program Nickname". Ensure downgrading and/or declassification guidance is annotated on the title or first page.

(8) Video Teleconference (VTC). VTC of FP information may be authorized by the FPPCO. Any FP VTC must use the appropriate level of crypto for the highest level of data to be discussed (minimum of confidential). The following procedures shall be enforced during any FP VTC:

(a) Only appropriately cleared personnel with valid NTK for the FP program to be discussed may be present in the conference room and control room.

(b) Any electronic record used and created during the VTC must be appropriately marked and controlled.

Subj: FOCAL POINT COMMUNICATION PROCEDURES

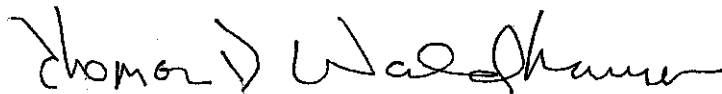
(c) Electronic systems used for the VTC must be "purged" of any FP information at the completion of the VTC. This should include sanitization of any electronic media and/or hard drives and any "temporary" or cache files created during electronic processing of the VTC.

8. Investigations. Any infraction of Focal Point security procedures, loss, unauthorized disclosure or other possible compromise of Focal Point material must be reported without delay to the FPPCO. Investigations are conducted IAW chapter 6, reference (b).

a. Data Spill Procedures. Compromise of FP program information can present an immediate and real threat to national security and personnel involved in mission execution. Anyone finding uncontrolled FP material shall take immediate action to secure the material and notify the FPPCO. The FPPCO will conduct any reporting, inquiry, investigation and damage assessment per specified guidelines. Use of the "Inadvertent Disclosure" form is not authorized.

b. Debriefing will follow guidelines in DoD 5200 1-R Series, C 10.1.8, Reasonable Risk Management Procedures, allow FP information incorrectly placed on non-approved electronic processing systems, transmitted to non-authorized personnel and/or systems can be removed by deleting the file and/or material from all affected systems unless the material is classified at a higher classification level than the system is accredited.

9. Recurring FP Training. The I MEF FPPCO will provide initial and annual security refresher training to I MEF FPP-briefed personnel. Refresher training will include various aspects of FPP security and individual responsibilities for protecting the information.



T. D. WALDHAUSER