MARINE EXPEDITIONARY UNIT ORDER 3070.1

From: Commanding Officer
To: Distribution List

Subj: 15TH MARINE EXPEDITIONARY UNIT (MEU) OPERATIONAL SECURITY (OPSEC)

Ref: (a) DOD Directive 5205.2
(b) Joint Publication 3-13.3
(c) All Marine Message 007/04
(d) MCWP 3-40.4.
(e) SEACNAVINST 5720.47B
(f) MCO 3070.2
(g) I MEF Operational Security SOP
(h) NSDD-298, the 1988 Presidential Directive

Encl: (1) 15th MEU Critical Information List (CIL)
(2) OPSEC Measures

1. Situation. To publish policy and guidance for OPSEC within the 15th MEU per the references.

2. Mission. This Order describes the concepts, responsibilities, policy, and standards that the 15th MEU and its personnel will follow for implementing OPSEC in the conduct of all aspects of unit operations, training, and administrative activities. It includes activities at home station, field training environments, and forward deployment.

3. Execution
   a. Commander's Intent and Concept of Operations

      (1) Commander's Intent. The MEU OPSEC Program is one element of the unit's comprehensive security system that complements other traditional security programs including Anti-terrorism, Physical Security, Information Security, Communications Security, and Personnel Security. To maximize their effectiveness, all of these programs must be integrated and mutually supporting. The 15th MEU OPSEC Program will provide the structure needed to offer OPSEC technical support to MEU programs and activities worldwide, conduct and/or support OPSEC surveys, and recommend improvements.

      (2) Concept of Operations. As outlined in references (f) and (g), the OPSEC program will employ the OPSEC five-step process to establish, guide, and manage the program. The program will provide an analytic methodology to protect critical mission information and improve mission effectiveness. The 15th MEU Commanding Officer will determine and specify the sensitive but unclassified information that is "critical" to the success, security, and safety of the unit, its personnel and families. This sensitive but unclassified information is identified in the Commander's Critical Information List (CIL) in enclosure (1). The program will recommend and...
describe OPSEC measures (see enclosure (2)) tailored to specific operations or activities that close vulnerability gaps and lower risk, and it will satisfy compliance with reference (h) that requires "each executive department and agency assigned or supporting national security missions with classified or sensitive activities to establish a formal OPSEC program," as well as references (f) and (g). In accordance with this plan and higher headquarters OPSEC SOPs and/or plans, all 15th MEU subordinate elements will participate in the 15th MEU OPSEC Program under the organizational structure outlined below.

(a) Organizational Structure

![Organizational Structure Diagram]

(b) 15th MEU Working Group. A 15th MEU Working Group consisting of representatives from the 15th MEU staff and major subordinate elements (MSEs) may be established in order to: review the 15th MEU OPSEC Program Plan; assist in facilitating consistent OPSEC implementation within the 15th MEU; serve as a forum for identifying and assessing OPSEC issues; and recommending policies, procedures, or actions to resolve those issues.

(c) MSE Coordinators. OPSEC Coordinators should be appointed from the Ground Combat Element (GCE), Logistics Combat Element (LCE), and the Aviation Combat Element (ACE).

b. Tasks

(1) S-1

(a) Ensure OPSEC measures are addressed in daily operations of the S-1, specifically when handling Personally Identifiable Information (PII) of personnel assigned to this command.

(b) Ensure S-1 personnel adhere to the OPSEC measures listed in enclosure (2) of this plan and develop additional measures related to the administrative functional area as necessary.
(c) Ensure S-1 personnel attend annual OPSEC training coordinated by S-3 Training.

(d) Ensure all newly joined S-1 permanent personnel receive the command OPSEC brief within 30 days of joining the command.

(2) S-2

(a) Lead staff in analyzing, processing and identifying adversaries and their collection capabilities in order to tailor OPSEC measures in support of operational planning.

(b) Ensure S-2 personnel adhere to the OPSEC measures listed in enclosure (2) of this plan and develop additional measure related to the intelligence functional area as necessary.

(c) Ensure S-2 personnel attend annual OPSEC training coordinated by S-3 Training.

(d) Ensure all newly joined S-2 permanent personnel receive the command OPSEC brief within 30 days of joining the command.

(e) Be prepared to designate an Officer/SNCO to serve on the 15th MEU OPSEC Working Group when established.

(3) S-3

(a) Exercise overall staff cognizance of the OPSEC program.

(b) Ensure OPSEC considerations and measures are included in all operational planning.

(c) Ensure S-3 personnel adhere to the OPSEC measures listed in enclosure (2) of this plan and develop additional measure related to the operations functional area as necessary.

(d) Ensure all newly joined permanent personnel receive the command OPSEC brief within 30 days of joining the command.

(e) Ensure OPSEC training is provided, on an annual basis, to individual command personnel by qualified instructors.

(f) Assign in writing an OPSEC Officer to manage the 15th MEU OPSEC program. Ensure the OPSEC Officer receives OPSEC Level II training within 90 days of appointment.

(g) Be prepared to establish the MEU OPSEC Working Group should it become necessary.

(4) S-4

(a) Ensure OPSEC measures are addressed in daily operations of the S-4.
(b) Ensure S-4 personnel adhere to the OPSEC measures listed in Encl (2) of this plan and develop additional measure related to the logistics functional area as necessary.

(c) Ensure S-4 personnel attend annual OPSEC training coordinated by S-3 Training.

(d) Ensure all newly joined S-4 permanent personnel receive the command OPSEC brief within 30 days of joining the command.

(e) Be prepared to designate an Officer/SNCO to serve on the 15th MEU OPSEC Working Group when established.

(5) S-6

(a) Ensure OPSEC measures are addressed in daily operations of the S-6.

(b) Ensure S-6 personnel adhere to the OPSEC measures listed in Encl (2) of this plan and develop additional measure related to the communications functional area as necessary.

(c) Ensure S-6 personnel attend annual OPSEC training coordinated by S-3 Training.

(d) Ensure all newly joined S-6 permanent personnel receive the command OPSEC brief within 30 days of joining the command.

(e) Be prepared to designate an Officer/SNCO to serve on the MEU OPSEC Working Group when established.

(6) OPSEC Officer

(a) Serve as the OPSEC advisor to the Commander and will provide appropriate OPSEC analysis support and recommend OPSEC measures.

(b) Brief the 15th MEU staff and subordinate command OPSEC Coordinators on OPSEC issues and changes based on the 15th MEU S-2’s assessed intelligence threat while forward deployed or as necessary.

(c) Ensure Working Group members or unit OPSEC Coordinators are replaced if any of the appointed personnel are unable to participate due to extended illness, long-term TDY/travel requirements, or reassignment.

(d) Coordinate all OPSEC efforts with the 15th MEU Security Manager.

(e) Complete OPSEC Level II training within 90 days of appointment.

(7) Major Subordinate Elements

(a) Provide one or more OPSEC Coordinator, depending on size and responsibilities of each element. Managers will ensure the OPSEC coordinator is replaced should the assigned person be unable to participate due to extended travel requirements, or reassignment. OPSEC Coordinators will
attend training as determined by the OPSEC Officer. OPSEC Coordinators will provide reports, assist with orientation and awareness training, and perform other OPSEC functions as determined by the OPSEC Officer.

(b) (Be prepared to) provide a senior representative to the OPSEC Working Group, if one is established. Working Group members will attend training as determined by the OPSEC Officer.

c. Coordinating instructions

(1) Training

(a) The OPSEC Officer will attend training, to include at a minimum an OPSEC Level II course, in order to develop the following skills:

1. Threat assessments;
2. Identification of Critical Information;
3. Identification of OPSEC indicators;
4. Analysis of OPSEC vulnerabilities;
5. Assessment of risk;
6. OPSEC measures development and implementation;
7. Contingency and emergency planning;
8. Awareness training development and presentation; and
9. OPSEC survey planning and execution.

(b) OPSEC Working Group members and OPSEC Coordinators, if assigned, will attend training designed to familiarize them with the OPSEC five-step process and with their OPSEC-related duties within the MEU. The OPSEC Officer will coordinate or conduct additional training for these individuals as required.

(c) All 15th MEU personnel will comply with the following:

1. Attend OPSEC orientation training, taught or coordinated by the unit OPSEC Officer, within 30 days of assignment to the unit or at the next available organizational unit training assembly. OPSEC Coordinators will conduct initial orientation training using materials provided by the OPSEC Officer.

2. Participate in annual OPSEC (Level I) awareness training. OPSEC Coordinators will ensure attendance by personnel in their command is documented, and will provide a report of completion to the OPSEC Officer within (30) days of the training.

(d) Separate OPSEC-related exercise are not required, but OPSEC activities and the implementation of OPSEC measures will be incorporated into
all training or operational readiness exercises to include those specifically focused on Anti-terrorism and Physical Security.

(e) OPSEC also will be incorporated into all tactical training exercises, to include those occurring during 15th MEU pre-deployment periods and annual training.

(2) OPSEC Reviews and Assessments

(a) OPSEC Reviews. The OPSEC Officer will ensure that systems are established within 15th MEU to conduct OPSEC reviews of documents and other media generated by unit members or its Family Readiness Officer, consistent with the procedures established in this Order.

(b) OPSEC Assessments

1. The OPSEC Officer will also provide OPSEC assessment support, to include providing additional threat information, analysis of a specific OPSEC problem area, and recommendations for all organizational elements of the 15th MEU.

2. The OPSEC Officer will ensure the 15th MEU conducts at least an annual OPSEC self-assessment, as well as conducting/coordinating OPSEC assessments of subordinate commands. The assessment plan will be approved by the Commander, and will be coordinated at least three months in advance of the required completion date.

4. Administration and Logistics. Recommendations and changes regarding this Order are encouraged and may be submitted to the 15th MEU OPSEC Officer via the chain of command.

5. Command and Signal

a. Command. This Order applies to all 15th MEU personnel, to include all Marines and Sailors, all attachments and detachments, and all military ship riders supporting the 15th MEU.

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

S. D. CAMPBELL

DISTRIBUTION: A
15th MEU Critical Information List (CIL)

1. This enclosure provides the 15th MEU Commander's critical information. The below listed information will be protected as sensitive but unclassified. All Marines, Sailors and family members should not divulge this information to anyone without a need to know. This information is not an all-encompassing checklist which can be robotically applied to all situations. Subordinate commanders and their staffs will use their judgment and experience to develop critical information unique to their mission.

2. Times, Dates and Locations
   a. Training exercises
   b. Operations Plans
   c. Deployment/Re-deployment

3. Capabilities
   a. Computer networks
   b. Communications systems (I.E. radios, BFT etc.)
   c. LFOC C2 systems
   d. Air platforms
   e. CBRNE defense
   f. Weapon systems/munitions
   g. Logistics

4. Operations
   a. Strategy and tactics
   b. Force composition, disposition
   c. Attrition and reinforcement
   d. Targets
   e. Time considerations
   f. Logistic capabilities and constraint
   g. Forces assigned and in reserve
   h. Targets

Enclosure (1)
i. Time considerations
j. Routes for combat units, support units, and resupply
k. Logistic capabilities and constraints

5. **Intelligence, Surveillance and Reconnaissance (ISR)**
   a. Purpose of collection efforts
   b. Targets of collection
   c. Time considerations
   d. Types of and capabilities of collection assets
   e. Processing capabilities
   f. Units requesting intelligence data
OPSEC Measures

1. The following OPSEC measures are general in nature and can be applied across a wide range of functional areas. Subordinate commanders and their staffs will use their judgment and experience to develop more specific OPSEC measures based on the vulnerabilities identified unique to their individual unit mission(s).

2. Operational and Logistic Measures

   a. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations and activities in terms of time, place, event, sequencing, formations, and command and control arrangements.

   b. Employ force dispositions and command and control arrangements that conceal the location, identify, and command relationships of major or important units.

   c. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

   d. Transport supplies and personnel to combat units in such a way to conceal the location and identity of combat units.

   e. Operate aircraft at a low altitude to avoid detection.

   f. Operate and deploy units or weapons systems in a way to minimize the reflective surfaces exposed to radar and sonar.

   g. Use darkness to mask deployments or force buildup.

3. Technical Measures

   a. Use proper radio procedures and techniques to minimize interception and evaluation of emissions. Use techniques such as burst transmissions, secure phones, couriers, encrypted transmission, and frequently changing codes and encryptions. Limit use of high frequency radios and directional super-high frequency transponders.

   b. Control radar emissions, operate at reduced power, and operate radars common to many units.

   c. Mask emissions, forces, and equipment from radar or visual detection by use of terrain.

   d. Use appropriate military deception. Use camouflage, smoke, background noise, or inclement weather to conceal movement of personnel, units, and equipment (be aware that this might create a contrast and attract the enemy's attention without conditioning or integration into a deception package).
4. **Administrative Measures**

   a. Avoid bulletin board notices, plan of the day, or planning schedule notices that reveal when events will occur (or other specific details).

   b. Conceal budgetary transactions, supply request and actions, and arrangements for services that reveal preparations or intentions for operations.

   c. Conceal the issuance of orders, the movement of special personnel and/or equipment to units, and the addition of special capabilities to units.

   d. Control trash disposal and other housekeeping functions to conceal the identity and location of units, and other details pertaining to the operation.

   e. Follow normal leave and liberty policies to the maximum extent possible to present a sense of normalcy.

   f. Ensure that personnel discreetly prepare for their family’s welfare in their absence.

5. **Military Deception in support of OPSEC**

   a. Cause enemy intelligence to not target friendly activities, ensuring failure to collect intelligence against our tests, operations, and exercises. Also attempt to prevent the enemy from determining through analysis vital capabilities and characteristics of weapon, systems, and vital aspects of policy, doctrine, and tactics.

   b. Create confusion about, or cause multiple interpretations of intentions, operations, tactics to be employed, and timetables.

   c. Create confusion about or cause multiple interpretations of vital information taken from open sources.

   d. Cause enemy observers to lose interest in the test, operation, exercise, or activity; or to assign a low priority to intelligence collection efforts.

   e. Convey inaccurate locating and targeting information to the enemy.

6. **Physical destruction and Electronic Warfare.** During hostilities, use physical destruction and electronic attack against the enemy’s assets used to collect and process intelligence. Offensive Information Operations actions that can be conducted include strikes against the following: satellites, communications centers or sites, radars, fixed sonar sites, reconnaissance aircraft, ships, or units.