



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:
3070
G-3/OPSEC
01 AUG 2011

POLICY LETTER 3-11

From: Commanding General
To: Distribution

Subj: OPERATIONS SECURITY

Ref: (a) MCO 3070.2
(b) I MEF Social Media Policy

Encl: (1) Inspector General's Checklist

1. Situation. Operations Security (OPSEC) is a systematic and proven process by which I Marine Expeditionary Force (IMEF) members can deny potential adversaries critical, unclassified information about unit capabilities, activities and intentions. Everyone within I MEF is responsible to ensure they incorporate OPSEC into all facets of training, operations, planning, deployment and support.

2. Mission. This letter provides continued guidance for the implementation of requirements of reference (a) and (b) to prevent an adversary or potential adversary from obtaining critical information that facilitates the prediction of friendly intentions, capabilities, or activities.

3. Commander's Intent. To ensure I MEF maintains strict adherence to the Department of Defense (DOD) and USMC OPSEC programs. Through strict adherence to the OPSEC practices outlined in this letter, I MEF will reduce its vulnerabilities and indicators while negatively impacting our adversary's abilities to collect critical information against our forces.

4. Execution. The I MEF G-3 will manage the OPSEC program. The I MEF OPSEC Program Manager and Major Subordinate Command (MSC) Coordinators will ensure all aspects of OPSEC Awareness are incorporated into daily activities. Commanders will appoint unit level coordinators to manage unit programs. All new join personnel will accomplish OPSEC Awareness Training within 90 days of assignment to I MEF. Unit specific OPSEC training will be conducted and tracked by unit level coordinators. All contractors, visitors and civilians will be incorporated into the I MEF OPSEC Awareness program. The I MEF Influence Working Group (IWG), which meets quarterly, will include an OPSEC Program Manager and Antiterrorism Force Protection (ATFP) representative in order to improve unit support and protection.

5. Subordinate Element Tasks. Per the following, efforts will be made to reduce I MEF OPSEC vulnerabilities.

a. All OPSEC Coordinators will conduct OPSEC self inspections semi-annually using Enclosure (1).

b. A 100 percent cross cut shred, or burn, policy is the I MEF standard for all paper, regardless of classification.

c. Use of Out-of-Office email reply and voicemail tool(s) are permitted with restrictions. Personnel will screen their replies to ensure it doesn't contain any information that violates sound OPSEC practices. Examples of prohibited Out-of-Office email/voicemail information are: Exact deployment/leave/TAD dates, deployment/leave/TAD locations, description/nature of absence, or any personal details that might lead to exploitation.

d. A clean desk policy is highly encouraged. Do not post Privacy Act related information in the office. This includes recall rosters, retirements, and orders with SSNs or any other protected information.

e. The leveraging of current technology is encouraged; however, personal cell usage will occur outside of buildings prohibiting cell phone use. Use of social networking sites is based on common sense and good judgment; however, you will not send any military related items or post critical information, such as unit or deployment identifying information, on these systems.

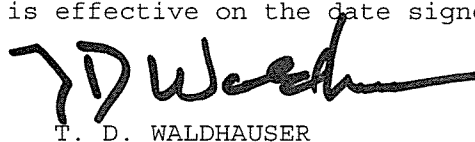
f. Unit Coordinators are encouraged to request a Staff Assistance Visit from the respective higher headquarters prior to an inspection.

6. Administration and Logistics. The point of contact regarding this policy letter is the I MEF G-3/FOPS section (760)725-9083.

7. Command and Signal

a. Command. This Policy Letter is applicable to all commands, organizations, units, and activities under the cognizance of I MEF.

b. Signal. This Policy Letter is effective on the date signed.



T. D. WALDHAUSER