



UNITED STATES MARINE CORPS
MARINE AIR GROUND TASK FORCE TRAINING COMMAND
MARINE CORPS AIR GROUND COMBAT CENTER
BOX 788100
TWENTYNINE PALMS, CA 92278-8100

CCO 3070.1B

3

AUG 12 2014

COMBAT CENTER ORDER 3070.1B

From: Commanding General
To: Distribution List

Subj: OPERATIONS SECURITY

Ref: (a) MCO 3070.2A

Encl: (1) Critical Information List

1. Situation. Marine Air Ground Task Force Training Command (MAGTFTC), Marine Corps Air Ground Combat Center (MCAGCC) and its subordinate commands shall develop an aggressive Operations Security (OPSEC) program in order to prevent an adversary or potential adversary from obtaining critical information that facilitates the prediction of friendly intentions, capabilities, or activities.

2. Cancellation. CCO 3070.1A.

3. Mission. In accordance with the reference, MAGTFTC, MCAGCC will implement measures in support of the OPSEC program. This Order provides responsibilities and procedures for MAGTFTC, MCAGCC and its subordinate commands to fulfill these requirements.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. MAGTFTC, MCAGCC will have a systematic approach to OPSEC which includes organizational support, regular OPSEC training, assessments, and the development and incorporation of the critical information list, enclosure (1), and the OPSEC planning process into operations, exercises, and garrison environments. OPSEC must become a way of life for all Marines. These efforts will ensure that OPSEC programs are developed, utilized, and are relevant to Marines across all MAGTFTC, MCAGCC endeavors.

(2) Concept of Operations. MAGTFTC, MCAGCC will achieve the Commandant of the Marine Corps' intent by developing OPSEC standards and then promulgating them throughout the command. This Order announces the standards for program requirements, training, and assessment procedures. By implementing the guidance contained within this Order, commanders will ensure their units have OPSEC officers appointed, develop OPSEC programs tailored to their commands, and utilize the OPSEC planning process. Commanders will also share their OPSEC concerns with public affairs officers and family members to reduce inadvertent disclosures. A thorough system of OPSEC assessments will ensure that these programs receive regular command attention so that they remain relevant to command needs.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

b. Subordinate Element Missions

(1) Commanding Officers (COs)

(a) OPSEC is a command responsibility. COs will incorporate OPSEC principles and policies into all operations.

(b) Assign, in writing, an OPSEC Program Manager or Coordinator. Program managers are personnel who have OPSEC duties as their primary job. Coordinators are personnel who perform OPSEC functions as an additional duty. COs will use their discretion in determining whether they require OPSEC Program Managers or Coordinators to fulfill their responsibilities.

(2) Operations Security Program Managers and Coordinators

(a) Maintain this OPSEC Order.

(b) Develop and implement an OPSEC program. A complete OPSEC program will contain all provisions listed within the reference. A thorough OPSEC program will integrate all aspects of policy and guidance, education, reviews, and assessments of all MAGTF/TC, MCAGCC commands.

(c) All OPSEC Program Managers and Coordinators will complete an OPSEC fundamentals course within 30 days of appointment. The course, Computer Base Training 1301, is available on-line at the following URL <https://www.portal.navy.mil/netwarcom/NIOC-N/COPCentral/opsec/default.aspx> on the Navy Information Operations Command website.

(d) Attendance at a resident course is at the discretion of the COs.

(e) Accomplish annual OPSEC training for all command personnel through the various command and section representatives. Minimum training requirements are:

1. The definition of OPSEC and its relationship to the command's security and intelligence programs.

2. An overview of the OPSEC process.

3. The command's current critical information list. This will ensure command members do not inadvertently disclose critical information.

4. A roster providing the command's personnel fulfilling OPSEC responsibilities.

(f) Prepare for OPSEC Program participation in the Commanding General's Inspection Program (CGIP). OPSEC is a functional area on the Inspector General's checklist and evaluations are required as part of each unit's Command Inspection Program and the CGIP. Inspection teams will review the OPSEC functional area of all commands.

(g) Coordinate with the command public affairs officer in order to ensure OPSEC principles are adhered to in official statements and through all command sponsored World Wide Web sites.

CCO 3070.1B
AUG 12 2014

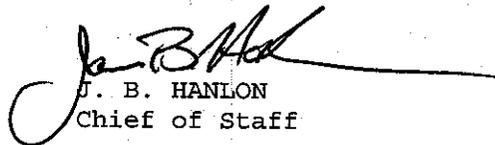
c. Coordinating Instructions. Commands seeking additional assistance with OPSEC tactics, techniques, procedures, and training support advice for command level OPSEC assessments, or OPSEC aids such as posters, can find this information at <https://www.portal.navy.mil/netwarcom/NIOC-N/COPCentral/opsec/default.aspx>.

5. Administration and Logistics. Distribution statement A directives issued by the Commanding General are distributed via email upon request and can be viewed at <http://www.29palms.marines.mil/Staff/G1Manpower/AdjutantOffice/Orders.aspx>.

6. Command and Signal

a. Command. This Order is applicable to all active duty, reserve, civilian personnel, and family members working, living, or visiting aboard the Combat Center.

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


J. B. HANLON
Chief of Staff

Distribution: A

Critical Information List



MAGTFC, MCAGCC, 29 Palms

Critical Information is an adversary's target of choice. Seemingly harmless UNCLAS data combined with other conversations, presentations, e-mails or documents could reveal classified information. Personnel will employ proper Operations Security (OPSEC) and protect Critical Information.

**DO NOT DISCUSS CRITICAL INFORMATION
OVER UNSECURED TELEPHONE LINES
OR UNCLASSIFIED E-MAIL
USE YOUR STE/STU III or SIPRNET !**

DO NOT DISCUSS:

- UNIT CAPABILITIES OR DEGRADATION
- PERSONALLY IDENTIFIABLE INFORMATION (PII)
- DETAILS OF PLANS, OPERATIONS, ORDERS, OR PROGRAMS
- REFERENCE OF MISSION ASSOCIATED INFORMATION, SUCH AS PERSONNEL/EQUIPMENT DEPLOYMENT DATES OR LOCATIONS
- SPECIFIC TAD/TDY DEPLOYMENT DATA, INCLUDING PERSONNEL NUMBERS, DURATION, LOCATION, SYSTEMS, ETC.
- SPECIFIC DETAILS CONCERNING TAD/TDY TRAVEL ITINERARIES AND PURPOSES OF TRAVEL BY KEY PERSONNEL
- ASSOCIATION OF ABBREVIATIONS, ACRONYMS, NICKNAMES, OR CODEWORDS WITH PROJECTS OR LOCATIONS
- NEW, PROJECTED, OR EXPANDED SECURE COMMUNICATIONS CAPABILITIES

BE AWARE:

- **DO NOT LEAVE YOUR CAC CARD IN YOUR COMPUTER UN-ATTENDED**
- **WITH WHOM YOU ARE TALKING TOO AND DO THEY NEED THE INFORMATION THEY ARE REQUESTING.**

Implementing OPSEC at work and home enables mission success by eliminating adversary options. Become a hard target!