



UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
POSTAL SERVICE CENTER BOX 8003
CHERRY POINT, NORTH CAROLINA 28533-0003

ASO 3070.1A
OPS
01 APR 2015

AIR STATION ORDER 3070.1A

From: Commanding Officer, Marine Corps Air Station, Cherry Point
To: Distribution List

Subj: OPERATIONS SECURITY (OPSEC) PROGRAM

Ref: (a) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," 20 Jun 2012
(b) Joint Publication 3-13.3, "Operations Security," 4 Jan 2012
(c) MCO 3070.2A, "The Marine Corps Operations Security (OPSEC) Program," 2 Jul 2013
(d) MARFORCOMO 3070.1, "Operations Security," 5 Jun 2014
(e) MCIEASTO 3070.1, "Operations Security (OPSEC)," 29 Nov 2007

Encl: (1) OPSEC Terms and Definitions

Report Required: Annual USMC Operations Security Report (Report Control Symbol DD-3070.1), par 4b(5).

1. Situation

a. Diverse operating environments present the Marine Corps with a multitude of threats ranging from the clearly defined to the masked and unknown. Our adversaries have become skilled at deception and in their methods of intelligence collection against us. As a Corps we have continually sought to vigorously protect classified information, today however, our adversaries gain and devote more than 80 percent of their operational planning intelligence to our open sourced, unclassified material.

b. OPSEC is a systematic and analytic process to deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations. The enclosure provides common use terms and definitions associated with OPSEC.

2. Cancellation. ASO 3070.1.

3. Mission. Marine Corps Air Station (MCAS) Cherry Point (CHERPT) will establish an aggressive OPSEC program in order to prevent an adversary or potential adversary from obtaining critical information on our intentions, capabilities, or activities.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. In accordance with reference (c), MCAS CHERPT will institute an OPSEC program utilizing the five-step OPSEC process consisting of: Identifying critical information, threat assessment, vulnerability

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

01 APR 2015

assessment, risk assessment, and applying OPSEC countermeasures. The nature of our operational environment calls for OPSEC to be engrained in our minds constantly. OPSEC needs to become a way of life. The end result of our efforts will undoubtedly be the protection of our most vital asset—Marines and our government civilian workforce.

(2) Concept of Operations. This Order outlines the standards for the Installation's OPSEC program requirements, training, and assessment procedures. Adhering to these procedures will ensure OPSEC coordinators are appointed and programs are developed in accordance with the five-step OPSEC process. To be successful, this will require commanders and supervisors at all levels, both military and civilian, to continually reinforce the importance of good OPSEC practices.

b. Coordinating Instructions

(1) The Installation OPSEC Coordinator is responsible for assisting subordinate commands with planning and executing their respective OPSEC programs. The OPSEC program needs to be closely coordinated with members of the staff, Joint Public Affairs Office (JPAO) Webmaster, and Family Readiness Officer (FRO).

(2) OPSEC is not a security or an intelligence function. While these functions often interact and overlap, they are mutually supportive. The OPSEC Coordinator will seek support from the Naval Criminal Investigative Service (NCIS) and Counterintelligence/Human Intelligence staff from higher headquarters if any intelligence support is required.

(3) Training Requirements

(a) Subordinate Command OPSEC Coordinators must complete the OPSEC Fundamentals Course, OPSE 1301, within 30 days of appointment. The computer-based training DVD can be ordered by contacting the Naval Information Operations Center (NIOC) organizational mailbox, opsec@navy.mil. It can also be completed through the Interagency OPSEC Support Staff (IOSS) at <http://www.ioiss.gov/> listed under "Training."

(b) The Installation OPSEC Coordinator shall: Attend the Interagency OPSEC Support Staff (IOSS) OPSEC Analysis and Program Management resident course (OPSE 2500) or equivalent course, within 90 days of appointment.

1. Registration for the OPSE 2500 course can be completed at www.ioiss.gov or via email at ioiss@radium.ncsc.mil.

2. Current OPSEC Coordinators who have completed the Navy OPSEC Course or the Headquarters Department of the Army OPSEC Level II Course will have satisfied this requirement.

(c) The Installation OPSEC Coordinator, Subordinate Command OPSEC Coordinators, and FROs, along with the Installation Public Affairs Officer and Webmaster shall complete "web-based" OPSEC training.

1. Training shall be completed within 90 days of appointment.

2. Training will be completed in accordance with Figure 1-1.

3. Annual refresher training is required to maintain situational awareness of internet-based capabilities and web based vulnerabilities.

(d) Annual OPSEC training requirements for command personnel are:

1. A definition of OPSEC and its relationship to the Command's security, intelligence, and cyber security programs.

2. An overview of the OPSEC process.

3. OPSEC and social media.

4. The Command's current Critical Information List (CIL).

5. A portion of the annual training requirements can be completed through MarineNet at www.marinenet.usmc.mil, using training event code "AO" and course code "OPSECUS001" for Uncle Sam's OPSEC. To complete the requirement, commands are required to provide a copy of the CIL and show the command's OPSEC relationship to the security, intelligence, and cyber security programs.

	Total force (including Contractors)	Coord/Mgr	PAO	FRO	Webmasters
Annual OPSEC Training	Required	Required	Required	Required	Required
OPSEC Fundamental (IOSS 1301)	Optional	Required	Optional	Optional	Optional
OPSEC Analysis & Pgrm Mgmt (IOSS 2500)	Optional	Required for Reg/Group and Higher	Optional	Optional	Optional
OPSEC & Public Release Decisions (IOSS 1500)	Recommended	Required	Required	Required	Required
OPSEC & Web Risk Assessment (IOSS 3500)	Recommended	Required	Required	Required	Required

Figure 1-1

(4) Inspections

(a) OPSEC is a functional area that will be evaluated and inspected as part of the Commanding General's Readiness Inspection (CGRI) Program.

01 APR 2015

(b) The Installation OPSEC Coordinator will conduct an annual inspection of subordinate commands utilizing the Detailed Inspection Checklist 481 which can be located at: www.hqmc.marines.mil/igmc/Resources/FunctionalAreaChecklists. Records of these inspections shall be retained for three years. A copy of these inspections will also be provided to the inspected entity for their records. Inspected entities will retain a copy of the inspection for three years.

(c) All commands required to maintain an OPSEC program will conduct an internal inspection utilizing the Detailed Inspection Checklist, at least annually. During this annual inspection, OPSEC Coordinators shall review their command's CIL, countermeasures, and threat statement for currency and relevance. Results from these inspections will be retained for three years. Commands will normally utilize their own personnel to conduct an annual, command-level OPSEC assessment.

(5) Annual Reporting Requirement (RCS DD-3070.1). Marine Transport Squadron One (VMR-1) and Headquarters and Headquarters Squadron (HQHQRON) OPSEC Coordinators will submit an annual calendar-year report, detailing their OPSEC program. Guidance on the format and submission date for this report will be released via the Marine Corps Action Tracking System (MCATS) as it becomes available. The Installation OPSEC Coordinator will be the primary point of contact for this report.

(6) Excessive OPSEC. Excessive OPSEC can degrade operational effectiveness by interfering with various day-to-day activities such as coordination, training, and logistical support. Commanders must evaluate each activity and operation and then balance required OPSEC countermeasures against operational needs. The OPSEC process will help commanders assess risk and apply appropriate OPSEC countermeasures.

(7) Program Awareness and Training Product Promotion

(a) Per reference (c), active promotion of the OPSEC program is the responsibility of all levels of commands. All Commanding Officers are encouraged to develop their own OPSEC promotional materials and use all suitable techniques of publicity and promotion consistent with the law and within funds available. Ideally, such items will be appropriate for the work environment and serve as a reminder of the benefits of participating in the program. Coffee mugs, key rings, lanyards, pens, trifolds, posters, cards, etc., are typical promotional items.

(b) As part of promotional efforts, commanders at all levels should:

1. Advertise the OPSEC program through posters, billboards, inserts in bulletins, or other media which frequently reach Marines, civilians, and contractors.

2. Develop slogans, logos, and other materials designed to promote their OPSEC program.

(c) The MCAS CHERPT OPSEC Coordinator will serve as the primary point of contact to subordinate commands for how to obtain OPSEC products and resources.

c. Tasks

(1) Operations Directorate

- (a) Develop and maintain an Installation OPSEC order.
- (b) Develop and implement an OPSEC program.
- (c) Develop OPSEC plans in support of operations and exercises.

(d) Appoint in writing, an officer, staff noncommissioned officer, or equivalent civilian employee as the Installation OPSEC Coordinator whose duties, at a minimum, will include:

1. Provide OPSEC subject matter expertise and recommendations to the Commanding Officer.

2. Develop, coordinate, and maintain the Installation OPSEC Program to include drafting policy/guidance.

3. Coordinate command OPSEC surveys as required.

4. Coordinate OPSEC education and training.

5. Conduct an annual assessment of VMR-1 and HQHQRON OPSEC programs, utilizing the Detailed Inspection Checklist 481.

6. Develop a CIL in accordance with reference (c). Provide a copy of the CIL to the Installation Joint Public Affairs Officer/Webmaster and the FRO in order to prevent inadvertent disclosure of this information.

7. Establish an OPSEC working group. This working group may be combined with the Mission Assurance Working Group. Ensure meetings are conducted at least quarterly, specifically addressing OPSEC.

(2) Subordinate Commanders

(a) Appoint an OPSEC coordinator in writing to:

1. Provide OPSEC subject matter expertise and recommendations.

2. Perform the five step OPSEC process in accordance with reference (c).

3. Develop a CIL in accordance with reference (c). Provide a copy of the CIL to the Installation Public Affairs Officer/Webmaster and your respective FRO in order to prevent inadvertent disclosure of this information.

4. Coordinate OPSEC matters with the Installation OPSEC Program Coordinator.

5. Provide OPSEC education and training for members of your staff.

0 1 APR 2015

6. Coordinate and conduct annual internal reviews and assessments utilizing the Detailed Inspection Checklist 481.

7. Provide representation to the OPSEC Working Group.

8. Commanders will discuss OPSEC concerns as part of their Family Readiness Program and stress the individual family's ability to contribute to the protection of the Command's critical information.

(3) Joint Public Affairs Office

(a) Ensure the Installation Webmaster reviews all Command websites to ensure there is no critical information published via text, graphics, or photographs.

(b) The Installation JPAO and Webmaster will complete OPSEC training in accordance with Figure 1-1.

(4) Family Readiness Officer. VMR-1 and HQHQRON FROs will complete OPSEC training in accordance with Figure 1-1.

5. Administration and Logistics. Recommendations for changes to this Order should be submitted to the MCAS CHERPT Operations Directorate (Attn: Mission Assurance Department) via the appropriate chain of command.

6. Command and Signal

a. Command. This Order is applicable to MCAS Cherry Point and its subordinate commands.

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



C. PAPPAS III

DISTRIBUTION: A

OPSEC Terms and Definitions

1. This enclosure contains common use terms and definitions associated with OPSEC and are provided for a clearer understanding of OPSEC as well as to assist with the OPSEC Program creation process.

a. Adversary. An individual, group, organization, or government that must be denied critical information.

b. Adversary Intelligence Systems. Resources and methods available to and used by an adversary for the collection and exploitation of critical information or indicators thereof.

c. OPSEC. A process of identifying unclassified critical information and subsequently analyzing friendly actions attendant to military operations and other activities (i.e., that prepare, sustain, or employ Marine forces during war, crisis, or peace) to:

(1) Identify those actions that can be observed by adversary intelligence systems.

(2) Determine indicators which adversary intelligence systems might obtain, that could be interpreted, or pieced together to derive critical intelligence in time to be useful to adversaries.

(3) Select and execute OPSEC countermeasures that eliminate or reduce to an acceptable level, the vulnerabilities of friendly actions to adversarial exploitation.

d. OPSEC Assessment. An evaluative process, conducted at least annually, of an organization, operation, activity, exercise, or support function to determine if sufficient OPSEC countermeasures are in place for protection from adversary intelligence exploitation. An OPSEC program assessment may include program reviews, Inspector General Inspection, or higher headquarters assessments that specifically address OPSEC.

e. OPSEC Coordinators. Personnel who have OPSEC duties as their responsibility on a part-time basis.

f. OPSEC Program Manager/OPSEC Manager. Personnel who have OPSEC duties as their primary responsibility on a full-time basis.

g. Countermeasures. Employment of devices and/or techniques for the purpose of impairing the operational effectiveness of enemy activity.

h. OPSEC Countermeasures. Methods and means to gain and maintain essential secrecy about critical information.

i. OPSEC Indicator. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

j. OPSEC Survey. A collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes.

01 APR 2015

k. OPSEC Vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

l. Critical Information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment.

m. Essential Elements of Friendly Information (EEFI). Key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities necessary for adversaries to plan and act effectively against friendly mission accomplishment.

n. Sensitive Information. Refers to unclassified information requiring special protection from disclosure that could cause compromise or threat to our national security, the Marine Corps, Marines, civilian Marines, DoD contractors, or family members.