UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
BEAUFORT, SOUTH CAROLINA 29904-5001

3000
S-3

2 6 JUL 2013

AIR STATION ORDER 3070.1

From: Commanding Officer
To: Distribution List

Subj: OPERATIONS SECURITY (OPSEC)

Ref: (a) DOD Directive 5205.2
(b) Joint Publication 3-13.3
(c) SECNAVINST 5720.47B
(d) OPNAVINST 3432.1
(e) MCO 3070.2
(f) MCIEASTO 3070.1

Encl: (1) Critical Information List

1. Situation

a. Today's security environment has evolved from one in which the threat from identifiable adversarial nation-states has been joined by the less identifiable trans-national terrorist. Regardless of status, these adversaries have the will and the ability to do harm to U.S. interest both at home and aboard. Rapid advances in available, information technologies and the development of sophisticated, aggressive collection organizations, forces us to reconsider what information can be used to compromise on-going military operations.

b. While the protection of classified information remains a priority, the protection of unclassified open source material must be considered. Today, collection efforts by adversaries are directed toward open source, unclassified information. Methods of collecting critical pieces of information may vary.

c. In most cases, classified information is no longer essential or necessary to build and accurate intelligence picture of what our military forces are doing. Using easily obtained, unprotected information, objectives can be determined and an appropriate response developed to deny us those objectives. Now more than ever, each Marine, Sailor, and civilian Marine must be cognizant of the importance of protecting unclassified, but potentially useful, information from those who would do harm to this nation and its military forces.

2. Mission. MCAS Beaufort will implement an OPSEC program in order to protect critical information from exploitation by any adversary seeking to impede or deny the success of our military operations.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To deny potential adversaries unimpeded access to information that could be useful in developing actions intended to be disruptive to military operations.

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

(2) Concept of Operations

(a) The Commander of MCAS Beaufort will appoint in writing, an Officer or Staff NonCommissioned Officer as the OPSEC Program Coordinator.

(b) Develop an OPSEC program meeting the requirements listed in the Coordinating Instructions of this order.

(c) Ensure the OPSEC program is reviewed by inspection teams operating as part of the Commanding General's Inspection Program.

(d) Conduct an annual review of the MCAS Beaufort's OPSEC program. This will be based on a fiscal-year time period.

(e) Develop and implement an OPSEC Program tailored to the command's needs. At a minimum, the Program shall consist of:

1. OPSEC Order.

2. OPSEC training as outlined in paragraph (3) (c) (3) of this plan.

3. A Critical Information List. (See Enclosure 1).

4. Emphasis on the importance of OPSEC with family members.

5. A coordinated effort with the Public Affairs Officer in order to prevent inadvertent disclosure of Critical Information via public affairs programs.

b. Subordinate Element Missions

(1) OPSEC Program Coordinator will:

(a) Coordinate and supervise all OPSEC matters for MCAS Beaufort.

(b) Develop and maintain the MCAS Beaufort OPSEC program.

(c) Coordinate OPSEC matters with adjacent and higher commands in order to reduce duplicated effort and expending limited resources.

(d) Review MCAS Beaufort websites to ensure they meet the OPSEC concerns listed in paragraph (4) (a) (5) of this plan.

(e) Direct the removal of information from websites that violate OPSEC standards unless adequate safeguards are employed.

(f) Ensure OPSEC training is conducted annually for all MCAS Beaufort personnel.

(2) S-3 will:

(a) Develop and maintain an OPSEC Order and OPSEC program for MCAS Beaufort.

(b) Assist the commander and operations staff in planning, coordinating, and executing counter-intelligence support and threat assessments during the drafting and reviewing of OPSEC plan

(3) Mission Assurance Program Manager will:

(a) Develop and maintain the Information Assurance Program that incorporates the MCAS Beaufort OPSEC plan requirements.

(b) Assist MCAS Beaufort OPSEC Program Coordinator in ensuring appropriate safeguards are in effect for information posted to websites.

c. Coordinating Instructions

(1) The OPSEC program needs to be closely coordinated with all departments and incorporate into the Anti-Terrorism/Force Protection and Security Programs. Close coordination must be maintained between all staff functions to ensure adequate OPSEC protection.

(2) OPSEC is not strictly a security or intelligence function. Security functions prevent unauthorized access to personnel, equipment, facilities, materials, and documents. Intelligence activities provide information on adversary forces, governments, and intentions. OPSEC and these activities often overlap and mutually supportive.

(3) OPSEC Training Requirements are as follows:

(a) All OPSEC Program Managers and Coordinators will complete an OPSEC Fundamentals Course within 30 days of appointment. The course is available online. It is listed as "CBT 1301" and is available at the Navy Information Operations Command website: https://www.niocnorfolk.navy.mil/opsec/index.html. Copies of this course can be obtained by emailing the following organizational mailbox, opsec®navy.mil or by mailing a request to: Navy Information Operations Command, ATTN: OPSEC, 2555 Amphibious Drive, Norfolk, VA 23521. Available Courses are:

1. Navy OPSEC Course; https://www.nioc-norfolk.navy.mil/

2. DoD OPSEC Officers Course; http://www.dss.mil/

3. OPSE 2380, 2390, 2400 Course; http://www.ioss.gov/

4. Army OPSEC Planner's Course; https://www.1stiocmd.army.mil/

(b) Annual OPSEC training is required for all command personnel. Minimum training requirements are:

1. A 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. If the list is classified, then this requirement is waived for personnel without the appropriate security clearance and access. However, commanders will then provide unclassified examples of notional types of

critical information in order to educate their command members on the general types of information they should not divulge.

4. A listing of the Group's personnel fulfilling OPSEC responsibilities.

(4) Monitor the MCAS Beaufort public web address http://www.beaufort.marines.mil/. Unclassified, publicly available websites present a potential risk to personnel, assets, and operations if inappropriate information is published. OPSEC Program coordinator will review the command's website to ensure no critical information is published via information, graphics or photographs. Specific information prohibited for publication on the MCAS Beaufort unclassified website can be found in references (g) and (h).

(5) Public Affairs is important in garnering public support, fostering community relations, and helping with the success of military operations. Public knowledge of military operations is inevitable because of advanced technology and instant media coverage. Public Affairs staffs must be included in the OPSEC planning process where media attention is expected or desired. The need for OPSEC should not be used as an excuse to deny noncritical information to the public.

(6) Commanders and the Family Readiness Officer will stress OPSEC concerns to families to further ensure the protection of the command's critical information.

4. Administration and Logistics

a. OPSEC Process has five steps which are usually applied in a sequential order. The OPSEC process steps are:

(1) Identification of Critical Information

(2) Analysis of Threats

(3) Analysis of Vulnerabilities

(4) Assessment of Risk

(5) Application of OPSEC Measures

b. OPSEC Indicators are friendly actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information. Enclosure (3) of reference (c) lists examples of OPSEC Indicators.

c. OPSEC Vulnerability is a condition in which friendly actions provide OPSEC Indicators that may be obtained and accurately evaluated by an adversary in time to provide for a basis for effective adversary decision making.

d. OPSEC Measures are actions taken to reduce the probability of an enemy from either collecting OPSEC Indicators or to correctly analyze their meaning.

e. OPSEC Assessments is defined as an examination of an operation or activity to determine if adequate protection from adversary intelligence exploitation exists. The OPSEC assessment *is* used to verify the effectiveness of OPSEC measure and determine if critical information is being protected. An assessment cannot be conducted until after critical information has been identified. Without understanding the critical information which should be protected, there can be no specific determination that OPSEC vulnerabilities exist.

5. Command and Signal

a. Command. This plan applies to all MCAS Beaufort activities, and personnel (to include personnel from other services and civilian employees serving with MCAS Beaufort).

b. Signal. This plan is effective on the date signed.

B. C. MURTHA

MCAS BEAUFORT CRITICAL INFORMATION LIST

1. The following is the MCAS Beaufort list of Essential Elements of Friendly Information (EEFI), which constitutes critical information that requires safeguarding in order to prevent disclosure of adversaries:

a. Unit composition and disposition.

b. Deployment and redeployment destinations.

c. Deployment and redeployment timelines.

d. Logistical capabilities, limitations and constraints.

e. Intent to mobilize before public announcement.

f. Transportation capabilities and limitations.

g. Military intentions.

h. Aircraft weapon system capabilities and limitations.

i. Squadron deployment routes in/out of theatre as well as training routes.

j. Flight schedules and training requirements.

k. Monitoring international military officer training.

l. Units requesting intelligence data or simulator and airfield access via MCAS Beaufort.

m. Peacetime weapons and military movements: origin and destination of units, personnel and equipment.

n. Detachments for Training (DFT) units, training objectives, players, and logistics.

o. Noncombatant evacuation operations for destructive weather, unit evacuations, logistics, staging areas, safe havens, routes, and time lines.

p. Frequency and concept of counterterrorism training.

2. All MCAS Beaufort personnel will be made aware of these EEFIs and the importance of protecting such information as per the references.