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

AIR STATION ORDER 3070.1B

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

Subj: OPERATIONS SECURITY (OPSEC) PROGRAM

Ref: (a) DODD 5205.02E Ch 1
       (b) Joint Publication 3-13.3
       (c) MCO 3070.2A
       (d) MARADMIN 134/21
       (e) MCIEASTO 3070.1A
       (f) CG MCIEAST POLICY LETTER 05-21

Encl: (1) OPSEC Terms and Definitions

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 3070.1A Ch 1.

3. Mission. Marine Corps Air Station Cherry Point (MCAS 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

        Commander's Intent. To deny potential adversaries access to information that could be useful in developing disruptive actions to ongoing and future operations. This will be accomplished by the following

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

actions:

(a) Implementation of an OPSEC Program and policies within each command and directorate within MCAS CHERPT. MCAS CHERPT and subordinate commands, will establish an OPSEC Program and institute OPSEC policies in accordance with references (a) through (f) and this Order.

(b) Provide OPSEC training as outlined in this Order and disseminate the Commander's OPSEC Critical Information and Indicators List (CIIL).

(c) Continued education of users at all levels to raise awareness and to better control the information on the Commander's OPSEC CIIL.

(d) Commanders and supervisors at all levels continually reinforce good OPSEC practices and enforce the policies contained in references (a) through (f).

(e) The desired end-state is denial of access to critical information by potential adversaries through the elimination or mitigation of existing OPSEC vulnerabilities. OPSEC shall be coordinated and integrated into all areas to include contracting, personnel, information, cyber, acquisition and procurement, industrial, law enforcement, antiterrorism/force protection (AT/FP), and physical security.

(2) Concept of Operations

(a) OPSEC is the responsibility of each Commander and Directorate. MCAS CHERPT will develop and maintain OPSEC programs based on the references. An annual OPSEC assessment conducted on both MCAS CHERPT and Headquarters and Headquarters Squadron (HQHQRON) programs will ensure that OPSEC programs receive command attention and are evaluated in order to remain relevant. By implementing this guidance, MCAS CHERPT and HQHQRON will decrease vulnerabilities by degrading adversary abilities to collect Unclassified, but Sensitive and Critical Information.

(b) In order to reduce inadvertent disclosures, command leadership at all levels should ensure command's unclassified CIIL and OPSEC concerns are shared with military Service Members, civilian employees, on-site contractors, and civilian family members. Leaders are encouraged to use family-oriented written media and briefs provided by the OPSEC Coordinator or Monitor, to inform family members of the need for OPSEC.

b. Coordinating Instructions

(1) Commanders are responsible for their command OPSEC Program and will maintain an effective program that ensures coordination between Communications Strategy and Operations (COMMSTRAT) or media representative, Cybersecurity, Physical Security, Operations, Acquisition and Procurement, Intelligence, Naval Criminal Investigative Service (NCIS), AT/FP, Law Enforcement, Critical Infrastructure, Training, Contracting, and the command's leadership. Each OPSEC Program shall include processes to report and mitigate disclosures of OPSEC Critical Information and address the punitive and potential disciplinary actions for those who violate OPSEC through negligence or disregard of policy. Each OPSEC Program shall include mechanisms for enforcement, accountability, and the highest level of leadership oversight.

(2) Training Requirements

(a) The Installation OPSEC Coordinator shall: Attend the 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 https://www.dni.gov/index.php/ncsc-what-we-do/operations-security.

   2. Marine Corps Installations (MCIEAST) offers the Navy OPSEC Course once a year at no cost. This course is sponsored by the MCIEAST OPSEC Manager for all Marines/Civilians and is located at Camp Lejeune.

   3. 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.

   (b) HQHQRON OPSEC Coordinator must complete the OPSEC Fundamentals Course, OPSE 1301, within 30 days of appointment. The computer-based training Digital Video Disc (DVD) can be ordered by contacting the Naval Information Operations Center (NIOC) organizational mailbox, opsec@navy.mil. If the OPSEC Fundamentals Course (OPSEC 1301) cannot be obtained you may complete the "OPSEC for All" course through the National Counterintelligence and Security Center (NCSC) at https://www.dni.gov/index.php/ncsc-what-we-do/operations-security.

   (c) The Installation OPSEC Coordinator, HQHQRON OPSEC Coordinator, and HQHQRON Uniformed Readiness Coordinator (URC), along with the Installation COMMSTRAT Director and Installation 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 (active and reserve Marines, Government Civilians and Contractors) in accordance with ref (e) are:

   1. All assigned personnel are aware of the information contained on the commands (CIIL).

   2. OPSEC measures (actions that must be taken to protect CIIL information).

   3. How to protect, transmit, and destroy Controlled Unclassified Information (CUI).

   4. Risks and guidance pertaining to geolocation-capable devices, application, and services.

   5. OPSEC review procedures for public release.

   6. Annual OPSEC training can be supplemented by completing either Uncle Sam's OPSEC and Identity Management (USOPSEC/IDM-4.0) found on the Total Workforce Management Services site http://mytwms.dc3n.navy.mil or Uncle Sam's OPSEC (OPSECUS001) found on MarineNet's training module https://marinenet.usmc.mil. This supplement training does not fulfill the annual requirement alone.

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

Figure 1-1

(3) Inspections

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

    (b) The Installation OPSEC Coordinator will conduct an annual inspection of HQHQRON 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) The Installation OPSEC Coordinator and HQHQRON OPSEC Coordinator will conduct an internal inspection utilizing the Detailed Inspection Checklist, at least annually. During this annual inspection, OPSEC Coordinators shall review their command's CIIL, countermeasures, and threat statement for currency and relevance. Results from these inspections will be retained for three years.

(4) 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:

4

<u>1</u>. Advertise the OPSEC program through posters, billboards, or other media which frequently reach Marines, civilians, and contractors.

<u>2</u>. Develop slogans, logos, and other materials designed to promote their OPSEC program.

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

(5) <u>OPSEC Monitor Program</u>

(a) Each directorate is responsible for assigning, in writing, a representative to serve as the directorate OPSEC Monitor.

(b) The OPSEC Monitor will ensure each directorate maintains accountability of internal OPSEC procedures and requirements. OPSEC Monitor duties are:

<u>1</u>. Disseminate the CIIL.

<u>2</u>. Ensure all personnel within your purview have reviewed the CIIL.

<u>3</u>. Report the completion of the annual review of the CIIL to the Installation OPSEC Coordinator.

<u>4</u>. Assist the Installation OPSEC Coordinator in testing the performance of OPSEC countermeasures that are in place.

<u>5</u>. Ensure all personnel within your purview have reviewed the CG MCIEAST Policy Letter 05-21 regarding 100 percent shred policy in accordance with ref (f).

<u>6</u>. Disseminate OPSEC material/information from the Installation OPSEC Coordinator to all personnel within your purview.

(6) <u>Shred Policy</u>

(a) As part of the daily battle rhythm, a 100 percent shred policy will be followed to minimize the possible loss of critical and sensitive information. In accordance with reference (f) personnel are to shred all paper products. MCAS CHERPT uses a contracted company called "ProShred". All paper products will be put into the locked "ProShred" containers located in your building. ProShred will shred these paper products on site, once a month.

c. <u>Tasks</u>

(1) <u>Installation OPSEC Coordinator</u>

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

(e) Coordinate OPSEC education and training.

(f) Conduct an annual assessment of HQHQRON OPSEC program, utilizing the Detailed Inspection Checklist 481.

(g) Develop a CIIL in accordance with reference (c). Provide a copy of the CIIL to all personnel using the OPSEC Monitor Program.

(h) 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) HQHQRON OPSEC Coordinator

(a) Develop and implement an OPSEC program.

(b) Provide OPSEC subject matter expertise and recommendations to the Commanding Officer.

(c) Coordinate OPSEC education and training.

(d) Conduct an annual self-assessment, utilizing the Detailed Inspection Checklist 481.

(e) Provide representation to the OPSEC Working Group.

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

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

6. Command and Signal

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

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

B. C. BURKS

DISTRIBUTION: A