UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS COMMAND
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
3070
G-3/5/7
SEP 30 2015

MARINE CORPS INSTALLATIONS COMMAND POLICY LETTER 7-15

From: Commander, Marine Corps Installations Command
To: Distribution List

Subj: OPERATIONS SECURITY (OPSEC)

Ref: (a) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
(b) Joint Publication 3-13.3, "Operations Security," January 4, 2012
(c) MCO 3070.2A, The Marine Corps Operations (OPSEC) Security Program

Encl: (1) MCICOM Critical Information List (CIL)

1. Situation

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

b. While the protection of classified information remains a priority, we are also committed to the protection of unclassified open source material. Methods of collecting critical pieces of information may include Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and Open Source Intelligence (OSINT), to name a few. Today, 80 percent of collection efforts by adversaries are directed toward open source unclassified information.

c. In most cases, classified information is no longer essential or necessary to build an accurate intelligence picture of what our military forces are doing. Our objectives can be ascertained and an appropriate response developed to deny us those objectives by using the plethora of easily obtained, unprotected information. Using by now, more than ever, each Marine, Sailor, civilian Marine, and contractor 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. Marine Corps Installations Command (MCICOM) will implement an Operations Security (OPSEC) program in order to protect critical information from exploitation by any adversary seeking to impede or deny the success of our operations and support to the operating forces.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To deny potential adversaries access to information that could be useful in developing actions intended to be disruptive to military operations. This will be accomplished by the following actions:

(a) Implementation of OPSEC programs and policies for Headquarters, MCICOM.

(b) Implementation of OPSEC programs and policies throughout all Regional Installations.

(c) Continued education of users at all levels to raise awareness, promote action, and increase control over available information.

(d) To be successful, commanders and supervisors at all levels, both military and civilian, must continually reinforce the importance of good OPSEC behaviors with their subordinates. All personnel must adhere to the OPSEC policies designed and implemented to protect our information from exploitation.

(e) End State: Denial of access to critical information by potential adversaries through the elimination or mitigation of existing vulnerabilities.

(2) Concept of Operations. References (a) through (c), as well as this policy letter, are intended to provide specific guidance for OPSEC plans and program development and establishment. MCICOM will achieve the Commander's intent by developing and implementing OPSEC programs based on those references. Each command will ensure their units have appointed OPSEC Program Managers/Coordinators, developed OPSEC programs tailored to their commands, and have utilized the OPSEC planning process. Commanders should provide briefings to family members and delegate to the OPSEC practitioner the responsibility to coordinate with the Public Affairs (PAO) and the Family Readiness Officers (FRO). An annual OPSEC Assessment will ensure that the MCICOM program receives regular command attention and is continuously evaluated in order to remain relevant and effective. By implementing this guidance, MCICOM installations will decrease their vulnerabilities while reducing our adversaries' ability to collect critical information.

b. Tasks

(1) Command Inspector General (IG), MCICOM

(a) Ensure the OPSEC functional area is reviewed by inspection teams operating as part of the Commander's Inspection Program.

(2) Command Public Affairs Officer (PAO), MCICOM

(a) Serve as the PAO representative on the OPSEC Team.

(3) Assistant Chief of Staff (AC/S), G-3/5/7, MCICOM

(a) Recommend to the Commander the appropriate G-3/5/7 representative (Military or Civilian) to be the OPSEC coordinator.

(4) Assistant Chief of Staff (AC/S), G-4, MCICOM

(a) Recommend to the Commander the appropriate contracting representative (Military or Civilian) to be a member of the OPSEC Team.

(5) Assistant Chief of Staff (AC/S), G-6, MCICOM

(a) Recommend to the Commander the appropriate information management representative (Military or Civilian) to be a member of the OPSEC Team.

(6) OPSEC Coordinator, Headquarters MCICOM

(a) Maintain an updated OPSEC Manager/Coordinator point of contact listing for subordinate commands: Marine Corps Installations East (MCIEAST), Marine Corps Installations West (MCIWEST), Marine Corps Installations Pacific (MCIPAC), and Marine Corps Installations National Capital Region (MCINCR), updated at least semi-annually in October and March.

(b) Provide OPSEC support for Regional Commanders and their staff.

(c) Ensure annual reviews of Regional Command's OPSEC programs are conducted, by Mission Assurance Assessments, Commanding General's Inspection Program or internal command review. The review will be the basis for a report which will be submitted to the Information Operations and Space Integration Branch (HQMC PP&O,PLI). The format and submission date for this report will be provided via separate correspondence, by HQMC PP&O,PLI in compliance with OUSD(I) guidance.

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

1. An OPSEC policy signed by the Commander.

2. OPSEC training as outlined in paragraph 3.c.(1)(c) of reference (c).

3. A Critical Information List (CIL).

4. Sharing the CIL with the Public Affairs and the information management representative. The OPSEC coordinator will ensure the public affairs officer receives current copies of their command's CIL in order to prevent inadvertent disclosure information via public affairs programs. The information management representative will use the CIL to monitor MCICOM websites for inadvertent disclosure information via public facing websites.

5. Developing and executing OPSEC plans in support of operations and exercises (as required) in cooperation with the security manager and the information management representative. Reference (c) contains an example of a notional OPSEC plan.

6. In cooperation with the contracting representative, ensure contract requirements properly reflect OPSEC responsibilities and

are included in contracts, when applicable. Specifically, ensuring industry partners take sufficient and appropriate action to protect sensitive government information throughout the contracting process.

7. In cooperation with the information management representative, ensure all personnel posting information to official command web sites (including command sponsored social media) have completed OPSEC training per paragraph 3.c.(1)(c) of reference (c).

8. In cooperation with the information management representative, ensure all official websites (to include command-sponsored social media) are reviewed quarterly by OPSEC trained personnel to ensure they meet the OPSEC concerns listed in reference (c).

9. Ensure the public affairs officer is trained in OPSEC as outlined in reference (c).

10. Emphasize the importance of OPSEC to the FRO so they can communicate with family members semi-annually, via official communication.

11. Utilizing the Inspector General's functional area, every command will conduct an annual OPSEC assessment as detailed in reference (c). The preferred annual assessment method will be detailed by PP&O OPSEC program manager directly to the MCICOM OPSEC coordinator.

12. Establish an MCICOM OPSEC Team in accordance with reference (c). The OPSEC Team will meet as required but no less then semi-annually. The minimum composition of the OPSEC Team will be:

a. The OPSEC coordinator.

b. The Public Affairs Officer.

c. The Contracting Representative.

d. The Information Management Representative.

(7) Regional Commanding Generals/Commander (MCIPAC, MCIWEST, MCIEAST, and MCINCR)

(a) Appoint in writing an officer, staff noncommissioned officer, or equivalent Department of Defense General Schedule employee as OPSEC Program Managers/Coordinators to:

1. Provide OPSEC subject matter expertise and recommendations.

2. Coordinate OPSEC matters with the MCICOM OPSEC Program coordinator.

3. Coordinate OPSEC education and training for members of the staff and command.

4. Coordinate and conduct periodic internal reviews and assessments under the OPSEC program.

5. Conduct annual OPSEC review.

a. Submit a copy of annual assessment findings to MCICOM OPSEC coordinator.

b. Coordinate with MCICOM OPSEC coordinator for inspections and support as needed.

(b) Develop, implement, maintain, and promulgate an OPSEC order in accordance with reference (c) and this policy.

(c) Ensure subordinate commands and units have meet the requirement for OPSEC as outlined in reference (c) and this policy.

(d) Assign responsibility for your commands OPSEC program development, implementation, and oversight.

(e) Develop OPSEC education and awareness program per reference (c) and this policy.

c. Coordinating Instructions

(1) At a minimum, the following will be included as part of OPSEC education programs:

(a) MCICOM OPSEC Program Managers/Coordinators will attend the Interagency OPSEC Support Staff (IOSS) OPSEC Analysis and Program Management resident course or equivalent course, within 90 days of appointment. Registration is through IOSS listed under "Training."

1. Registration for the OPSE course can be completed at http://www.ioss.gov or via email at ioss@radium.ncsc.mil.

2. There will be a six month grace period to complete the IOSS OPSEC course, following the publication date of this policy.

3. Current program managers and coordinators who have completed the Navy's OPSEC course or the Headquarters Department of the Army's OPSEC Level II course will have satisfied this requirement.

(b) All OPSEC program managers and coordinators must complete the OPSEC fundamentals course, within 30 days of appointment. This course can be completed through the IOSS, listed under "Training." It is highly recommended to also attend the resident OPSEC Analyses Course. Registration is through IOSS listed under "Training."

(c) Minimum annual OPSEC training requirements for all personnel are:

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

2. An overview of the OPSEC training process.

3. OPSEC and social media.

4. The commands current CIL.

5. A list of the commands personnel fulfilling OPSEC responsibilities will be maintained with the G-3/S-3 and be made available upon request.

6. The on-line 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 as outlined in reference (c). To complete the requirement commands are required to provide a copy of the CIL and show the commands OPSEC relationship to the security, intelligence, and cyber security programs.

(2) Enclosure (1) is the MCICOM CIL.

4. Administration and Logistics

a. Administration

(1) Provide contact information of OPSEC Program Managers/Coordinators to the MCICOM OPSEC coordinator. The MCICOM OPSEC coordinator will be immediately notified of any changes to contact information.

(2) Submit OPSEC survey information to the MCICOM OPSEC coordinator when requested.

b. Logistics

(1) Capture all costs associated with the OPSEC program for future budgetary adjustments.

(2) When requested, submit cost data to MCICOM OPSEC coordinator.

5. Command and Signal

a. Command. This policy letter is applicable to MCICOM Headquarters and MCICOM Regions.

b. Signal. This policy letter is effective the date signed.

C. L. HUDSON

DISTRIBUTION: C

CRITICAL INFORMATION LIST (CIL)

1. **Personnel Information**

a. Privacy Act information

b. Joint Personnel Adjudication System (JPAS) data

c. Standard Labor Data Collection & Distribution Application (SLDCADA) data

d. Defense Travel System (DTS) data

e. Training records

f. Timecards(SLDCADA)

2. **Unit Information**

a. Appointment letters

b. Access rosters

c. Work schedules

d. Personnel strengths and shortfalls

e. Watch schedules and reaction times

3. **Facilities Information**

a. Identification of any "open access" entry control points

b. GIS or other mapping sources with specific plain language identification of sensitive areas, i.e., II MEF HQTRS vice HP1

c. Building schematics which are available open source

d. Specific CG/CO office location within headquarter buildings

e. Mission Essential Vulnerable Area(MEVA) list

f. Critical infrastructure locations and schematics, i.e., water systems, electrical grids, communications, etc.

g. Maintenance requests and contracts

h. Future construction project information

i. Contract information

j. Planned land use

k. Locations of sensitive storage sites (HAZMAT, arms, ammunition, explosives), map and text

4. **Equipment/Specialized Equipment Information**

a. Security camera location/capability

b. IDS systems location/capability

c. CBRNE (chemical, biological, radiological, nuclear, high-explosive) sensor location/capability

d. Equipment capabilities

5. **Plans, Policies, and Procedures**

a. AT Plan

b. Integrated Action Sets

c. Special Orders

d. Security plans

e. CBRNE response capabilities, guidelines and procedures

f. FPCON security augmentation requirements

g. DoD School Critical Incident Plans

h. Installation and unit Random Antiterrorism Measures (RAMs)

6. **IT Systems/Communications Systems Information**

a. System Authorization Access Request (SAAR) Database

b. System Security Accreditation Agreement (SSAA) data with associated IP addresses

c. Information Assurance Vulnerability program data

d. Interim Approval to Operate/Connect (IATO/IATC) data

e. Protected Distribution System (PDS) approvals

f. CAC PIN reset information

7. **Reports, Surveys, Administrative Information, Related Documentation**

a. Security Assessments

b. PMO physical security and crime prevention surveys

c. Law enforcement sensitive information, i.e., Threat and Location Observation Notices (TALON), FBI Alerts, etc.

d. PMO, Brig, and FESD incident reports, traffic accident reports, etc.

e. PMO blotters, desk journals, stats sheets, etc.

f. Safety Mishap reports and associated records

g. Completed or ongoing internal and criminal investigations

8. **Special Event Information**

a. Distinguished visitor information

b. Schedules of events

c. Locations of Events

d. Special events LOIs

9. **Logistics Information**

a. Freight shipment data associated with particular Exercises or Operations

b. Billing/Accounting data

c. TMO Personal Property Files

d. Transportation Operational Personal Property System (TOPPS) data