



UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS NATIONAL CAPITAL REGION
MARINE CORPS BASE QUANTICO
3250 CATLIN AVENUE
QUANTICO, VIRGINIA 22134-5001

IN REPLY REFER TO:
MCINCR-MCBQO 3070.1
B 033
23 Oct 2017

MARINE CORPS INSTALLATIONS NATIONAL CAPITAL REGION - MARINE
CORPS BASE QUANTICO ORDER 3070.1

From: Commander, Marine Corps Installations National Capital
Region - Marine Corps Base Quantico

To: Distribution list

Subj: OPERATIONS SECURITY (OPSEC)

Ref: (a) DoD Directive 5205.02E, DoD Operations Security
(OPSEC) program
(b) Joint Publication 3-13.3, Operations Security
(c) MCO 3070.2A, Marine Corps Operations Security (OPSEC)
Program

Encl: (1) OPSEC Terms and Definitions
(2) Training Requirements
(3) MCINCR-MCBQ Critical Information List
(4) Social Media
(5) OPSEC Assessments

1. Situation

a. Information of all types can be used by our adversaries to interfere with or compromise our operations and activities. All personnel must be aware of their responsibility to protect potentially useful information.

b. Operations Security (OPSEC) is the process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to:

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

(2) Determine OPSEC indicators that may be obtained by hostile intelligence systems that could be interpreted or pieced together to derive critical information.

(3) Eliminate or reduce exploitation of friendly actions to adversaries.

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

23 Oct 2017

c. OPSEC terms and definitions are outlined in enclosure (1) of this order.

d. All USMC organizations will promulgate policies and procedures for maintaining an effective OPSEC program.

2. Mission. In accordance with references (a) through (c), Marine Corps Installations National Capital Region - Marine Corps Base Quantico (MCINCR-MCBQ) conducts a comprehensive OPSEC program in order to identify, control and protect critical information from exploitation by adversaries.

3. Execution

a. Commander's Intent. The purpose of the MCINCR-MCBQ OPSEC program is to protect friendly information and deny its use by our adversaries. We will accomplish this by conducting a comprehensive OPSEC program as outlined in this order. The endstate is that sensitive information that could compromise operations is protected from exploitation from our adversaries.

b. Concept of Operations. The MCINCR-MCBQ OPSEC program is executed in six elements:

(1) Program Management. OPSEC is a command responsibility that requires close coordination among the staff, subordinate organizations and tenant commands. Though each commander is required to assign an OPSEC coordinator to manage the command's OPSEC program, other members of the staff have a significant role in supporting the OPSEC effort. In addition to the primary staff, key OPSEC support personnel include:

(a) OPSEC Program Coordinator. Manages the overall OPSEC program, oversees and conducts OPSEC training and exercises, and submits required OPSEC reports. The MCINCR-MCBQ OPSEC coordinator must be designated in writing and have completed OPSEC training. Each subordinate command shall also appoint a command OPSEC coordinator.

(b) Public Affairs Officer (PAO). Public Affairs is important in garnering public support, fostering community relations, and helping with the success of base operations. Because of advanced technology and social media, the public often has instant access to many aspects of military operations. Therefore Public Affairs staffs must be included in the OPSEC planning process so that they can ensure information is properly

screened before it is released to the public. All PAO personnel shall complete OPSEC training.

(c) Family Readiness Officer (FRO). FRO's are the voice of the command for family members and utilize various social media venues to communicate with the family members. The FRO's role in ensuring adherence to OPSEC rules when using social media is critical. FRO's are required to complete OPSEC training.

(2) OPSEC Planning

(a) A MCINCR-MCBQ OPSEC plan is developed and maintained IAW the references.

(b) Subordinate MCINCR-MCBQ commands shall develop OPSEC plans that are in accordance with the references and aligned with the MCINCR-MCBQ plan.

(3) Education and Awareness. Education and awareness will be achieved during unit annual training and continuously by the Public Affairs Office using social media (Facebook, Twitter, MCB Quantico website) and the base newspaper.

(4) Training

(a) Key OPSEC personnel (OPSEC Program Coordinators, PAO, and FRO's) must complete required training as outlined in enclosure (2).

(b) All personnel must complete annual OPSEC training as outlined in enclosure (2).

(5) Assessments. An annual MCINCR-MCBQ command level OPSEC assessment is conducted to ensure that the overall OPSEC program is functioning IAW the references. Subordinate commands shall also conduct an assessment of their respective OPSEC program in support of the overall command assessment. Subordinate commands shall submit the results of their assessments to the MCINCR-MCBQ Program Coordinator. Assessments shall be conducted as outlined in enclosure (5).

(6) Reporting. OPSEC reports are submitted annually and are used to identify the readiness and effectiveness of the OPSEC program. Annual reports are submitted to MCICOM by the MCINCR-MCBQ Program Coordinator.

c. Tasks

(1) Assistant Chief of Staff, G-3

(a) Appoint in writing an Officer, Staff Non-Commissioned Officer, or equivalent Department of Defense civilian to serve as the MCINCR-MCBQ OPSEC Program Coordinator to:

1. Plan and execute the MCINCR-MCBQ OPSEC Program.

2. Provide oversight to ensure all subordinate command OPSEC Program Coordinators and locally assigned FRO's receive proper training within 30 days of assignment.

3. Ensure all personnel assigned to MCINCR-MCBQ receive annual OPSEC training.

4. Serve as chairperson of the MCINCR-MCBQ OPSEC working group.

5. Conduct an annual command level assessment of the MCINCR-MCBQ OPSEC program.

(b) Develop and implement the command OPSEC program. At a minimum, the program shall include:

1. An OPSEC Order

2. OPSEC training

3. Development of a Critical Information List (see enclosure (3)).

4. Identifying the importance of OPSEC to family members.

5. Contract support and oversight to ensure adherence to OPSEC program requirements. When contacted by the DSS, ensure contract industrial security efforts are adequate.

6. Web site reviews to ensure they meet the OPSEC requirements listed in enclosure (4) of this order.

7. Information sharing with the Public Affairs Officer. OPSEC Coordinators will ensure that Public Affairs

23 Oct 2017

Officers receive current copies of their command's Critical Information List in order to prevent inadvertent disclosure of information.

8. Command level OPSEC assessment in accordance with enclosure (5).

9. Incorporation of OPSEC principles into all operations and exercises.

(2) Public Affairs Officer

(a) Conduct quarterly reviews of all MCINCR-MCBQ social networking sites to ensure they do not violate the command OPSEC policy. Document the results of the review and submit the findings to the MCINCR-MCBQ OPSEC Program Coordinator.

(b) Ensure all MCINCR-MCBQ social networking sites contain the following disclaimer: "This is an official Marine Corps page. However, the appearance of hyperlinks does not constitute endorsement by the U. S. Marine Corps. The U. S. Marine Corps does not exercise any editorial control over the information you may find at linked locations."

(c) Utilize social media and the Base newspaper to promote good OPSEC practices and ensure the base population is aware of the importance of OPSEC.

(3) Commanding Officer, Headquarters & Service Battalion

(a) Establish and maintain an effective OPSEC program in accordance with the references.

(b) Appoint in writing an Officer, Staff Non-Commissioned Officer, or equivalent Department of Defense civilian to serve as the OPSEC Program Coordinator.

(c) Conduct annual OPSEC program assessments and submit the results to the MCINCR-MCBQ OPSEC Program Coordinator.

(d) Ensure FRO's complete the required OPSEC training as outlined in enclosure (2).

(4) Commanding Officer, Security Battalion

(a) Establish and maintain an effective OPSEC program in accordance with the references.

(b) Appoint in writing an Officer, Staff Non-Commissioned Officer, or equivalent Department of Defense civilian to serve as the OPSEC Program Coordinator.

(c) Conduct annual OPSEC program assessments and submit the results to the MCINCR-MCBQ OPSEC Program Coordinator.

(d) Ensure FRO's complete the required OPSEC training as outlined in enclosure (2).

(5) Commanding Officer, Marine Corps Air Facility Quantico

(a) Establish and maintain an effective OPSEC program in accordance with the references.

(b) Appoint in writing an Officer, Staff Non-Commissioned Officer, or equivalent Department of Defense civilian to serve as the OPSEC Program Coordinator.

(c) Conduct annual OPSEC program assessments and submit the results to the MCINCR-MCBQ OPSEC Program Coordinator.

(d) Ensure FRO's complete the required OPSEC training as outlined in enclosure (2).

(6) Director, Regional Contracting Office. Review all contracts to ensure they meet the OPSEC requirements in accordance with reference (c).

d. Coordinating Instructions

(1) OPSEC Working Group

(a) The OPSEC working group will be incorporated into the Mission Assurance Working Group that is held quarterly. Additional OPSEC working groups will be scheduled as required.

(b) The MCINCR-MCBQ OPSEC Coordinator will chair the OPSEC Working Group.

23 Oct 2017

(2) When feasible, all units/commands will shred documents containing command critical or sensitive information prior to being discarded.

(3) All violations of OPSEC will be reported to the OPSEC coordinator, who will then notify the chain of command.

(4) Excessive OPSEC. Excessive OPSEC can degrade operational effectiveness by interfering with activities such as coordination, training, and logistical support. Military operations are inherently risky, therefore, commanders must evaluate each activity and operation and then balance required OPSEC measures against operational needs. Using the OPSEC process will help commanders assess the risk and apply appropriate OPSEC measures.

4. Administration and Logistics

a. Administration. The MCINCR-MCBQ OPSEC Coordinator is responsible for completing and submitting an annual OPSEC report to MCICOM.

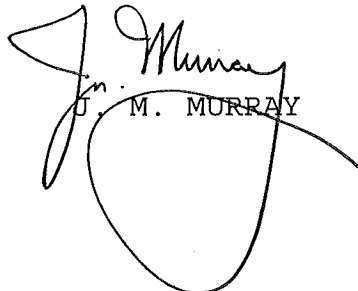
b. Logistics. None.

5. Command and Signal

a. Command. This Order applies to all Marine Corps activities, commands, units, and personnel (to include personnel from other services, civilian employees, and contractors) assigned to MCINCR-MCBQ.

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

Distribution: A


J. M. MURRAY

OPSEC TERMS AND DEFINITIONS

1. Critical Information. These are specifics about friendly intentions, capabilities, and activities collected by adversaries and used to delay or disrupt friendly mission accomplishment.
2. Indicator. These are friendly detectable actions and open sources of information that adversary intelligence systems can detect, obtain and then interpret to derive friendly critical information.
3. OPSEC Assessments. 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 measures and determine if critical information is being protected. An assessment cannot be conducted until critical information has been identified. Without understanding critical information, which should be protected, there can be no specific determination that OPSEC vulnerabilities exist.
4. OPSEC Measures. These are actions taken to reduce the probability of an enemy's collection and analysis of OPSEC indicators.
5. OPSEC Process. OPSEC planning is accomplished through the OPSEC process. The five steps involved in the OPSEC process are; identification of critical information, threat analysis, vulnerability analysis, risk assessment, and application of OPSEC measures.
6. OPSEC Program Managers and Coordinators. Program Managers are personnel who perform OPSEC functions as their primary duty. Coordinators are personnel who perform OPSEC functions as an additional duty. Commanders will use their discretion in determining whether they require Program Managers or Coordinators to fulfill their OPSEC responsibilities.
7. OPSEC Working Groups. A group of subject matter experts from the command's organization designed to assist the command with OPSEC matters and the OPSEC program.
8. Threat. Any individual or organization that seeks to do harm by interrupting ongoing military operations or activities. In order to be classified as a threat, both of the following conditions must be satisfied:

23 Oct 2017

a. An intent to do harm must exist.

b. A capability to do harm must exist.

9. Vulnerability. A condition in which friendly actions provide OPSEC indicators that may be obtained and evaluated by an adversary and used for effective decision making.

Training Requirements

1. All OPSEC Program Managers and Coordinators must complete an OPSEC Fundamentals Course within 30 days of appointment. The course is available on-line. It is listed as "CBT 1301" and is available by registering at the Interagency OPSEC Support Staff website at

<https://webarchive.library.unt.edu/eot2008/20090117192804/http://www.iooss.gov/training/1301.html>. Copies of this course can be attained 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.

2. All Family Readiness Officers must complete an OPSEC Fundamentals Course within 90 days of appointment. The course is available on-line. It is listed as "CBT 1301" and is available by registering at the Interagency OPSEC Support Staff website at

<https://webarchive.library.unt.edu/eot2008/20090117192804/http://www.iooss.gov/training/1301.html>. Copies of this course can be attained 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.

3. Annual OPSEC training (Uncle Sam's OPSEC) is required for all command personnel. Computer based training is available at the MarineNet website at <https://www.marinenet.usmc.mil> under course OPSECUS001 (Uncle Sam's OPSEC). Minimum training requirements are:

- a. A definition of OPSEC and its relationship to the command's security and intelligence programs.
- b. An overview of the OPSEC process.
- c. The command's current critical information requirements.
- d. A listing of the command's personnel fulfilling OPSEC responsibilities.

23 Oct 2017

MCINCR-MCBQ Critical Information List

1. Items contained in the Critical Information List (CIL) are sought by adversaries to disrupt and delay mission accomplishment. These items are sensitive in nature and close attention should be given to avoid disclosure.

a. Personal Information

- (1) Privacy Act Information
- (2) Joint Personnel Adjudication System data
- (3) Standard Labor Data Collection and Distribution Application (SLDCADA) data
- (4) Defense Travel System data
- (5) Training Records
- (6) Vehicle Registration data
- (7) Home addresses of any personnel

b. Unit Information

- (1) Appointment Letters
- (2) Access Rosters
- (3) Work Schedules
- (4) Personnel strengths and shortfalls
- (5) Watch schedules and reaction times for first responders
- (6) Training data of units using MCBQ to include Camp Upshur

c. Facilities Information

- (1) Identification of any "open access" entry control points
- (2) Specific Commanding General/Commanding Officer office locations within Headquarters buildings

23 Oct 2017

(3) Critical Infrastructure locations and schematics

(4) Location of sensitive storage sites (hazardous materials, arms, ammunition, explosives), map and text

d. Equipment/Specialized Equipment Information

(1) Security camera location/capability

(2) Intrusion Detection Systems location/capability

(3) CBRNE sensor location/capability

(4) Equipment capabilities

e. Plans, Policies, and Procedures

(1) FPCON Integrated Action Sets

(2) Special orders

(3) Security plans

(4) CBRNE response capabilities, guidelines and procedures

(5) Force protection security augmentation requirements

(6) DODEA School Critical Incident Plans

(7) Installation and unit Random AT Measures (RAM)

f. IT Systems/Communications Systems Information

(1) System authorization access request database

(2) Interim approval to operate/connect data

(3) Protected distribution system approval

(4) System Security Accreditation Agreement data with associated Internet Protocol that addresses Information Assurance Vulnerability program data

(5) Common Access Card Personal Identification Number reset information

23 Oct 2017

g. Reports, Surveys, Administrative Information, and Related Documentation

- (1) Security Assessments
- (2) Provost Marshal's Office (PMO) physical security and crime prevention surveys
- (3) Law Enforcement sensitive information
- (4) PMO, and Fire & Emergency Services incident reports, traffic accident reports, etc.
- (5) PMO blotters, desk journals, stats sheets, etc.
- (6) Safety mishap reports and associated records
- (7) Completed and ongoing command and criminal investigations

h. Special Event Information

- (1) Distinguished visitor information
- (2) Schedules of certain high level events
- (3) Locations of certain high level events
- (4) Special events Letters of Instruction

i. Logistics Information

- (1) Freight shipment data associated with exercises or operations
- (2) Billing/accounting data
- (3) Traffic Management Office Personal Property files

23Oct 2017

Social Media

1. Unclassified, publicly available websites present a potential risk to personnel, assets, and operations if inappropriate information is published. OPSEC Officers will review their command's website to ensure no critical information is published (data, graphics, or photographs).

2. Unclassified, publicly available websites shall not include classified material, "For Official Use Only" information, proprietary information, or information that could enable the recipient to infer this type of information. This includes, but is not limited to, lessons learned or maps with specific locations of sensitive units, ship battle orders, threat condition profiles, etc., activities or information relating to ongoing criminal investigations into terrorist acts, force protection levels, specific force protection measures being taken or number of personnel involved, Plans of the Day, or Plans of the Month. When it is necessary to gain release authority from a senior in the chain of command, subordinate commands will submit material for clearance only after it has been reviewed and necessary amendments made to the fullest capability of the submitting command.

3. Unclassified, publicly available websites shall not identify family members of Department of the Navy personnel in any way including; in photos or photo captions, except for the spouses of senior leadership who are participating in public events such as a ship naming or commissioning, etc. Furthermore, family member information will not be included in any online biographies.

4. Unclassified, publicly available websites shall not display personnel lists, "roster boards", organizational charts, or command staff directories which show individuals' names, phone numbers, or e-mail addresses which contain the individual's name. General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable. The names, telephone numbers, and personalized official e-mail addresses of command/activity public affairs personnel and/or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories.

23Oct 2017

5. Biographies of general officers, commanders, commanding officers, officers in charge, executive officers or deputies, the civilian equivalents of those officers just listed, and Master Gunnery Sergeants or Sergeants Major may be posted to command unclassified, publicly available websites. However, biographies published on unclassified, publicly accessible websites will not include date of birth, current residential location, nor any information about family members.

23 Oct 2017

OPSEC ASSESSMENTS

1. General. The purpose of the OPSEC assessment is to thoroughly examine 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 measures. The assessment will determine if critical information identified during the OPSEC planning process is being protected. An assessment cannot be conducted until after an operation or activity has at identified its critical information. Without a basis of critical information, there can be no specific determination that actual OPSEC vulnerabilities exist.

2. Requirement

a. Each command will conduct an annual command assessment using the Inspector General's Checklist criteria.

b. Any command may request a formal assessment after they have completed their command assessment. Because of the extremely limited number of formal assessments which can be conducted, HQMC/PP&O/PLI will consolidate and prioritize requests from Marine Corps commands.

3. There are two types of assessments: Command and Formal.

a. The majority of USMC assessments will be a Command assessment. The scope of these assessments can vary depending on the commander's guidance. Recognizing that an all-encompassing assessment would levy a high burden on a typical command, commanders are encouraged to develop an approach in which functions are routinely evaluated, but done so over a period of time. For example, a commander could evaluate administrative OPSEC during one field exercise, while evaluating website OPSEC on the next exercise.

b. A formal assessment is composed of and conducted by members from within and outside the command. The formal assessment will often cross command lines and needs to be coordinated appropriately. Formal assessments are normally directed by higher headquarters to subordinate echelons, but may be requested by subordinate commands. Each OPSEC assessment is unique because of the different activities of varying units. Additional factors are the nature of the information to be protected, the enemy's intelligence collection capabilities, and the environment of the activity to be surveyed.

4. OPSEC assessments differ from security inspections in that security inspections seek to ensure compliance with directives and regulations concerning classified material, and security of physical structures/installations. However, assessment teams should also ensure that security measures are not creating OPSEC indicators.

5. Assessments are not to be used as a punitive tool, but should be conducted on a non-attribution basis. This will ensure better cooperation and honesty when surveying activities, plans, and operations.

6. Results of assessments should be given to the commander of the unit surveyed. Results may also be forwarded to higher headquarters on a non-attribution basis to derive lessons learned that may be applied to other units within the Marine Corps.

7. The OPSEC Assessment is composed of the following phases (planning, field assessment, and analysis and reporting).

a. OPSEC Assessment Planning Phase

(1) Determine the Scope. Limit the extent of the assessment to manageable proportions based on time, geography, units to be observed, operations or activities to be observed, staffing, funding, and other practical considerations. As outlined in reference (b), the following areas could be evaluated: Intelligence Collection Operations; Logistics; Communications; Operations; and Administration and Support. See Enclosure (7) for Functional Outlines and Profile Guidelines for these areas.

(2) Select the Assessment Team Members. Select members from the various staff functions (e.g. intelligence, communications, logistics, administration, operations, FRO, MCCS, PAO) to ensure an adequate breadth of expertise. OPSEC is an operations function, so the team OIC should be from the S-3/G-3.

(3) Understand the Operation or Activity to be Assessed. Team members must be thoroughly briefed on the operation plan, and any other matters affecting the operation. This will help team members develop a functional outline for the aspect of the operation they are responsible to survey.