



UNITED STATES MARINE CORPS  
I MARINE EXPEDITIONARY FORCE  
U. S. MARINE CORPS FORCES, PACIFIC  
BOX 555300  
CAMP PENDLETON, CA 92055-5300

I MEFO 3070.2A  
G-3  
APR 1 2016

I MARINE EXPEDITIONARY FORCE ORDER 3070.2A

From: Commanding General  
To: Distribution List

Subj: I MARINE EXPEDITIONARY FORCE (I MEF) OPERATIONS SECURITY  
(OPSEC) PROGRAM

Ref: (a) DOD Directive 5205.2E, DOD Operations Security  
(OPSEC) Program  
(b) MCO 3070.2A, The Marine Corps Operations Security  
(OPSEC) Program  
(c) Joint Publication 3-13.3

Encl: (1) OPSEC Terms and Definitions  
(2) Example OPSEC Plan  
(3) Training Requirements  
(4) Examples of Critical Information  
(5) Unclassified Website OPSEC  
(6) Example OPSEC Assessment  
(7) I MEF Critical Information List

1. Situation

a. Purpose. To establish policy and procedures for the Operations Security Program within I MEF and its Major Subordinate Commands and Elements (MSCs/MSEs), as well as any commands or units that may be assigned or attached to I MEF.

b. Background. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities by carrying out the following tasks:

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

(2) Determining potential OPSEC indicators adversary intelligence systems might obtain, which could be used to derive critical information in sufficient time to be useful to adversaries.

(3) Selecting and executing OPSEC measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

(4) Incorporating OPSEC during the planning, preparation, execution, and post-execution of operations and activities to achieve essential secrecy.

(5) Ensuring OPSEC is a continuous process that contributes to the overall effort for mission success and allows each individual to participate in the process on a daily basis.

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

APR 1 2016

c. Definitions. See enclosure (1).

2. Cancellation. I MEF Policy Letter 3-11.

3. Mission. I MEF will maintain an aggressive and effective OPSEC program that promotes education and awareness to ensure all I MEF personnel are responsible for and prepared to support OPSEC, safeguarding information in order to deny an adversary or potential adversary access to critical information that could be used to predict friendly intentions, capabilities, or activities.

4. Execution

a. Commanders Intent. To prevent an adversary or potential adversary from obtaining critical information that facilitates the prediction of friendly intentions, capabilities, or activities that pertain to I MEF operations.

b. Concept of Operations. In accordance with references (a) and (b), ensure that unclassified, but sensitive information, is being safeguarded and all Marines, civilians, and contractors assigned to I MEF are using proper OPSEC measures. This will be accomplished by:

- (1) Appointing appropriate OPSEC Program Managers/Coordinators.
- (2) Maintaining an OPSEC plan, in accordance with enclosure (2).
- (3) Exercising a rigorous education and awareness campaign.
- (4) Conducting required training for key personnel as outlined in enclosure (3).
- (5) Conducting annual command level assessments.
- (6) Submitting annual reports to HQMC.
- (7) Incorporating OPSEC into planning and execution.
- (8) Establish an OPSEC Working Group.
- (9) Incorporate OPSEC into the contracting process.

c. Tasks

(1) All I MEF Staff Sections. Appoint in writing an officer, staff Noncommissioned officer, or appropriate Department of Defense (DoD) civilian to serve on and support the collective efforts of the I MEF OPSEC working group.

(2) Assistant Chief of Staff (AC/S) G-1, I MEF

(a) AC/S G-3 in planning, coordinating, and executing security support during the drafting and reviewing of OPSEC plans.

(b) Provide functional expertise, as required, in the planning, execution, and analysis of command OPSEC assessments of the I MEF command element.

APR 1 2016

(3) AC/S G-2, I MEF

(a) Assist the AC/S G-3 in planning, coordinating, and executing counterintelligence support during the drafting and reviewing of OPSEC plans.

(b) Provide functional expertise, as required, in the planning, executing, and analysis of command OPSEC assessments of the I MEF command element.

(c) Provide threat analysis to the OPSEC working group to identify adversaries, or potential adversaries, to include intent and capability to collect sensitive, but unclassified, information.

(4) AC/S G-3, I MEF

(a) Serve as lead agency and program manager on OPSEC matters for I MEF.

(b) Develop, maintain, and disseminate an OPSEC order and program for I MEF.

(c) Chair OPSEC working groups as required. Working groups consisting of representatives from all Staff Sections including Assistant Chief of Staff G-6, Public Affairs Officer, and Family Readiness Officer will:

1. Coordinate OPSEC matters amongst the I MEF staff and MSCs/MSEs.

2. Assist in development and implementation of the command OPSEC program.

(d) In accordance with ref (b), appoint in writing an officer, staff Noncommissioned officer, or DoD equivalent civilian as OPSEC Program Manager or Coordinator to perform the following duties:

1. Provide OPSEC subject matter expertise and recommendations to the commander.

2. Develop, coordinate, and maintain the command OPSEC program to include writing policy/guidance documents.

3. Develop and coordinate OPSEC education and training.

4. Coordinate command OPSEC assessment.

5. Conduct the annual OPSEC program review.

6. Submit annual OPSEC reports.

7. Provide assistance to MSC/MSE OPSEC managers/coordinators as required.

(5) Public Affairs Officer, I MEF

(a) Assist the AC/S G-3 in planning, coordinating, and executing public affairs support during the drafting and reviewing of OPSEC plans.

APR 1 2016

(b) Receive and support application of the I MEF Critical Information List (CIL) and safeguard the data categories it contains.

(c) Ensure public affairs programs prevent inadvertent disclosure of CIL items.

(d) Execute activities and efforts as required to prevent the publishing of inappropriate information on public facing websites, social media, or other such information sources. Completion of reviews of such sites will be reported and documented quarterly to the I MEF OPSEC Program Manager/Coordinator. Inappropriate/unapproved information includes, but is not limited to:

1. For Official Use Only (FOUO) information
2. Classified information
3. Critical information
4. Identity of family members
5. Biographies that contain family information
6. Personnel roster, organizational charts, and staff directories that contain individual names

(e) Ensure completion of all required formal training for public affairs and webmaster personnel per reference (b) and forward training completion documentation to the I MEF OPSEC Program Manager/Coordinator.

(6) AC/S G-6

(a) Support the development of threat assessments and their use in OPSEC process applications and the OPSEC program generally, as vulnerability analysis, risk assessment, and identification of measures and countermeasures are conducted.

(b) Assist the AC/S G-3 in planning, coordinating, and executing information management support during the drafting and reviewing of OPSEC plans.

(c) Support activities and efforts to prevent the publishing of inappropriate information on public facing websites, social media, or other such information sources. Support will be directly to the I MEF OPSEC Program Manager/Coordinator, who has direct responsibility, and to I MEF Public Affairs, who will take lead in executing these functions.

(7) Family Readiness Officer, I MEF

(a) Assist the AC/S G-3 in planning, coordinating, and executing family readiness support during the drafting and reviewing of OPSEC plans.

(b) Ensure family readiness programs prevent inadvertent disclosure of CIL items.

(c) Execute activities and efforts as required to prevent the publishing of inappropriate information on public facing websites, social

media, or other such information sources. Inappropriate/unapproved information includes but is not limited to:

1. For Official Use Only (FOUO) information
2. Classified information
3. Critical information
4. Identity of family members
5. Biographies that contain family information
6. Personnel roster, organizational charts, and staff directories that contain individual names.

(8) Command Inspector General, I MEF

(a) Evaluate OPSEC as part of each unit's Command Inspection Program and the Commanding General's Readiness Inspection (CGRI) Programs. Inspection teams will review the OPSEC functional area of all commands visited by the Inspector General (IG) teams.

(b) The IG Marine Corps (IGMC) maintains an online database of Functional Area Checklists (FAC). The website at which units will find the most recent OPSEC FAC (481) is:  
<http://www.hqmc.marines.mil/igmc/Resources/FunctionalAreaChecklists.aspx>

(9) Security Manager, I MEF

(a) Support the development of threat assessments and their use in OPSEC process applications and the OPSEC program generally, as vulnerability analysis, risk assessment, and identification of measures and countermeasures are conducted.

(b) Coordinate staff security training with I Marine Expeditionary Force Headquarters Group (I MHG) and I MEF OPSEC Program Manager/Coordinator to ensure the inclusion of required OPSEC training topics and the maintenance of training completion/attendance records.

(10) All Commanding Generals and Commanding Officers

(a) Develop and publish a command OPSEC program tailored to the command's mission. At a minimum, the program shall consist of:

1. An OPSEC order signed by the commander.
2. OPSEC training as outlined in enclosure (3).
3. Development of a CIL as in enclosure (4). OPSEC managers/coordinators will ensure the Public Affairs and Family Readiness Officers receive current copies of the command's CIL in order to prevent inadvertent disclosure of this information.
4. Developing and executing plans in support of operations and exercises in cooperation with the Anti-terrorism Officer, Physical Security Manager, Cyber Security, and the Intelligence Officer.

5. Ensuring 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, and when contacted by the Defense Security Service, (DSS), support them in their role of ensuring contract industrial security efforts are adequate).

6. Ensuring the unit understands social networking concerns, periodically reviews unit operated websites and meets the OPSEC responsibilities listed in enclosure (5) of this Order.

7. Conducting assessments and program reviews in accordance with enclosure (6) to include, at a minimum:

a. Conducting an annual, command level OPSEC assessment utilizing the IG's Inspection Checklist.

b. Registering the OPSEC Program Manager/Coordinator for an Enterprise Protection Risk Management (EPRM) account within 30 days of appointment (EPRM is an automated risk assessment process that will assist planners and program managers/coordinators in the evaluation of risks posed to an organization's critical information) at the following website: <https://eprm.csd.disa.smil/mil> on SIPRNET.

(b) Appoint in writing an officer or staff non-commissioned officer as the OPSEC Program Manager or Coordinator.

(c) Consolidate OPSEC Lessons Learned as part of the Marine Corps Lessons Learned Program and ensure these lessons are passed to the I MEF OPSEC Program Manager/Coordinator for inclusion in the Joint Staff's Lessons-Learned Database.

d. Coordinating Instructions

(1) OPSEC is a command responsibility under the cognizance of the G-3. If a command has an Information Operations Officer or cell, that individual or group may be tasked with managing the command's OPSEC program; however, the OPSEC program will be closely coordinated with other staff sections.

(2) 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, the commander must evaluate each activity and operation and balance required OPSEC measures against operational needs. Using the OPSEC process will help commanders assess the risk and apply appropriate OPSEC measures.

(3) OPSEC Violations. All violations of OPSEC will be reported to the OPSEC Program Manager/Coordinator, who will then notify the chain of command.

5. Administration and Logistics

a. Administration

(1) Points of Contact. MSCs/MSEs will collect contact information on OPSEC Program Managers and Coordinators within I MEF and provide to the I MEF OPSEC Program Manager/Coordinator. The OPSEC Program Manager/Coordinator will be notified of any changes to contact information immediately.

(2) Inspections. Records of all assessments and program reviews will be retained for three years. Enclosure (6) outlines further detail.

(3) Report Submission. MSCs/MSEs will submit command OPSEC reports by unit OPSEC Program Managers/Coordinators with information consolidated from subordinates and submitted to I MEF AC/S G-3 semi-annually. Reports are due at the end of June and December. The report will be a Microsoft Word document with the following information:

(a) OPSEC program status.

(b) Activities conducted during the reporting period that support the OPSEC program or command OPSEC posture (for example, training classes, working group meetings, assessments, program reviews, events, etc.).

(c) Identified vulnerabilities and implemented OPSEC measures and/or countermeasures.

(d) Lessons learned (as required).

(e) Forecast of OPSEC activities during next reporting period.

(f) Updated roster of all I MEF MSC/E assigned OPSEC Program Managers/Coordinators down to the battalion/squadron level.

b. Logistics. As part of the semiannual and annual reports, identify any resource or funding requirements affecting the OPSEC program to the I MEF OPSEC Program Manager/Coordinator.

6. Command and Signal

a. Command. This Order is applicable to all I MEF activities, commands, units, and personnel, to include personnel from other services, DoD civilian employees, and contract employees who are subject to military law, and any unit that is established under this command in the foreseeable future.

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



D. H. BERGER

Distribution: I/II

OPSEC TERMS AND DEFINITIONS

operations security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities.

aspect. An operational feature, detail, or conclusion that can be logically derived by adversary collection and analysis of friendly information or activity.

capability. An aspect of friendly activity that may be derived from an observable.

intent. What the force must do, and the conditions the force must establish to accomplish the mission.

location. Where: the projected physical or virtual position where a force will act to achieve a desired effect.

method. How forces intend to accomplish an objective: the operational approach.

presence. Current physical or virtual placement within the operational environment.

readiness. A cumulative aspect of friendly activity that refers to the adversary's assessment of our preparedness for a given military action.

strength. An aspect of friendly activity which refers to the level or percentage of capability accessible to the force as measured by what is required to achieve an operational objective or task with acceptable risk.

timing. An aspect of friendly operations that, when correctly interpreted by the adversary in conjunction with previous aspects, allows the adversary to potentially prepare for and interdict friendly action.

critical information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

CIL. A list of critical information that has been fully coordinated within an organization and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

essential secrecy. The condition achieved from the denial of critical information to adversaries through the combined efforts of traditional security programs and the operations security process.

essential secrets. Specific aspects of planned friendly operations that, if compromised, would lead to adversary knowledge of exploitable conditions and a potential failure to meet the commander's objectives and/or endstate.

observable. What is visible to adversary, Foreign Intelligence Entities, or neutral (i.e. media) observers and/or collectors that might be analyzed and used by the adversary military decision maker to form conclusions about friendly operations and activity.

OPSEC assessment. An evaluative process, usually exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence.

OPSEC coordinator. An individual trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC program manager or primary representative.

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

OPSEC countermeasure. Planned actions to affect adversary collection, analysis, delivery, or interpretation of information by the adversary decision maker.

OPSEC measure. Planned actions to conceal friendly critical information from disclosure, observation, or recognition.

OPSEC plan. A plan that provides the organization a living document that can be used to implement the appropriate countermeasures given the mission, assessed risk, and resources available to the unit. OPSEC plans generally take two forms; both should be updated as circumstances and personnel change over time. An OPSEC operations plan provides specific countermeasures to be applied in a specific operation. It may be generated as an annex to a Joint Operation Planning and Execution System plan or as a local document endorsed by the commander. An OPSEC program plan provides guidelines for implementation of routine procedures and measures to be employed during daily operations or activities of a given unit. The plan should be endorsed by the unit commander.

OPSEC planner. A functional expert trained and qualified to plan and execute OPSEC.

OPSEC process. A process that examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by adversaries. It is an analytical, risk-based process that incorporates five distinct elements.

- Critical information identification
- Threat analysis
- Vulnerability analysis
- Risk assessment
- OPSEC countermeasures

OPSEC program manager. A full-time appointee or primary representative assigned to develop and manage an OPSEC program.

OPSEC survey. An application of the OPSEC process by a team of subject matter experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries.

APR 1 2016

OPSEC working groups. Teams of personnel with representatives from the different elements of the command's organization designed to assist the command with OPSEC matters and its program.

signature. The characteristic of an indicator that makes it identifiable or causes it to stand out.

physical signature. Unique properties that can be collected or analyzed using the human senses (including sensors that replicate or augment the human eye.) Collection normally involves line of sight.

technical signature. Unique electromagnetic, infrared, thermal, or other emanations not readily discernable by human senses. Adversary attribution of technical signature to a friendly activity or capability normally involves association.

administrative signature. Documents or other observable coordination normally attributed to a friendly activity or capability employment.

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:

An intent to do harm must exist.

A capability to do harm must exist.

threat analysis. A process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

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.

vulnerability analysis. A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.

EXAMPLE OPSEC PLAN

(CLASSIFICATION)

Command Name

Command Address

Tab C (Operations Security) to appendix 3 (Information Operations) to annex C (Operations)

References:

- (a) MCO 3070.2A
- (b) Other references as needed

1. Situation. Refer to other annexes and paragraphs in the basic plan as much as possible to avoid duplication. When publishing the OPSEC annex separately from the basic order, however, it is necessary to copy the information here in detail. That allows the OPSEC annex to be a useful, standalone document.

a. Enemy Forces

(1) Current Enemy Intelligence Assessment. State the estimated enemy's assessment of friendly operations, capabilities, and intentions. Specifically address any known enemy knowledge of the friendly operation covered in the basic plan.

(2) Enemy Intelligence Capabilities. State the enemy's intelligence collection capabilities according to major categories (SIGINT, HUMINT, and so forth). Address all potential sources to include the capabilities of any non-belligerents, who may provide support to the enemy. Describe how the enemy's intelligence system works to include the time required for intelligence to reach key decision makers. Identify major analytical organizations and key personalities. Discuss unofficial intelligence organizations, if any, that support the leadership. Identify strengths and weaknesses.

b. Friendly Forces

(1) Friendly Operations. Briefly describe the major actions of friendly forces during execution of the basic plan.

(2) Critical Information. List the identified critical information. Include the critical information of higher headquarters. In phased operations, list it by phase: information that is critical in an early phase may not require protection in later phases.

c. Assumptions. Identify any assumptions unique to OPSEC planning.

2. Mission. Provide a clear and concise statement of the OPSEC mission.

3. Execution

a. Concept of Operations. Describe the general concept to implement OPSEC measures. Give it by phase and major activity (maneuver, logistics, communications, and so forth), if appropriate. Address OPSEC support to other elements of the Information Operations Plan, if applicable.

b. Tasks. Identify specific OPSEC measures which will be implemented. List by phase, if appropriate. Assign responsibility for execution to the command issuing the order or to subordinate commands. Add an exhibit to this tab for detailed or lengthy lists.

c. Coordinating Instructions. Identify requirements to coordinate OPSEC measures between subordinate elements. Address required coordination with public affairs. Provide guidance on how to terminate OPSEC related activities of this operation. Address declassification and public release of OPSEC related information. Describe OPSEC assessments or surveys conducted in support of this plan. Identify any After Action Reporting Requirements.

4. Administration and Logistics. Give special OPSEC related administrative or logistical support requirements.

5. Command and Signal

a. Command. Describe feedback mechanisms which will monitor the effectiveness of OPSEC measures during execution. Identify specific intelligence requirements.

b. Signal. Cover special or unusual OPSEC related communications requirements.

APR 1 2016

TRAINING REQUIREMENTS

1. All Marines, civilians, and contractors, who have authorized access to Marine Corps resources by virtue of employment or contractual relationship, will complete annual OPSEC training as outlined under paragraph 5.

2. All OPSEC program managers and 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](mailto:opsec@navy.mil). It can also be completed through the Interagency OPSEC Support Staff (IOSS) at <http://www.ioss.gov/> listed under "Training." It is highly recommended to also attend the resident OPSEC Analysis Course, OPSE-2380. Registration is through IOSS listed under "Training".

3. Command OPSEC program managers and coordinators at the Regimental/Group level and higher and supporting agencies/activities:

a. Attend the IOSS OPSEC Analysis Course, OPSE-2380; and OPSEC Program Management Course, OPSE-2390, or equivalent course, within 90 days of appointment.

b. Registration for the OPSE-2380 OPSE-2390 courses can be completed at <http://www.ioss.gov/> or via email at [ioos@radium.ncsc.mil](mailto:ioos@radium.ncsc.mil). There will be a six month grace period to complete the IOSS OPSE-2380 OPSE-2390 courses, following the publication date of this Order.

4. Per reference (b), all command OPSEC managers and coordinators, Public Affairs Officers, family readiness officers, webmasters, and any other personnel authorized to review information for public release via the internet, shall complete OPSEC and Public Release Decisions, OPSE-1500; and OPSEC and Internet Based Capabilities Course, OPSE-3500. Training shall be completed within 90 days of appointment.

5. Annual OPSEC training requirements for command personnel are:

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

b. An overview of the OPSEC process.

c. OPSEC and social media.

d. The command's current CIL.

(1) To ensure command members do not inadvertently disclose critical information, an unclassified version of the CIL will be provided during annual training. The unclassified CIL may contain actual critical information and/or examples of notional types of critical information. Enclosure (4) provides examples of critical information which commanders can use for tailoring their training material.

(2) If the CIL is classified, it will be provided during annual training, but only to personnel with the appropriate security clearance and access.

(3) A portion of the annual training requirements can be completed through MarineNet at [www.marinenet.usmc.mil](http://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.

(4) A listing of the command's personnel fulfilling OPSEC responsibilities will be maintained with the S- 3 and made available upon request.

6. All OPSEC program managers and coordinators will be compliant with the training requirements no later than six months from the publication date of this Order.

Examples of Critical Information

1. This enclosure provides examples of questions which could be used to generate a command's critical information. The below lists are not "cookie cutter" lists which can be applied to all situations, nor are they an all-encompassing checklist which can be applied to all situations. Commanders and their staffs will use their judgment and experience and develop critical information unique to their mission.

2. Political and Military Crisis Management

- a. Target selection and deployment destinations.
- b. Timing considerations.
- c. Logistical capabilities and limitations.
- d. Alert posture, Defense Condition, and response time.

3. Mobilization

- a. Intent to mobilize before public announcement.
- b. Impact on military industrial base.
- c. Impact on civilian economy.
- d. Transportation capabilities and limitations.

4. Military intervention

- a. Intentions.
- b. Military capabilities.
- c. Strategy and tactics.
- d. Forces assigned and in reserve.
- e. Targets.
- f. Time considerations.
- g. Routes for combat units, support units, and resupply.
- h. Logistic capabilities and constraints.
- i. Third-nation or host-nation arrangements.

5. Open Hostilities

- a. Force composition, disposition.
- b. Attrition and reinforcement.
- c. Targets.

- d. Time considerations.
  - e. Logistic capabilities and constraint.
6. Intelligence, Reconnaissance, and Surveillance
- a. Purpose of collection efforts.
  - b. Targets of collection.
  - c. Time considerations.
  - d. Types of and capabilities of collection assets.
  - e. Processing capabilities.
  - f. Units requesting intelligence data.
7. Peacetime Weapons and other Military Movements
- a. Fact of movement.
  - b. Origin and destination of units, personnel, and equipment being moved.
  - c. Capabilities of units, personnel, and equipment being moved.
  - d. Inventory of equipment being moved.
8. Command Post and Field Training Exercises
- a. Participating units.
  - b. OPLAN or other contingencies that are being exercised.
  - c. Command relationships.
  - d. Command, control, communications, and computer connections and weaknesses.
  - e. Logistics capabilities and weaknesses.
9. Counterterrorism Operations
- a. Forces.
  - b. Contingency plans.
  - c. Standing SOP.
  - d. Targets.
  - e. Time considerations.
  - f. Staging or basing locations.
  - g. Tactics.

- h. Ingress and egress methods.
- i. Logistic capabilities and constraints.

APR 1 2016

Unclassified Website OPSEC

1. Unclassified, publicly available websites present a potential risk to personnel, assets, and operations if inappropriate information is published. OPSEC managers and coordinators 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 (military or civilian) in any way, except when cleared for release and published by authorized Public Affairs personnel. 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, individuals' 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.

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.

Example 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 operation or activity being assessed uses OPSEC measures to protect its critical information. 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 least identified its critical information. Without a basis of critical information, there can be no specific determination that actual OPSEC vulnerabilities exist.

2. Requirement. At a minimum, each command will conduct an annual command assessment using the IG's Checklist criteria. Any command may request a formal assessment.

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

a. The majority of I MEF 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.

(2) Select the Assessment Team Members. Select members from the various staff functions (e.g. intel, comm, logistics, admin, ops) and other entities as needed (e.g. public affairs) 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.

(4) Determine the Enemy's Intelligence Collection Capabilities. Intelligence and counterintelligence staffs will normally provide this information (found in annex B of the OPLAN).

(5) Conduct Empirical Studies (if possible). An example would be to review results of preparations (workups) to the major operation; such as, computer simulations, war games, sand table exercises, field exercises, and command post exercises. This may already be available from information used to complete step 3 of the OPSEC Process. These reviews can help the team identify vulnerabilities that cannot be determined through observation of the operation and interviews of personnel.

(6) Develop a Functional Outline. Functional outlines for each functional area to be surveyed will be completed.

(a) Start by developing a timetable of events to occur. Comparing the event chronology with the known or projected enemy intelligence collection capabilities can often identify vulnerabilities not previously identified. All of the functional chronologies can later be correlated to build the big picture of the operation.

(b) Next, use the chronology to build a functional outline. An example is provided on the next page. The functional outlines project a time-phased picture of events associated with the planning, preparation, execution, and conclusion of the operation. The outline provides an analytical basis for identifying events and activities that are vulnerable to enemy exploitation.

(7) Determine the Vulnerabilities. A review of the OPSEC Plan in the OPLAN, the projected enemy intelligence threat, the chronology of events, and any empirical studies will identify the potential OPSEC indicators. Friendly vulnerabilities can now be confirmed or identified.

(8) Determine Procedures to Conduct the Assessment. Develop any SOP needed, to include coordinating for free access to units and personnel. Determine if any training is required, or if members need familiarization

with a particular functional area (if they do not have expertise in that area).

(9) Announce the Assessment. Announce the assessment far enough in advance to allow the command to prepare for the assessment, and to support the assessment team. Include in the announcement:

- (a) Assessment purpose and scope.
- (b) List of team members and clearances.
- (c) List of required briefings and orientations.
- (d) Time frame involved.
- (e) Administrative or Logistical support requirements.
- (f) Any other details deemed pertinent.

b. Example of a Functional Outline. The outline below can be applied to all the different functional areas such as intelligence, logistics, communications, operations, and administration and support.

(1) Planned Event Sequence. The OPLAN and command/staff briefs form the basis for this timeline. This can be formulated using a lineal listing, a matrix, or another suitable method as required.

(2) Actual Event Sequence. Observe and record events as they actually occur while surveying activities. Be especially cognizant of the information listed in paragraphs three through five below.

(3) Critical Information. List critical information that the command has identified in their OPLAN.

(4) OPSEC Indicators. List OPSEC indicators of critical information that you expect to see based on review of the OPLAN and command/staff briefs prior to field assessment commencing.

(5) OPSEC Measures. List the OPSEC measures developed in the OPLAN that you can expect to see during the assessment.

(6) Analysis. Determine any OPSEC vulnerabilities through review of the OPLAN, command/staff briefs, and actual activities/operations observed. You are looking for OPSEC indicators that can reveal critical information. This condition creates a vulnerability that can be exploited by the enemy. Are the identified OPSEC measures effective in protecting the critical information by preventing the enemy from collecting and accurately interpreting the OPSEC indicators?

c. OPSEC Field Assessment Phase. This phase involves observing operations/activities, reviewing documents, and interviewing personnel. See Enclosure (7) for format examples. The following actions are required:

(1) Conduct a Command Brief. This action is a two-step brief. The commander and staff brief the operation to the assessment team. The assessment team should take this opportunity to clarify questions developed in the planning phase; then the assessment team briefs the command on the

assessment objectives and procedures. Include in the brief a summary of the hostile collection capabilities threat and the vulnerability assessment. The command should be asked to comment on this to validate the assessment. This brief to the command can be a formal presentation or informal discussion.

(2) Refine the Functional Outlines. Using information from the command brief, make changes to the functional outlines as needed. During the actual assessment, changes to the outline may also be needed as data is collected.

(3) Collect the Data. Collect data using personnel interviews, document collection and review, and observations of activities in each functional area. Observe activities and operations using the function.

## I MEF Critical Information List (CIL)

By order of the Commanding General, this CIL will be posted in plain view of every workstation.

Critical information encompasses those specific facts about friendly intentions, capabilities, and activities an adversary needs to plan and act effectively to guarantee failure or unacceptable consequences to the friendly mission. Elements of this information are both classified and unclassified. This list provides categories of information that need protection, regardless of classification. Specific facts related to critical information will not be transmitted via unencrypted telecommunications (phone, fax, internet, email, radio), posted to internet blogs or social media, or discussed in public areas where personnel without a need to know may be present. **Your phone calls and NIPR email are subject to monitoring by the Joint Communication Security Monitoring Activity (JCSMA). This list is NOT a classification guide.**

1. Mission changes indicating strategy or intentions.
2. Intelligence sources, collection, and analytical methods.
3. I MEF support to contingencies and operations.
4. Scope of specific operations; movement of forces, forces capabilities/limitations, tactics/techniques/procedures (TTPs).
5. Mission associated times, such as deployment/redeployment dates, flight times, and travel times.
6. Specific TAD details of key personnel (general officers, command deck personnel, etc.).
7. Specific TAD deployment data indicating an unusually large number of personnel, duration, location, etc.
8. Intelligence, surveillance, and reconnaissance asset support. Collection techniques, capabilities/limitations, associated mission call signs or code words.
9. Detailed diagrams of camps/bases, photos showing sensitive areas and/or geospatial data.
10. Specific peripheral operational related to VIPs/DVs, i.e. itineraries/time tables, meetings, conferences, working groups, driver/aides and personal security detail schedules.
11. Communications involved with or in support of an operation. Capabilities/limitations, frequencies, call signs, information network vulnerabilities, computer passwords, special equipment.
12. Administrative support to an operation. Recall rosters, travel plans, planning rosters, joint manning documents, shortfalls, unit organizational charts, and personal data.
13. Personally identifiable information including social security numbers, telephone numbers, addresses, dates of birth, security clearances, and data related to family members.
14. Logistical support to an operation or special activity. Deployment of special equipment, status of weapons, equipment, spare parts, convoy routes/times, supply and POL delivery.
15. New TTPs being considered exercised or evaluated.
16. Dignitary or high value targets movements/itineraries.
17. Battle damage assessments. Casualties-WIA and KIA, casualty assistance forms, PII details of catastrophic incidents, aviation mishaps, IDF attacks, IED attack.
18. Any items under investigation or that involves external influences.

**Broad categories of information have been compiled to the Critical Information List. Not every subject, procedure, or item that is critical or sensitive has been listed. Refer to the list and utilize sound common sense and good judgment.**

**SHRED ALL PAPER REGARDLESS OF IMPORTANCE**