



UNITED STATES MARINE CORPS

MARINE CORPS INSTALLATIONS EAST
PSC BOX 20005
CAMP LEJEUNE, NORTH CAROLINA 28542-0005

IN REPLY REFER TO:
MCIEASTO 3070.1

G-3
29 NOV 2007

MARINE CORPS INSTALLATIONS EAST ORDER 3070.1

From: Commanding General
To: Distribution List

Subj: OPERATIONS SECURITY (OPSEC)

Ref: (a) DOD Directive 5205.2, DOD Operations Security Program
(b) Joint Pub 3-13.3, Joint Doctrine for Operations Security
(c) MCO 3070.2, The Marine Corps Operations Security (OPSEC) Program
(d) MARFORCOMO 3070.1, Operations Security

Encl: (1) OPSEC Terms and Definitions
(2) The OPSEC Process
(3) The OPSEC Assessment
(4) Sample Format for Final OPSEC Assessment Report
(5) Examples of Critical Information

Report Required: Annual USMC Operations Security Report (Report Control Symbol DD-3070-01, par. 3c(1)(d))

1. Situation

a. Today's security environment has evolved from one in which the threat from identifiable adversarial nation-states has been joined by the less identifiable trans-national terrorist. Regardless of status, these adversaries have the will and the ability to do harm to U.S. interests 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 information can be used to compromise on-going military operations.

b. While the protection of classified information remains a priority, the protection of unclassified open source material

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

must be considered. Methods of collecting critical pieces of information may include Signals Intelligence, Human Intelligence, and Open Source Intelligence, 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. Using the plethora of easily obtained, unprotected information, our objectives can be ascertained and an appropriate response developed to deny us those objectives. Now, more than ever, each Marine, Sailor, and civilian Marine must be cognizant of the importance of protecting unclassified, but potentially useful, information from those who would do harm to this nation and its military forces.

2. Mission. Marine Corps Installations East (MCIEAST) will implement an OPSEC program in order to protect critical information from exploitation by any adversary seeking to impede or deny the success of our military operations.

3. Execution

a. Commander's Intent and Concept of Operations

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

(a) Implementation of OPSEC programs and policies for this headquarters.

(b) Implementation of OPSEC programs and policies throughout all installations under my span of control.

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

(d) To be successful, this will require commanders and supervisors at all levels, both military and civilian, to continually reinforce the importance of good OPSEC practices with their subordinates. All personnel must adhere to the OPSEC

policies designed and implemented to protect our information from exploitation. 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 (d), as well as this Order, provide specific guidance for OPSEC plans and program development and establishment. MCIEAST installations will achieve the Commanding General's intent by developing and implementing OPSEC programs based on the references listed. Each command will ensure their units have OPSEC Coordinators appointed, develop OPSEC Programs tailored to their commands, and utilize the OPSEC Planning Process. Commanders will also share their OPSEC concerns with Public Affairs and family members to reduce inadvertent disclosures. An annual OPSEC Assessment will ensure that the MCIEAST program receives regular command attention and is continually evaluated in order to remain relevant to command needs. By implementing this guidance, MCIEAST installations will decrease their vulnerabilities while negatively impacting adversary abilities to collect critical information against our command.

b. Tasks

(1) AC/S, G-3, MCIEAST

(a) Designated as lead Director on OPSEC matters for MCIEAST.

(b) Develop and maintain an OPSEC order and OPSEC program for MCIEAST.

(c) Host OPSEC working group to:

1. Coordinate OPSEC matters among the staff and departments.

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

(d) Appoint in writing an officer, staff noncommissioned officer, or Department of Defense equivalent civilian as OPSEC Program Manager 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 surveys.
5. Conduct annual OPSEC review.
6. Develop and maintain an OPSEC lessons learned database.
7. Chair OPSEC working group.
8. Coordinate and execute command assessments of MCIEAST OPSEC program.
9. Coordinate with other working groups (i.e. Anti-Terrorism/Force Protection (ATFP) working group, Critical Infrastructure Protection (CIP) working group, Information Assurance (IA) working group, etc.) on OPSEC related matters.
10. Provide assistance to MCIEAST Installations OPSEC Program Coordinators as required.

(2) Command Inspector General, MCIEAST. Incorporate OPSEC as a functional area to be inspected during Commanding General's Inspection Program (CGIP) utilizing the checklist found in reference (c).

(3) Assistant Chiefs of Staff and Directors of Special Staff Sections, MCIEAST

- (a) Appoint in writing OPSEC Program Coordinators to:
1. Provide OPSEC subject matter expertise and recommendations.
 2. Coordinate OPSEC matters with the MCIEAST OPSEC Program Manager.
 3. Coordinate OPSEC education and training for members of your staff.

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

5. Act as member of OPSEC Assessment Team when required.

(b) Provide representation to the OPSEC working group as required by the OPSEC Program Manager. This individual may serve as your OPSEC Program Coordinator as well.

(4) MCIEAST Installation Commanders

(a) Develop and maintain an OPSEC order.

(b) Develop and implement an OPSEC program.

(c) Designate subordinate units or activities that require an OPSEC program.

(d) Assign responsibility for your command's OPSEC program development, implementation, and oversight.

(e) Appoint in writing an officer, staff noncommissioned officer, or equivalent Department of Defense Government Service (GS) employee as OPSEC Program Coordinator whose duties, at a minimum, will include:

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

2. Developing, coordinating, and maintaining the Command OPSEC Program to include writing policy/guidance documents.

3. Coordinating OPSEC education and training.

4. Coordinating command OPSEC surveys.

5. Conducting annual OPSEC review.

6. Developing and maintaining an OPSEC lessons learned database.

(f) Develop OPSEC education and awareness program.

1. Ensure all personnel are provided OPSEC education and awareness training annually.

2. Develop a program for ensuring newly joined personnel are provided OPSEC education.

3. Ensure education and awareness program stresses the importance and role of family in OPSEC.

(g) Conduct assessment annually of OPSEC program effectiveness utilizing the Automated Inspection Reporting System Inspection checklist as well as references (a) through (d).

1. Submit a copy of annual assessment findings to the MCIEAST OPSEC Program Manager.

2. Coordinate with the MCIEAST OPSEC Officer for inspectors, assistance, and support as needed.

c. Coordinating Instructions

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

(a) MCIEAST Program Manager and Installation OPSEC Program Coordinators will attend a resident course within 90 days of appointment.

Available courses are:

1. Navy OPSEC Course; <http://www.nioc-norfolk.navy.mil/>
2. DoD 2400 Course; <http://www.dss.mil/>
3. OPSE 2380-2390 Course; <http://www.iooss.gov/>
4. Army OPSEC Planner's Course; <https://www.1stiocmd.army.mil/>

(b) OPSEC Program Manager and Coordinators will 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 at the Navy Information Operations Command website; <https://www.niocnorfolk.navy.mil/operations/opsec/main.shtml>. 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:

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

1. An overview of the OPSEC process.
2. Defining OPSEC and its relationship to the command's security programs.
3. Reviewing the command's current critical information list.
4. Reviewing the list of the command's personnel fulfilling OPSEC responsibilities for situational awareness.

(d) Annual Reporting Requirement. Commanders will submit an annual report, based on fiscal-year time period, detailing their OPSEC program. Guidance on the format and submission date for this report will be released via separate correspondence.

(2) Enclosure (1) is provided as a list of common OPSEC definitions.

(3) Enclosure (2) is provided as an explanation and outline of the OPSEC Process.

(4) Enclosure (3) is provided as a sample format of a Final OPSEC Assessment Report.

(5) Enclosure (4) is provided as examples of Critical Information.

4. Administration and Logistics

a. Administration

(1) Provide contact information of OPSEC Program Coordinators to the MCIEAST OPSEC Program Manager. The MCIEAST OPSEC Program Manager will be immediately notified of any changes to contact information.

(2) Provide copy of all OPSEC assessments to MCIEAST OPSEC Program Manager (See enclosure (3) for assessment outline).

(3) Submit OPSEC Survey Information to the MCIEAST OPSEC Program Manager when requested.

b. Logistics

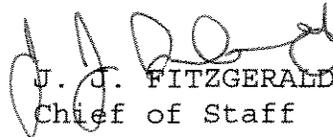
(1) Capture all costs associated with the OPSEC Program for future budgetary adjustments.

(2) When requested, submit cost data to MCIEAST OPSEC Program Manager.

5. Command and Signal

a. Command. This Order is applicable to Marine Corps Installations East.

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


J. J. FITZGERALD
Chief of Staff

DISTRIBUTION: A

Copy to: COMMARFORCOM G-3-5-7

29 NOV 2007

OPSEC Terms and Definitions

1. This enclosure contains common use terms and definitions associated with OPSEC and are provided for a clearer understanding of OPSEC as well as assisting with the OPSEC Program creation process.

a. Critical Information. These are specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

b. Excessive OPSEC. Excessive OPSEC can degrade operational effectiveness by interfering with activities such as coordination, training, and logistical support. Military operations are inherently risky, and the commander 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.

c. Essential Elements of Friendly Information (EEFI). EEFI is a term used extensively throughout the Marine Corps and is defined as "Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness."

d. OPSEC Assessments. An OPSEC assessment is 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 after critical information has been identified. Without understanding critical information which should be protected, there can be no specific determination that OPSEC vulnerabilities exist.

30 NOV 2007

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

f. OPSEC Process. OPSEC planning is accomplished through the OPSEC Process. This has five steps which are usually applied in a sequential order. In dynamic situations, the steps may be revisited at any time to adjust to new threats or information. Enclosure (2) provides a detailed explanation of the OPSEC Process.

g. OPSEC Program Managers and Coordinators. Program Managers are personnel who have OPSEC duties as their primary job. Coordinators are personnel who perform OPSEC functions as an additional duty. Commanders will use their discretion in determining whether they require OPSEC Program Managers or Coordinators to fulfill their responsibilities.

h. OPSEC Working Groups. These are 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.

i. Threat. A threat is any individual or organization that seeks to do harm by interrupting ongoing military operations or activities. In order to be classified a threat two conditions must be satisfied:

- (1) An intent to do harm must exist.
- (2) A capability to do harm must exist.

If both conditions cannot be met than a threat does not exist.

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

k. Indicator. These are friendly detectable actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information.

2. Many of these terms are further subdivided into categories. Their definitions can be found in references (a) through (d).

The OPSEC Process

1. General

a. OPSEC is an operations function vice security, intelligence, or counter-intelligence function.

b. OPSEC is a process by which we identify critical information, analyzing friendly actions concerning military operations and activities, our vulnerabilities and how the threat can exploit them to gain information, and the measures that we can implement to reduce our vulnerabilities thereby protecting our critical information

c. OPSEC is a command responsibility.

2. OPSEC Process. The OPSEC process is a five step process. Those responsible for OPSEC program creation/implementation shall apply this five-step process that entails:

a. Step 1: Identification of Critical Information. The commander and staff tries to identify the questions that they believe the enemy will need to know about friendly intentions, capabilities (and limitations), and activities. These questions are the EEFI. Critical information is only part of the EEFI, it is the information vitally needed by the enemy. This serves to focus the OPSEC Process on protecting the vital information, rather than attempting to protect all information. The EEFI is found in the OPLAN in Tab C to Appendix 3 to Annex C (Operations). This critical information will often times be similar to what you would want to know about the enemy.

b. Step 2: Analysis of Threats. This involves the research and analysis of intelligence information, counterintelligence, reports, and open source information to identify who the likely enemy will be. The friendly commander will ask questions, such as:

(1) Who is the enemy or adversary that has intent and capability to take action against us?

(2) What are the enemy's intentions and goals?

(3) What is the enemy's strategy for opposing the planned operation or activity?

- (4) What type of tactics and forces will the enemy employ?
- (5) What critical information does the enemy already know?
- (6) What critical information is it too late to protect?
- (7) What are the enemy's intelligence collection capabilities?
- (8) How does the enemy process and disseminate their collected data?

c. Step 3: Analysis of Vulnerabilities. This action identifies an operation's or activity's vulnerabilities. This requires examining the parts of the planned operation and identifying OPSEC indicators that could reveal critical information. Vulnerabilities exist when the enemy is capable (with the available collection and processing assets) of observing an OPSEC indicator, correctly analyzing it, and then taking appropriate and timely action. The commander will need answers to questions such as these:

- (1) What OPSEC indicators of critical information not known to the enemy will be created by friendly actions that result from the planned operation or activity?
- (2) What OPSEC indicators can the enemy actually collect?
- (3) What OPSEC indicators can the enemy actually use to our disadvantage?

d. Step 4: Assessment of Risk. This step essentially has two components. First, planners analyze the identified vulnerabilities and then identify possible OPSEC measures against them. Second, specific OPSEC measures are selected for execution based on the risk assessment done by the commander and staff.

- (1) OPSEC Measures can be used to:
 - (a) Prevent the enemy from detecting an OPSEC indicator.
 - (b) Provide an alternate analysis of an indicator from the enemy viewpoint (deception).

(c) Directly attack the enemy's collection system(s).

(2) Besides physical destruction, OPSEC measures can include:

(a) Concealment and camouflage.

(b) Deception (across all aspects of operations and Information Operations).

(c) Intentional deviations from normal patterns; and conversely, providing a sense of normality.

(d) Practicing sound information security, physical security, and personnel security.

(3) More than one OPSEC measure may be identified for each vulnerability and one OPSEC measure can be identified for multiple vulnerabilities. Primary and secondary OPSEC measures can be identified for single or multiple OPSEC indicators. OPSEC measures are most effective when they provide the maximum protection while minimally effecting operational effectiveness.

(4) Risk assessment involves comparing the estimated cost (time, effort, resource allocation, and money) of implementing an OPSEC measure to the potential effects on mission accomplishment resulting from an enemy exploiting a particular vulnerability. Questions to ask include:

(a) What is the risk to mission effectiveness if an OPSEC measure is taken?

(b) What is the risk to mission effectiveness if an OPSEC measure is not taken?

(c) What is the risk to mission effectiveness if an OPSEC measure fails to be effective?

(d) Will the cost of implementing an OPSEC measure be too much as compared to the enemy's exploitation of the vulnerability?

(e) Will implementing a particular OPSEC measure create an OPSEC indicator? Will it create an OPSEC indicator that you want the enemy to see (e.g., deception)?

(f) Do we even have the capability to implement the OPSEC measure? If we do, can the assets under our control accomplish this, or do we need to request assets from outside sources?

(5) Planning for OPSEC measures requires coordination amongst all staff elements, and supporting elements or assets outside the command. Particular care must be taken to ensure that OPSEC measures do not interfere with other operations (e.g., deception plans, psychological operations). Solid staff functioning and planning will ensure OPSEC plans integrate with and support other programs and operations.

e. Step 5: Application of OPSEC Measures. In this step, the commander implements the OPSEC measures selected in the previous step (Risk Assessment). Planning and integrating OPSEC measures into the OPLAN is critical to ensure counter measures are applied at the right time, place, and manner.

(1) The enemy reaction to our OPSEC measures will be monitored to determine effectiveness. Provisions and methods for feedback from combat units, intelligence and counterintelligence staffs, and other Information Operations elements, will have to be planned for in the OPLAN. This feedback will help determine the following:

(a) Is the OPSEC measure producing the desired effect? Or is it producing an undesired effect?

(b) Is the OPSEC measure producing an unforeseen effect? If so, does this result in positive or negative effects for friendly forces?

(c) Do we need to continue executing the OPSEC measure? Will it still be effective, or has it accomplished its task and been overcome by the tempo of operations?

(d) Do we need to cease the OPSEC measure because of no observable results, negative, or unintended consequences?

(e) Do we need to modify the OPSEC measure based on the result?

(f) Do we need to implement previously selected (secondary) OPSEC measures to replace ineffective OPSEC measures based on the results?

(g) Do we need to devise new OPSEC measures to replace ineffective OPSEC measures?

(h) Have we identified new requirements, or unforeseen OPSEC indicators that will need new OPSEC measures? Again, this is dynamic process, and previous steps may have to be revisited.

(2) In addition to ongoing operations, feedback provides information for OPSEC planning for future operations through lessons learned.

(3) The OPSEC Assessment is an excellent method and tool for providing feedback on the effectiveness of OPSEC measures.

The OPSEC Assessment

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 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

a. At a minimum, 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 internal assessment.

3. Two Types of Assessments

a. Command Assessment. Concentrates on events within the command and is normally performed by using only personnel assigned to the command being reviewed. The majority of assessments will be this type. 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 period, while evaluating website OPSEC on the next period.

b. Formal Assessment. Is composed 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 assessment are normally directed by higher headquarters to subordinate echelons, but may be

2 9 NOV 2007

requested by subordinate commands. These formal assessments are typically large scale endeavors requiring large amounts of personnel (25+) and lead times in excess of four months.

4. Each OPSEC Assessment is unique. This is due to the differing activities of varied 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.

5. OPSEC Assessments are different from Security Inspections. 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.

6. Assessments are not a Punitive Tool. They should be conducted on a non-attribution basis. This will ensure better cooperation and honesty when surveying activities, plans, and operations.

7. Results of Assessments. These should be given to the commander of the unit surveyed. Results will also be forwarded to higher headquarters on a non-attribution basis to derive lessons learned that may be applied to other units within MCIEAST.

8. OPSEC Assessment Planning Phase. The OPSEC Assessment is composed of the following phases:

a. 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.

b. Select the Assessment Team Members. Select members from the various staff functions and other entities as needed (e.g. public affairs) to ensure an adequate breadth of expertise. OPSEC is an operations function, so the team leader should be from Operations.

29 NOV 2007

c. 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.

d. Determine the Threat's Intelligence Collection Capabilities. Intelligence and counterintelligence elements can provide this information.

e. Conduct Empirical Studies (if possible). An example would be to review results of preparations (workups) for a major operation or activity such as support operations for tenant operating forces, 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.

f. Develop a Functional Outline. Functional outlines for each functional area to be surveyed will be completed.

(1) Start by developing a timetable of events to occur. Comparing the event chronology with the known or projected threat 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.

(2) 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.

g. Determine the Vulnerabilities. Review of the OPSEC Plan, 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.

h. Determine Procedures to Conduct the Assessment. Develop any SOP required including 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).

i. 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:

- (1) Assessment purpose and scope.
- (2) List of team members and clearances.
- (3) List of required briefing and orientations.
- (4) Timeframe involved.
- (5) Administrative or logistical support requirements.
- (6) Any other details deemed pertinent.

9. 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.

a. Planned Event Sequence. The OPSEC Program or 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.

b. Actual Event Sequence. Observe and record events as they actually occur while surveying activities. Be especially cognizant of the information listed in paragraphs 10c(3) through 10c(5) of this enclosure.

c. Critical Information. List critical information that the command has identified in their OPSEC Program or OPLAN.

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

e. OPSEC Measures. List the OPSEC measures developed in the OPSEC Program or OPLAN that you can expect to see during the assessment.

f. Analysis. Determine any OPSEC vulnerabilities through review of OPSEC Program, 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?

10. OPSEC Field Assessment Phase. This phase involves observing operations and activities, reviewing documents, and interviewing personnel. The following actions are required:

a. Conduct a Command Brief. This action is a two-step brief. The commander and staff brief the OPSEC Program or OPLAN 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 threat collection capabilities 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.

b. 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.

c. Collect the Data

(1) Collect data using personnel interviews, document collection and review, and observations of activities in each functional area. Observe activities and operations using the functional outline as your guide.

(2) Assessment members should assure the interviewees that the information they provide will be protected by a non-attribution policy. Interviews should cover the purpose of the interview; description and duties of the interviewee; details of the tasks performed as to exactly how, what, where, and when they perform them with a view toward determining what

information they receive, handle, or generate, and what they do with it; whether the individual's actions reflect an awareness of the hostile collection capabilities; and whether the interviewee's actions produce OPSEC indicators.

(3) Incorporate the collected data into the functional outline. As the data is entered, this changes the outline from a projection of events to a record of actual events. The outline then is a chronological record of what actually was done or happened, who did it, where it happened, and how and why it was done. The recordings should include an assessment of the identified vulnerabilities in light of the enemy collection threat, and any OPSEC indicators generated by the activities or operations.

(4) If a finding is considered to have serious negative mission impact, the commander should be notified to allow for early corrective action.

(5) Conduct a daily post brief among the assessment team. This is a chance to compare and correlate data, assess the functional outlines and refine as needed, and redirect team efforts or members as needed.

11. Analysis and Reporting Phase

a. During this phase, the assessment team correlates and assesses the data collected in the field assessment phase.

b. Identify Vulnerabilities. Correlate and assess the data to identify vulnerabilities, those that were previously developed, and those that were identified during the field assessment. OPSEC indicators that were observed are identified as potential vulnerabilities. Again, vulnerabilities are conditions that the threat may be able to exploit to reveal critical information. The key characteristics of vulnerabilities are observable OPSEC indicators, and the threat's ability to collect or observe the indicators. The ability of the threat to effectively exploit the vulnerability in a timely manner indicates the actual risk to friendly forces.

c. OPSEC Assessment Report. The report is generated, addressed, and delivered to the commander of the operation/activity surveyed. A suggested format is included in enclosure (4). Format for findings can be presented in

chronological order, order of significance, or grouped into the different functional areas. The report should discuss:

- (1) Observed OPSEC indicators.
- (2) Ability of the enemy to collect and process the indicators.
- (3) Vulnerabilities identified.
- (4) Analysis of the vulnerability's risk to the command's operations.
- (5) Recommended OPSEC measures or modification to existing OPSEC measures.
- (6) Answer the question: Is the critical information being protected?
- (7) Care must be taken to ensure the appropriate level of classification is given to discussions of vulnerabilities, and recommended OPSEC measures.

Sample Format for Final OPSEC Assessment Report

1. Overview

a. Background. Address the purpose and scope of the OPSEC assessment.

b. Conduct of Assessment. Brief discussion of team composition, procedures used, units or commands visited, timeframes involved, and any problems encountered.

c. Critical Information. List the critical information identified in the OPSEC Program or OPLAN.

d. Threat. List the enemy intelligence collection capabilities.

2. Findings, Analysis, Conclusions/Recommendations. This is the main body of this report. Discussions may be listed chronologically, by command, chronologically by commands, by the different functional areas, or a combination of all the above. Compress the recorded facts observed into the significant points. List the positive and negative points. The intent is to reinforce OPSEC that is working, and changing that which is not working or filling an existing void. The following is the suggested format for this section of the final report:

a. Observation. List the observed OPSEC indicators that could reveal identified information. This will include previously identified indicators (from the OPSEC Program or OPLAN and briefs); and indicators not previously identified but observed during the assessment.

b. Analysis. Discuss the vulnerabilities observed. The key here is whether or not the enemy has the intelligence collection capability to observe and process the OPSEC indicators. If the command or other types of units (not involved in the operation) can reasonably expect to face future threats that will have the collection capability, include this in the discussion. This information can be important to future operations and can be disseminated appropriately. The main points of your analysis will be whether or not the indicator revealed critical information. If so, then the OPSEC measure is not working. Did the OPSEC indicator even have an OPSEC measure

applied to protect the critical information? If the OPSEC indicator revealed or can be inferred to have revealed critical information, then this condition is a vulnerability.

c. Conclusions/Recommendations. Recommend OPSEC measures to counter the OPSEC indicators, to protect the critical information. If the OPSEC Assessment team does not have the expertise and knowledge to recommend an OPSEC measure, then be honest and state this. The command can then plan, develop, and apply appropriate OPSEC measures for future or current operations. The command needs to determine if OPSEC lessons learned can be applied to other commands and disseminate the information appropriately. Care must be taken to appropriately classify and handle the final OPSEC Assessment Report in accordance with the appropriate security directives.

Examples of Critical Information

1. This enclosure provides examples of information that could be used to generate a command's Critical Information List. Each item has examples of EEFI listed below. This list is not 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. 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
- g. Vehicle Registration Data
- h. Ranks/names of officer and SNCOs on assigned base quarters

3. Unit Information

- a. Appointment Letters
- b. Access Rosters
- c. Work Schedules
- d. Personnel Strengths and Shortfalls
- e. Watch Schedules and Reaction Times
- f. Training Data of units using MCBCL Facilities

4. 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 headquarters 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

5. 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

6. Plans, Policies, and Procedures

- a. AT Plan
- b. Integrated Action Sets

29 NOV 2007

- 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)
 - i. DWX SOP
7. 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
8. 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 Fire Emergency Services Division incident reports, traffic accident reports, etc.
 - e. PMO blotters, desk journals, stats sheets, etc.
 - f. Safety Mishap Reports and associated records

29 NOV 2007

g. Completed or ongoing internal and criminal investigations

9. Special Event Information

- a. Distinguished Visitor Information
- b. Schedules of Events
- c. Locations of Events
- d. Special events LOIs

10. 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