



UNITED STATES MARINE CORPS
MARINE CORPS BASE
PSC BOX 20004
CAMP LEJEUNE NC 28542-0004

BO 3070.1

S-3

AUG 10 2010

BASE ORDER 3070.1

From: Commanding Officer
To: Distribution List

Subj: OPERATIONS SECURITY (OPSEC)

Ref: (a) MCO 3070.2, The Marine Corps Operations
Security Program (DRAFT)
(b) MARFORCOMO 3070.1, Operations Security
(c) MCIEASTO 3070.1, Operations Security

Encl: (1) OPSEC Terms and Definitions
(2) The OPSEC Process
(3) The OPSEC Assessment
(4) Critical Information List (FOUO)
(5) Inspector General's Checklist

Report(s) Required: Annual USMC Operations Security Report
(Enclosure 8)

1. Situation

a. Today's security environment finds Marine Corps Base, Camp Lejeune (MCB CamLej) at the forefront of supporting the Global War on Terror as well as numerous other engagements world-wide. No longer are the lines of battle neatly delineated on a map with clearly defined forward and rear areas. Instead, we find ourselves combating adversaries that are asymmetrical in time, space, capability, and ambition. The threat is not only represented by hostile nations and transnational terrorist organizations, but also foreign allies and U.S. citizens all seeking access to information. Through a variety of available means, whether sophisticated methods such as signals intelligence and imagery intelligence or unsophisticated methods such as open source intelligence and human intelligence, our adversaries seek to gain a positional advantage relative to the U.S. and/or hinder the success of ongoing and future military operations by exploiting the information they gather.

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

b. While the protection of classified information remains important, we must also focus on protecting unclassified open source materials. These materials allow an adversary the ability to build a reasonably coherent intelligence picture of our current and future operations, as well as the luxury of preparing a response to be executed at the time and place of their choosing. Now, more than ever, each Marine, Sailor, Coast Guardsman 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. MCB CamLej implements an Operations Security (OPSEC) program to protect the critical information sought by adversaries that would be used to disrupt our military operations.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To execute an OPSEC program designed to deny potential adversaries access they would need to develop countermeasures and actions used to disrupt ongoing and future military operations. These actions would include the creation and implementation of a formal OPSEC program, the creation and implementation of the policies and procedures necessary to support our OPSEC program, the continued education of users at all levels to raise awareness and increase control over open source information, and the continued refinement of the OPSEC program over time to meet emerging threats. 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. End state: denial of access to critical information by potential adversaries through the elimination or mitigation of existing vulnerabilities.

(2) Concept of Operations. References (a) through (c), and this Order, provide specific guidance for OPSEC plans, policy and program development. MCB CamLej will achieve the Commander's Intent by developing and implementing an OPSEC program based on the references listed.

AUG 10 2010

b. Tasks(1) Director, S-3, MCB CamLej

(a) Designated as lead agency on OPSEC matters for MCB CamLej.

(b) Maintain an OPSEC order and OPSEC program for MCB CamLej.

(c) Host OPSEC Working Group (WG) to:

1. Coordinate OPSEC matters among the staff and departments.

2. Implement the MCB CamLej OPSEC program.

(d) Appoint in writing an officer, staff noncommissioned officer, or Department of Defense (DoD) equivalent civilian as OPSEC Program Manager to perform the following duties:

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

2. Coordinate and maintain the Command OPSEC Program to include writing changes to policy/guidance documents as necessary.

3. Coordinate OPSEC education and training.

4. Coordinate command OPSEC surveys.

5. Conduct annual command OPSEC assessments.

6. Maintain an updated/current OPSEC lessons learned database.

7. Chair OPSEC WG.

8. Coordinate and execute command assessments of the MCB CamLej OPSEC program.

9. Coordinate with other relevant working groups on OPSEC related matters (e.g., Antiterrorism (AT) WG, Physical Security WG, Critical Infrastructure WG, Threat Fusion WG, and Chemical, Biological, Nuclear and High-Yield Explosives (CBRNE) WG).

AUG 1 0 2010

10. Provide assistance to MCB CamLej staff sections and subordinate element OPSEC Coordinators as required.

11. Coordinate with Marine Corps Installations East (MCIEAST) OPSEC Program Manager for support of MCB CamLej OPSEC Program.

(2) Command Inspector General, MCB CamLej. Incorporate OPSEC as a functional area to be inspected during Commanding Officer's Readiness Inspections (CORI).

(3) Directors and Special Staff Sections, MCB CamLej

(a) Appoint in writing OPSEC Program Coordinators to:

1. Provide OPSEC subject matter expertise and recommendations.

2. Coordinate OPSEC matters with the MCB CamLej OPSEC Program Manager.

3. Coordinate OPSEC education and training for members of your staff.

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

5. Act as a member of the OPSEC Assessment Team.

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

(4) Commanding Officers, Headquarters and Support Battalion, and Weapons Training Battalion, MCB CamLej

(a) Appoint in writing an OPSEC Program Coordinator to:

1. Provide OPSEC subject matter expertise and recommendations.

2. Coordinate OPSEC matters with the MCIEAST OPSEC Manager.

3. Coordinate OPSEC education and training for members of your command.

AUG 1 2010

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

5. Act as a member of the OPSEC Assessment Team.

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

c. Coordinating Instructions

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

(a) MCB CamLej OPSEC Program Manager will attend a resident course within ninety days of appointment. Available courses are:

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

(b) MCB CamLej 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.nioc-norfolk.navy.mil/opsec>. 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. Review of the command's current Critical Information List.

4. Review of the command's personnel fulfilling OPSEC responsibilities.

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

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

(4) Enclosure (3) is provided as an example of The OPSEC Assessment.

(5) Enclosure (4) is MCB CamLej Critical Information list.

(6) Enclosure (5) is the Inspector General's Checklist.

4. Administration and Logistics

a. Administration

(1) Commanding officers, directors, and special staff provide contact information of OPSEC Coordinators to the MCB CamLej OPSEC Program Manager. The MCB CamLej OPSEC Program Manager will be immediately notified of any changes to contact information.

(2) Provide a copy of all OPSEC assessments to MCB CamLej OPSEC Program Manager for submission 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 budget adjustments.

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

BO 3070.1
AUG 10 2010

5. Command and Signal

a. Command. This Order is applicable to all military and civilian personnel assigned to MCB CamLej.

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


D. J. LECCE

DISTRIBUTION: A

OPSEC Terms and Definitions

1. This enclosure contains common use terms and definitions associated with OPSEC, and is provided to present a clear 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. 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.

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.

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 then 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.

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

AUG 10 2010

The OPSEC Process1. General

a. OPSEC is an operations function vice security, intelligence, or counterintelligence 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 try to identify the questions they believe the enemy will need to know about friendly intentions, capabilities (and limitations), and activities. These questions are the Essential Elements of Friendly Information (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. EEFI's are found in Operation Plans (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?

(2) Who has intent and capability to take action against us?

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

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

Enclosure (2)

AUG 1 2 0010

(5) What type of tactics and forces will the enemy employ?

(6) What critical information does the enemy already know?

(7) What critical information is it already too late to protect?

(8) Are there OPSEC measures that can be taken later in the process to protect critical information or deceive the enemy on compromised critical information?

(9) What are the enemy's intelligence collection capabilities?

(10) 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.

Enclosure (2)

(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 (IO).

(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?

Enclosure (2)

AUG 10 2019

(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, etc.). 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 countermeasures 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 IO 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?

Enclosure (2)

AUG 1 0 2010

(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 a 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.

Enclosure (2)

AUG 10 2010

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 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

a. At a minimum, each commander, director, and special staff will conduct an annual Command Assessment using the Inspector General's Checklist. (See enclosure (5) for checklist)

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 assessments are normally directed by higher headquarters to subordinate echelons, but may be 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.

AUG 10 2010

4. Each OPSEC Assessment is Unique. This is due to the differing activities of varied units and departments. 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 (e.g., only conducting identification checks at the gate during VIP visits).

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 or director of the staff section 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 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 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.

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.

Enclosure (3)

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 activities 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 assessed 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 outline projects 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 Standing Operating Procedures (SOP) needed, including coordinating for free access to units/departments 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

Enclosure (3)

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, 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 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 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

Enclosure (3)

AUG 10 2010

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/director and staff brief the OPSEC Program 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

Enclosure (3)

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/director 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/director 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.

Enclosure (3)

AUG 10 2010

(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.

Enclosure (3)

Critical Information List

1. This enclosure provides the Critical Information List for MCB Camp Lejeune. Each item has examples of Essential Elements of Friendly Information (EEFI) listed below. This list is not an all-encompassing checklist which can be applied to all situations. Commanders and their staffs may use their judgment and experience to develop critical information unique to their mission.

2. Personnel Information

- a. Privacy Act information
- b. Joint Personnel Adjudication System data
- c. Standard Labor Data Collection and Distribution Application (SLDCADA) data
- d. Defense Travel System data
- e. Training records
- f. Timecards
- g. Vehicle registration data
- h. Ranks/names of officers and staff non commissioned officers on assigned base

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 MCB CamLej facilities

AUG 10 2010

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 Marine Expeditionary Force Headquarters vice HP1
- c. Building schematics which are available open source
- d. Specific commanding general/commanding officer office location within headquarters buildings
- e. Mission Essential Vulnerable Area 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 (hazardous materials, arms, ammunition, explosives), map and text

5. Equipment/Specialized Equipment Information

- a. Security camera location/capability
- b. Intrusion detection systems location/capability
- c. Chemical, biological, radiological, nuclear, high-explosive sensor location/capability
- d. Equipment capabilities

6. Plans, Policies, and Procedures

- a. AT Plan
- b. Integrated Action Sets

Enclosure (4)

AUG 10 2010

- c. Special Orders
- d. Security plans
- e. CBRNE response capabilities, guidelines and procedures
- f. Force protection condition security augmentation requirements
- g. DoD School Critical Incident Plans
- h. Installation and unit Random AT Measures
- i. Destructive Weather Exercise SOP

7. IT Systems/Communications Systems Information

- a. System Authorization Access Request Database
- b. System Security Accreditation Agreement data with associated Internet Protocol addresses Information Assurance Vulnerability program data
- d. Interim Approval to Operate/Connect data
- e. Protected Distribution System approvals
- f. Common Access Card Personal Identification Number reset information

8. Reports, Surveys, Administrative Information, Related Documentation

- a. Security Assessments
- b. Provost Marshal's Office (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 Service Division incident reports, traffic accident reports, etc.
- e. PMO blotters, desk journals, stats sheets, etc.

Enclosure (4)

- f. Safety Mishap reports and associated records
- 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 Letter of Instruction

10. Logistics Information

- a. Freight shipment data associated with particular Exercises or Operations
- b. Billing/Accounting data
- c. Traffic Management Office Personal Property Files
- d. Transportation Operational Personal Property System (TOPPS) data
- e. Law enforcement sensitive information, i.e., TALON, FBI Alerts, etc.
- f. PMO, Brig, and Fire & Emergency Service Division incident reports, traffic accident reports, etc.
- g. PMO blotters, desk journals, stats sheets, etc.
- h. Safety Mishap reports and associated records
- i. Completed or ongoing internal and criminal investigations

Enclosure (4)

AUG 10 2010

Inspector General's Checklist

- 481 01 001 Has the command appointed in writing an OPSEC Program Manager or Coordinator to serve as the POC for all OPSEC matters?
Reference: MCO 3070.2, paragraph 4b(9)(a)
- 481 01 002 Does the command have an OPSEC Order?
Reference: MCO 3070.2, paragraph 4b(9)(b)1
- 481 01 003 Does the command have a Critical Information List?
Reference: MCO 3070.2, paragraph 4b(9)(b)3
- 481 01 004 Does the command ensure contract requirements properly reflect OPSEC responsibilities, when applicable?
Reference: MCO 3070.2, paragraph 4b(9)(b)5
- 481 01 005 Is the command's Critical Information List provided to the Public Affairs Officer?
Reference: MCO 3070.2, paragraph 4b(9)(b)7
- 481 01 006 Does the command develop OPSEC plans in support of operations and exercises?
Reference: MCO 3070.2, paragraph 4b(9)(b)8
- 481 01 007 Did the command conduct an annual command level assessment?
Reference: MCO 3070.2, paragraph 4b(9)(b)9
- 481 01 008 Has the OPSEC Program Manager or Coordinator Completed the OPSEC Fundamentals Course within 30 days of being appointed? If the online course is not accessible, has the command requested that a copy of the course be mailed to the command?
Reference: MCO 3070.2, paragraph 4c(5)(a)
- 481 01 009 If required, has the OPSEC Program Manager or Coordinator attended or requested to attend a resident course within 90 days of appointment?
Reference: MCO 3070.2, paragraph 4c(5)(b)

- 481 01 010 Does the command conduct annual training with the following minimum requirements: A definition of OPSEC and its relationship to the command's security and intelligence programs; an overview of the OPSEC Process; The command's current critical information list; and a listing of the command's personnel fulfilling OPSEC responsibilities?
Reference: MCO 3070.2, paragraph 4c(5)(c)
- 481 01 011 Does the command's unclassified publicly available website(s) have critical information posted?
Reference: MCO 3070.2, paragraph 4c(6)(a)
- 481 01 012 Does the command's unclassified publicly available website(s) have classified information, "For Official use Only" information, proprietary information, or information that could enable the recipient to infer this type of information?
Reference: MCO 3070.2, paragraph 4c(6)(b)
- 481 01 013 Does the command's unclassified publicly available website(s) identify family members of Department of the Navy personnel in any way, except for spouses of senior leaders who are participating in public events?
Reference: MCO 3070.2, paragraph 4c(6)(c)
- 481 01 014 Does the command's unclassified publicly available website(s) include online biographies which include family member information?
Reference: MCO 3070.2, paragraph 4c(6)(c)
- 481 01 015 Does the command's unclassified publicly available website(s) display personnel lists, "roster boards" organizational charts, or command staff directories which show individual's names, individual's phone numbers, or email addresses which contain the individual's names?
Reference: MCO 3070.2, paragraph 4c(6)(d)
- 481 01 016 Does the commander emphasize the importance of OPSEC with family members?
Reference: MCO 3070.2, paragraph 4c(8)

Enclosure (5)