UNITED STATES MARINE CORPS
2D MARINE AIRCRAFT WING
II MARINE EXPEDITIONARY FORCE
POSTAL SERVICE CENTER BOX 8050
CHERRY POINT, NC 28533-0050

WgO 3070.1D
G-3
MAR 13 2012

WING ORDER 3070.1D

From: Commanding General, 2d Marine Aircraft Wing
To: Distribution List

Subj: 2D MARINE AIRCRAFT WING (2D MAW) OPERATIONS SECURITY (OPSEC) PROGRAM

Ref: (a) DoD Directive 5205.02-M
(b) Joint Publication 3-13.3
(c) MCO 3070.2
(d) ALMAR 007/04
(e) Automated Inspection Reporting System (AIRS) Checklist, Functional Area 481
(f) MCWP 3-40.4
(g) SECNAVINST 5720.47B

Encl: (1) The OPSEC Process
(2) Examples of Critical Information
(3) Examples of OPSEC Indicators
(4) Examples of OPSEC Measures
(5) Notional OPSEC Plan
(6) OPSEC Assessments
(7) Functional Outline and Profile Guideline for Intelligence, Logistics, Communications, Operations, Administration and Support

1. Situation

a. Reference (a) directs the Marine Corps to implement certain measures in support of operational security programs. This Order provides policy, responsibilities and procedures for 2d MAW in order to fulfill these requirements. Reference (b) is an excellent source for information on planning and executing OPSEC programs.

b. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

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

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

(2) Determine what OPSEC indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

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

(4) Identify the OPSEC process by using enclosure (1) of reference (c). Additional information on critical information is contained in enclosure (2) of reference (c). Additional information on OPSEC indicators is contained in enclosure (3) of reference (c) and examples of OPSEC measures are contained in enclosure (4) of reference (c).

2. Cancellation. WgO 3070.1C.

3. Mission. Upon issuance of this Order, 2d MAW develops an aggressive OPSEC program in order to prevent an adversary or potential adversary from obtaining critical information that facilitates the prediction of friendly intentions, capabilities or activities.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. 2d MAW units will utilize OPSEC, which includes organizational support, regular OPSEC training, regular OPSEC assessments and also the development and incorporation of critical information lists and the OPSEC planning process into operations, exercises and garrison environments. As directed in reference (d), OPSEC must become a way of life for all Marines. The final result of these efforts will be ensuring that these programs are developed, utilized and relevant to all personnel assigned to 2d MAW.

(2) Concept of Operations. 2d MAW will achieve the Commandant of the Marine Corps (CMC) intent by developing new OPSEC standards and then promulgating them throughout 2d MAW. This Order announces the new standards for program requirements, training and assessment procedures. By implementing the guidance contained within this Order, Commanders will ensure their units have OPSEC Officers appointed, develop OPSEC

programs tailored to their commands and utilize the OPSEC planning process. Commanders will also share their OPSEC concerns with Public Affairs Officers (PAOs) and family members to reduce inadvertent disclosures. A thorough system of OPSEC assessments will ensure that these programs receive regular command attention and are continually evaluated so that they remain relevant to command needs. Finally, the Marine Corps Lessons Learned System will be utilized in order to provide a repository for OPSEC lessons for use by all Marines. By implementing this guidance, 2d MAW units will decrease their vulnerabilities while negatively impacting adversary abilities to collect critical information against our forces.

b. Subordinate Element Missions

(1) Assistant Chief of Staff (AC/S), G-3, 2d MAW:

(a) Serve as the lead office on OPSEC matters for 2d MAW. Appoint a full-time OPSEC Program Manager to serve as the point of contact for all OPSEC matters.

(b) Develop and maintain the 2d MAW OPSEC Order.

(c) Supervise the prioritization for OPSEC assessments which will be conducted by the 2d MAW operations security support element or other commands.

(d) Develop an OPSEC program meeting the requirements listed in paragraph 4b (9) of reference (c).

(e) Conduct an annual review of subordinate commands' OPSEC programs. This will be based on a fiscal year time period. The review will be the basis for a report which will be submitted to the Information Operations (IO) and Space Integration Branch (Headquarters, U. S. Marine Corps (HQMC)/Plans, Policy and Operations (PP&O)/Position Location Information (PLI).

(2) AC/S, G-2, 2d MAW: develop and disseminate policies regarding intelligence support, to include counterintelligence, to OPSEC.

(3) AC/S, G-6, 2d MAW

(a) Develop and maintain the Marine Corps Information Assurance Program and coordinate its requirements with the 2d MAW OPSEC Order.

(b) As required, coordinate command, control, communications and computer support to OPSEC assessments.

(c) Assist in ensuring that appropriate safeguards are in effect for information posted to websites and direct the removal of information from websites that violate OPSEC standards unless adequate safeguards are employed.

(4) Wing Inspector: ensure that the OPSEC functional area is reviewed by inspection teams operating as part of the Commanding General's (CGs) Inspection Program.

(5) All Commanding Officers (COs) will

(a) Appoint in writing an Officer, Staff Noncommissioned Officer (SNCOs) or equivalent Department of Defense (DoD) civilian as the OPSEC Manager or Coordinator, as appropriate.

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

1. An OPSEC order.

2. OPSEC training as outlined in paragraph 4c (5) of reference (c).

3. Development of a critical information list.

4. Emphasizing the importance of OPSEC with family members.

5. Ensuring contract requirements properly reflect OPSEC responsibilities and are included in contracts, when applicable.

6. Ensuring that websites are reviewed to ensure they meet the OPSEC concerns listed in paragraph 4c (6) of reference (c).

7. Sharing the critical information list with the PAO. OPSEC Officers will ensure that PAOs receive current copies of their command's critical information list in order to prevent inadvertent disclosure of this information via public affairs programs.

8. Developing OPSEC plans in support of operations and exercises. Enclosure (5) of reference (c) contains an example of a notional OPSEC plan.

9. Command Assessments. Each command will conduct assessments and record the findings as directed in reference (c). At a minimum, every command will conduct an annual command level OPSEC assessment, utilizing reference (e).

c. Coordinating Instructions

(1) The operations staff (G-3/S-3) is responsible for assisting commanders in planning and executing the command's OPSEC program. As outlined in reference (f), commands which have an IO cell will normally have the IO Officer responsible for the command's OPSEC Program. Regardless of the staff officer assigned OPSEC duties, the OPSEC program must be closely coordinated with members of the commander's staff, attached and supporting elements and any joint and/or coalition forces.

(2) OPSEC is not a security or an intelligence function. Security functions prevent unauthorized access to personnel, equipment, facilities, materials and documents. Intelligence activities provide information on adversary forces, governments and intentions. Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of, foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist activities. OPSEC and these activities often overlap and are mutually supportive. The intelligence staff (G-2/S-2) is responsible for assisting commanders in planning, coordinating and executing counterintelligence support during the drafting and reviewing of OPSEC plans. Commands without an organic counterintelligence capability will coordinate with the Counterintelligence/Human Intelligence Officer at the next appropriate level of command for support. Close coordination must be maintained between all staff functions to ensure adequate OPSEC protection.

(3) 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.

(4) OPSEC Working Groups. These are personnel teams with representatives from the different elements of the command's organization. Forming an OPSEC working group to assist in the command's OPSEC program is extremely effective and highly encouraged, but not directed. Commanders will use their discretion in determining the need for these groups.

(5) Training Requirements

(a) All OPSEC Program Managers and Coordinators will complete an OPSEC Fundamentals Course within 30 days of appointment. The course is available online. It is listed as "CBT 1301" and is available at the Navy Information Operations Command website: http://www.nioc-norfolk.navy.mil. 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.

(b) OPSEC Program Managers and Coordinators assigned to major subordinate commands will attend a resident course within 90 days of appointment.

(c) Available courses are:

1. Navy OPSEC Course; http://www.nioc-norfolk.navy.mil/.

2. DoD OPSEC Officers Course; http://www.dss.mil/.

3. OPSEC 2380, 2390 or 2400 Course; http://www.ioss.gov/.

(d) Annual OPSEC training for all command personnel. Minimum training requirements are:

1. Must complete MarineNet Cyber Awareness Training Course Code "CYBER0000" which encompasses the required OPSEC Course, "Careless Keystrokes can Kill" IAW MARADMIN 118/11.

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

3. An overview of the OPSEC process.

4. The command's current critical information list. This will ensure command members do not inadvertently disclose critical information. If the list is classified, then this requirement is waived for personnel without the appropriate security clearance and access. However, commanders will then provide unclassified examples of notional types of critical information in order to educate their command members on the general types of information they should not divulge. Enclosure (2) of reference (c) provides examples of unclassified, general types of information which commanders can use for tailoring their training material.

5. A listing of the command's personnel fulfilling OPSEC responsibilities.

(6) Unclassified Website OPSEC. Unclassified, publicly available websites present a potential risk to personnel, assets and operations if inappropriate information is published. OPSEC Officers will review their command's website to ensure no critical information is published via information, graphics or photographs. In addition, as directed in reference (g), the following guidance is provided:

(a) 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, 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.

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

(c) 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 email 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.

(d) Biographies of general officers, commanders, COs, Officers In Charge (OICs), 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.

(7) Public Affairs. Public affairs are important in garnering public support, fostering community relations and helping with the success of military operations. Public knowledge of military operations is inevitable because of advanced technology and instant media coverage. Therefore, public affairs staffs must be included in the OPSEC planning process where media attention is expected or desired. The need for OPSEC should not be used as an excuse to deny non-critical information to the public.

(8) Family. Commanders will discuss OPSEC concerns as part of their Unit Family Readiness Program and stress the family's ability to contribute to protection of the command's critical information.

(9) Inspections

(a) OPSEC is a functional area on the Inspector General's Checklist and will be evaluated as part of each unit's Command Inspection Program and the CGs Inspection Program. Inspection teams will review the OPSEC functional area of all commands visited by Inspector General Teams.

(b) Commands will normally utilize their own personnel to conduct an annual, command level OPSEC assessment. Because formal assessments require support from organizations

such as the Joint Information Operations Warfare Command (JIOWC) or the Navy Information Operations Command, commands which desire a formal assessment will forward a request to HQMC/PP&O/PLI. HQMC/PP&O/PLI will prioritize these requests and interface with organizations external to the Marine Corps.

(10) Annual Reporting Requirement. Commanders will submit an annual report, based on a fiscal year time period, detailing their OPSEC program. These consolidated reports will incorporate subordinate unit reports per reference (a). Guidance on the format and submission date for this report will be released via separate correspondence.

(11) 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.

5. Administration and Logistics

a. Marine Corps Operations Security Support Element. Reference (a) directs each service to provide for an OPSEC support element. For the Marine Corps, this function is being provided by the Navy Information Operations Command's OPSEC support element. Commands seeking additional assistance with OPSEC tactics, techniques and procedures, training support, advice for command level OPSEC assessments or OPSEC aids such as posters should contact this command via the command's website, http://www.nioc-norfolk.navy.mil/ or their organizational mailbox, opsec@navy.mil.

b. Definitions

(1) 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. The OPSEC Process steps are:

(a) Identification of critical information.

(b) Analysis of threats.

(c) Analysis of vulnerabilities.

(d) Assessment of risk.

(e) Application of OPSEC measures.

(2) OPSEC 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. Enclosure (3) of reference (c) lists examples of OPSEC indicators.

(3) OPSEC 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.

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

(5) 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 the critical information which should be protected, there can be no specific determination that OPSEC vulnerabilities exist.

(6) Critical Information and its relationship to Essential Elements of Friendly Information (EEFI)

(a) Critical information is a term used throughout the OPSEC community and refers to "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) 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."

(c) These two terms are very similar and the difference in the terms is in their specificity. EEFIs are more general in nature and thought of in terms of a question, while

critical information is more specific and thought of as the answer to the question. For example, a tactical situation would have "Time for Unit X to cross the Line of Departure" as an EEFI, while "0400L" would be the specific fact (answering the EEFI) and therefore would represent critical information.

6. Command and Signal

a. Command. This Order applies to all 2d MAW activities, commands, units and personnel (to include personnel from other services and civilian employees serving with Marine Corps units).

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

R. W. REGAN
Chief of Staff

DISTRIBUTION: A

THE OPSEC PROCESS

1. The OPSEC Process involves five steps applied in a sequential order. In dynamic situations, the steps may be revisited at any time to adjust to new threats or information.

2. 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 can be thought of as the answer to 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 Operation Plan (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.

3. 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:

a. Who is the enemy or adversary? Who has intent and capability to take action against us?

b. What are the enemy's intentions and goals?

c. What is the enemy's strategy for opposing the planned operation? What type of tactics and forces will the enemy employ?

d. What critical information does the enemy already know about the operation or friendly forces? What critical information is it too late to protect? Are there OPSEC measures that can be taken later in the process to protect critical information or deceive the enemy on compromised critical information?

e. What are the enemy's intelligence collection capabilities? How does the enemy process and disseminate their collected data? Friendly intelligence and counterintelligence staffs can provide this information.

4. 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. Reviewing results of preparations (workups) to the operation such as computer simulations, war games, sand table exercises, field exercises and command post exercises will help identify vulnerabilities not readily apparent. The commander will need answers to questions such as these:

a. 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?

b. What OPSEC indicators can the enemy actually collect?

c. What OPSEC indicators can the enemy actually use to our disadvantage?

5. 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.

a. OPSEC Measures can be used to:

(1) Prevent the enemy from detecting an OPSEC indicator.

(2) Provide an alternate analysis of an indicator from the enemy viewpoint (deception).

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

b. Besides physical destruction, OPSEC measures can include:

(1) Concealment and camouflage.

(2) Deception (across all aspects of operations).

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

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

c. 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.

d. 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:

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

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

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

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

(5) 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)?

(6) 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?

e. 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.

6. 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.

a. 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:

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

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

(3) 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?

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

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

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

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

(8) 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.

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

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

EXAMPLES OF CRITICAL INFORMATION

1. This enclosure provides examples of questions which could be used to generate a command's critical information. The below categories would be the EEFI and the specific answers to the EEFI would constitute the 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 robotically 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. Noncombatant Evacuation Operations

a. Targets.

b. Forces involved.

c. Logistic capabilities and constraints.

d. Safe havens or staging areas.

e. Routes.

f. Time considerations.

10. Counterdrug Operations

a. Military forces involved.

b. Law Enforcement Agencies (LEAs) involved.

c. Military support to LEAs.

d. Host-Nation cooperation or involvement.

e. Capabilities of military forces/LEAs.

f. Time considerations.

g. Tactics to be used.

h. Logistic capabilities and constraints.

11. Counterterrorism Operations

a. Forces.

b. Contingency plans.

c. Standing Standard Operating Procedure (SOP).

d. Targets.

e. Time considerations.

f. Staging or basing locations.

g. Tactics.

h. Ingress and egress methods.

i. Logistic capabilities and constraints.

EXAMPLES OF OPSEC INDICATORS

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

2. There are five basic characteristics to an OPSEC indicator that make them potentially useful for deriving critical information.

a. Signature. A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out. An indicator's uniqueness reduces the ambiguity of the indicator and minimizes the number of other indicators that must be observed to confirm a single indicator's significance or meaning. For example, a thermal-imaging satellite detects an infrared heat exhaust emission at an expeditionary field. Analysis of the emissions indicates it is a ground equipment unit used for medium or large fixed-wing transport aircraft. The enemy analysts had previously identified different emissions from Ground Support Equipment (GSE) and identified them as belonging to a particular aircraft or types of aircraft. The analyst only needs to look into their database to compare this recent indicator to identify what type or class of aircraft the GSE is being used for.

(1) An indicator's signature stability implies constant or stereotyped behavior that allows an enemy to anticipate future actions. Reducing the uniqueness or stability of the indicator's signature increases the ambiguity of the enemy's observations.

(2) Procedural features are important to a signature and they serve to identify how, when and where the indicator occurs and what part it plays in the overall scheme of operations.

b. Associations. Association is the relationship of an indicator to other information or activities. Intelligence analysts compare their current observations with what has been seen in the past to identify possible relationships.

(1) Using the previous example, the enemy analyst knows that the GSE is used for fixed-wing transport aircraft. The analyst also knows that the length and composition of the landing strip will only support transport aircraft as large as a C-130. Additionally, United States Marine Forces are the only units that have used this field in the last two years. An

analyst would likely take the GSE indicator and associate it with the previous information and conclude that KC-130s are operating in the area.

(2) Another aspect to associations involves the continuity of actions, objects or other indicators that register as patterns to an analyst. These indicators may not be the result of planned procedures, but may result from repetitive practices or sequencing to accomplish a goal. Using the earlier example, two more GSE units are observed at the same airbase. Past repetitive practices observed indicated that three GSE units signify a detachment of six KC-130s conducting operations in the area.

(3) Another useful association involves organizational patterns. Most military forces have a symmetrical organization. For example, an infantry Headquarters (HQ) Company observed in the area signifies an entire infantry battalion in the area. Thus in many situations, a pattern taken as a whole can be derived from a single indicator.

c. Profiles. Each functional activity generates its own set of unique signatures and associations. The sum of these signatures and associations is the activities profile.

(1) Given sufficient data, an analyst can determine the profile of any activity or unit. Over time, analysts attempt to identify and record the profiles of their adversary's activities or units. For example, an infantry regiment has many unique indicators. Over a period of several years, the enemy analysts have cataloged these indicators and created a standard picture, or profile of the indicators an infantry regiment creates. The enemy observes many indicators, compares them to their database and can identify what type of unit is there.

(2) A profile for a major organization has sub-profiles for functional activities needed to effect the operation. Observation of one or several of these sub-profiles can be associated with the major profile to accurately predict what type of operation will occur. For example, the enemy observes indicators, compares them to their database and then can identify what type of unit is there. If they had identified the profiles for a heavy weapons company and an infantry battalion, they will probably conclude that there is a regimental-size unit conducting operations.

d. Contrasts. Contrasts are differences observed between an activity's standard profile and current or recent activities. The deviation from the established profile is relatively easy to detect and will attract the enemy analysts' attention. The analyst will then focus more intelligence collection efforts to find out what the contrast signifies. For example, the enemy identifies a profile of what appears to be an infantry unit, but observes indicators that do not fit that standard profile. The enemy then focuses its collection efforts and observes more indicators. Comparing these indicators to the profiles database reveals that there are units there that fit the profile for a Marine Expeditionary Unit (MEU)

e. Exposure. Exposure refers to when and for how long an indicator is observed. The duration, repetition and timing of an indicators exposure can affect its relative importance and meaning. Limiting the exposure period reduces the amount of detail that can be observed and the associations that can be formed.

(1) An indicator that appears over a long period of time will be assimilated into an overall profile and assigned meaning. An indicator that appears periodically will be further studied as a contrast to the normal profile. More detail can be gleaned from each exposure, adding to its meaning and relationship to a profile.

(2) An indicator that appears only briefly and then disappears may arouse strong interest or little, depending on the detail observed and value assigned. Limiting an indicator's exposure in time and occurrence will make it hard for the enemy to detect and evaluate the indicator.

(3) For example, using good OPSEC measures during the MEU workup exercises will limit the contrasts observed from the normally observed infantry battalion profile. This can shield the composition of the force and prevent the enemy analysts from knowing that it is a MEU-level operation. This can further confuse the enemy to the purpose of the operation.

3. Examples of Indicators:

a. Indicators of general military capabilities:

(1) The presence of unusual types of units for a given area or base.

(2) Friendly reactions to adversary exercises or actual hostile actions.

(3) Actions, information or material associating reserve units with specific commands or units (e.g., Take Off (T/O) for mobilization).

(4) Actions, information or material indicating the levels of manning, readiness and experience of personnel and/or units.

(5) Actions, information or material revealing spare parts availability for equipment or systems.

(6) Actions, information or material indicating equipment or systems reliability (e.g. visits of technical representatives or special repair team/unit).

(7) Movement of friendly ships, aircraft and/or ground units in response to detection of enemy activities.

(8) Actions, information or material revealing tactics, techniques and procedures employed in different types of training exercises or during equipment/systems operational tests and evaluation.

(9) Stereotyped patterns in performing the organizational mission that reveal the sequence of specific actions or when and how they are accomplished.

b. Indicators of General Command and Control Capabilities

(1) Actions, information or material providing insight into the volume of orders and reports needed to accomplish a specific task or operation.

(2) Actions, information or material showing unit subordination for deployment, mission or a task.

(3) Association of particular commanders with patterns of behavior in various tactical situations.

(4) Information revealing problems of coordination between the commander's staff elements or subordinate units.

(5) In exercises or operations, indications of the period between the occurrence of a need to act or react and the

action taking place; of consultations that occur with higher commands and the types of actions initiated afterward.

(6) Unusual actions with no apparent direction reflected in communications.

c. Indicators from Communications

(1) Personnel using handheld radios or testing aircraft, vehicle or man-packed radios.

(2) Establishing and testing new communication nets. Without conditioning the enemy, the sudden appearance of a new net may cause the enemy to increase intelligence collection efforts.

(3) Increasing, decreasing or ceasing (radio silence) radio transmission when close to starting an operation, exercise or test. Again, without conditioning the enemy, unusual changes will catch the enemy's attention.

(4) Using the same or common call signs for units, certain individuals (e.g., for the commander .6.); code words for activities or conditions (e.g., .Winchester.) or infrequently changing radio frequencies and encryption. This allows for easier enemy monitoring and adds to profiles.

(5) Using stereotyped message characteristics that indicate particular types of activity allowing adversary's to monitor and evaluate friendly activity.

(6) Requiring check-in and check-out with multiple or consistent control stations before, during and after an activity (e.g., air operations).

d. Indicators for Equipment and Systems

(1) Unencrypted emissions during tests and exercises.

(2) Budget data that provide insight into the objectives and scope of system research and development effort or sustainability of a fielded system (this often comes from public media).

(3) The equipment or system hardware itself.

(4) Information on test and exercise schedules that

allow adversaries to better plan the use of intelligence collection efforts.

(5) Deployment of unique units, targets and sensor systems to support tests associated with particular equipment or systems.

(6) Unusual visible security imposed on particular development effort that highlights their significance.

(7) Information indicating special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract or activity.

(8) Notices to Airmen (NOTAMS) and Mariners that might highlight test areas and a particular operation.

(9) Stereotyped use of location, procedures and sequences of actions when preparing for and executing test activities for specific types of equipment or systems.

(10) Use of advertisements that a company has a contract on a system or possesses military technology.

e. Indicators of preparations for operations. Many indicators deal with the preparatory phase, as opposed to the execution phase. Much of this is logistical in nature:

(1) Provisioning of special supplies.

(2) Requisitioning of special or an unusual volume of supplies to be filled by a particular date.

(3) Embarking special units, installing special capabilities and preparing unit equipment with special configurations (e.g., desert paint schemes).

(4) Increased prepositioning of ammunition, fuel, weapons and other types of supply items.

(5) Procuring large numbers or unusual types of maps/charts for a particular area.

(6) Making medical arrangements, mobilizing medical personnel, stockpiling pharmaceuticals (e.g., anthrax vaccine) and blood stocks.

(7) Focusing intelligence and reconnaissance assets on a particular geographical area or type of activity.

(8) Requisitioning or assigning an increased number of linguists of a particular language or related group of languages to an area.

(9) Initiating and maintaining unusual liaison with foreign nationals or governments for political or military support.

(10) Providing increased or specific types of training to personnel.

(11) Holding rehearsals to test aspects of an operation.

(12) Increasing the number of trips and conferences for senior officials and staff members.

(13) NOTAMS making seaport and airspace reservations/restrictions.

(14) Arranging for tugboats and pilots at seaports; requesting supplies or provisions for support at seaports.

(15) Recalling personnel on leave and liberty to their duty locations; canceling leave and liberty.

(16) Imposing unusual off-limits restrictions.

(17) Preparing units for combat operations through equipment checks as well as operational or maintenance stand downs in order to achieve a required readiness level for equipment and personnel.

(18) Making billeting and transportation arrangements for particular units or personnel.

(19) Taking large-scale action to change mailing addresses or arrange for mail forwarding; providing for wills and powers of attorney.

(20) Posting supply delivery, personnel arrival, transportation or ordnance loading schedules in a manner where people without a need to know have access.

(21) Storing boxes, equipment or other supplies in an uncontrolled area with labels or shipping forms indicating the destination or the operation name.

(22) Employing un-cleared personnel to handle material used only in particular types of operations or activities.

(23) Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.

(24) Requesting unusual or increased meteorological, oceanographic or ice information for a specific area/region.

(25) Setting up Wide Area Network (WAN) over commercial lines.

f. Indicators During the Execution Phase

(1) Unit and equipment departures from base.

(2) Enemy radar, sonar or visual detection of friendly units.

(3) Friendly unit identifications through improper communications or physical observation of unit symbols (e.g. placards with unit Identification (ID), squadron ID on aircraft).

(4) Force composition and tracks or routes of advance that can be provided by emissions from units or equipment and systems that provide identifying data.

(5) Stereotyped procedures; static and standard ways of composing, disposing and controlling strike and defensive elements against particular threats and predictable reactions to enemy reactions or operations.

(6) Trash and garbage dumped by units or from ships at sea or picked up by commercial vendors that might provide identifying data or other information.

(7) Alert of civilians in operational areas.

(8) Transportation or requisitioning of spare parts or personnel to deploying or deployed units via military or commercial means.

(9) Changes in oceanographic high frequency transmission.

(10) Changes in activity, volume over the WAN.

g. Indicators of Post-Engagement Operations or Residual Capabilities:

(1) Repair and maintenance facility schedules.

(2) Urgent, increased or unusual requests for maintenance personnel, units, equipment or supplies.

(3) Movement of supporting maintenance resources.

(4) Unusual medical activity.

(5) Unusual re-supply of a unit or activity.

(6) Assignment of new units to an area.

(7) Search and rescue activity.

(8) Personnel orders or reassignment.

(9) Discussion of repair, maintenance or supply issues in unsecure areas or by unsecure means.

(10) Termination or modification of procedures for reporting of unclassified meteorological, oceanographic or ice information.

EXAMPLES OF OPSEC MEASURES

1. The following OPSEC measures are examples only and are provided in order to generate ideas as Marines develop their own OPSEC measures. Development of specific OPSEC measures is as varied as the specific vulnerabilities they are designed to offset.

2. Operational and Logistic Measures

a. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations and activities in terms of time, place, event, sequencing, formations and command and control arrangements.

b. Employ force dispositions and command and control arrangements that conceal the location, identify and command relationships of major or important units.

c. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

d. Transport supplies and personnel to combat units in such a way to conceal the location and identity of combat units.

e. Operate aircraft at a low altitude to avoid detection.

f. Operate and deploy units or weapons systems in a way to minimize the reflective surfaces exposed to radar and sonar.

g. Use darkness to mask deployments or force buildup.

3. Technical Measures

a. Use proper radio procedures and techniques to minimize interception and evaluation of emissions. Use techniques such as burst transmissions, secure phones, couriers, encrypted transmission and frequently changing codes and encryptions. Limit use of high frequency radios and directional super-high frequency transponders.

b. Control radar emissions, operate at reduced power and operate radars common to many units.

c. Mask emissions, forces and equipment from radar or visual detection by use of terrain.

d. Use appropriate military deception. Use camouflage, smoke, background noise or inclement weather to conceal movement of personnel, units and equipment (be aware that this might create a contrast and attract the enemy's attention without conditioning or integration into a deception package).

4. Administrative Measures

a. Avoid bulletin board notices, plan of the day or planning schedule notices that reveal when events will occur (or other specific details).

b. Conceal budgetary transactions, supply request and actions and arrangements for services that reveal preparations or intentions for operations.

c. Conceal the issuance of orders, the movement of special personnel and/or equipment to units and the addition of special capabilities to units.

d. Control trash disposal and other housekeeping functions to conceal the identity and location of units and other details pertaining to the operation.

e. Follow normal leave and liberty policies to the maximum extent possible to present a sense of normalcy.

f. Ensure that personnel discreetly prepare for their family's welfare in their absence.

5. Military Deception in Support of OPSEC use to:

a. Cause enemy intelligence to not target friendly activities, ensuring failure to collect intelligence against our tests, operations and exercises. To prevent the enemy from determining through analysis vital capabilities and characteristics of weapons, systems and vital aspects of policy, doctrine and tactics.

b. Create confusion about or cause multiple interpretations of intentions, operations, tactics to be employed and timetables.

c. Create confusion about or cause multiple interpretations of vital information taken from open sources.

d. Cause enemy observers to lose interest in the test,

operation, exercise or activity or to assign a low priority to intelligence collection efforts.

e. Convey inaccurate locating and targeting information to the enemy.

6. Physical destruction and Electronic Warfare. During hostilities, use physical destruction and electronic attack against the enemy's assets used to collect and process intelligence. Offensive IO actions that can be conducted include: strikes against satellites; communications centers or sites; radars; fixed sonar sites; reconnaissance aircraft, ships or units.

NOTIONAL OPSEC PLAN

(CLASSIFICATION)

Command Name
Command Address

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

References:

a. MCO 3070.2
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 (Signals Intelligence (SIGINT), Human Intelligence (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. Identity 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 HQ. 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 OPLAN, 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.

CLASSIFIED BY:
DECLASSIFY:

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

a. At a minimum, each command will conduct an annual command assessment using the 2d MAW inspection checklist.

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

3. There are two types of assessments Command and Formal

a. 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 USMC assessments will be this type of 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 HQ to subordinate echelons, but may be requested by subordinate commands.

4. 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.

5. 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.

6. 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.

7. Results of assessments should be given to the commander of the unit surveyed. Results may also be forwarded to higher HQ on a non-attribution basis to derive lessons learned that may be applied to other units within 2d MAW and the Marine Corps.

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

a. OPSEC Assessment Planning Phase.

(1) Determine the Scope. Limit the extent of the assessment to manageable proportions based on time, geography, units to be observed, operations or activities to be observed, staffing, funding and other practical considerations. As outlined in reference (b), the following areas could be evaluated: intelligence collection operations; logistics; communications; operations and administration and support. See enclosure (7) for functional outlines and profile guidelines for these areas.

(2) Select the Assessment Team Members. Select members from the various staff functions (e.g. intelligence, communications, logistics, administration, operations) 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 G-3/S-3.

(3) Understand the operation or activity to be assessed. Team members must be thoroughly briefed on the OPLAN 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 briefing and orientations.

(d) Timeframe 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 (annex B).

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

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

(6) Analysis. Determine any OPSEC vulnerabilities through review of the OPLAN (annex B), 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

(a) 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.

(b) Assessment members should assure the interviewees that the information they provide would 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.

(c) Incorporate the collected data into the functional outline. As the data is inputted, 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/operations.

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

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

d. Analysis and Reporting Phase

(1) During this phase, the assessment team correlates and assesses the data collected in the field assessment phase.

(2) 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 enemy may be able to exploit to reveal critical information. The key characteristics of vulnerabilities are observable OPSEC indicators and the enemy's ability to collect or observe the indicators. The ability of the enemy to effectively exploit the vulnerability and in a timely manner indicates the actual risk to friendly forces.

(3) OPSEC assessment report. The report is generated, addressed and delivered to the commander of the operation/activity surveyed. The OPSEC assessment report can be presented in chronological order, order of significance or grouped into the different functional areas. The report should discuss:

(a) Observed OPSEC indicators.

(b) Ability of the enemy to collect and process the indicators.

(c) Vulnerabilities identified.

(d) Analysis of the vulnerability's risk to the command's operations.

(e) Recommend OPSEC measures or modification to existing OPSEC measures.

(f) Answer the question, "Is the critical information being protected?"

(g) Care must be taken to ensure the appropriate level of classification is given to discussions of vulnerabilities and recommended OPSEC measures.

9. Example format for a Final OPSEC Assessment Report:

a. Overview

(1) Background. Address the purpose and scope of the OPSEC assessment.

(2) Conduct of assessment. Brief discussion of team composition, procedures used units or commands visited, timeframes involved and any problems encountered.

(3) Critical information. List the critical information identified in the inspected command's OPLAN.

(4) Threat. List the enemy intelligence collection capabilities.

b. 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 a list of 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:

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

(2) 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 enemies 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.

(3) 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.

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR INTELLIGENCE, LOGISTICS, COMMUNICATIONS, OPERATIONS, ADMINISTRATION AND SUPPORT

1. General. The completed profile reflects a picture of the intelligence collection effort. Intelligence collection is normally one of the first functional areas to present indicators of an impending operation or activity.

2. Planned event sequence. See the intelligence collection plan prepared by intelligence staff element.

3. Actual event sequence. Observe events in the joint intelligence center.

4. Analysis. Determine any OPSEC vulnerabilities. If vulnerabilities exist, determine whether they exist because of an error or because they are the result of normal procedures.

5. Examples of Typical Indicators:

a. Appearance of specialized intelligence collection equipment in a particular area.

b. Increased traffic on intelligence communications nets.

c. Increased manning levels and/or work hours in intelligence facilities.

d. Increased research by known intelligence activities and personnel in libraries and electronic databases.

e. Increased activity of friendly agent nets.

f. Increased levels of activity by airborne intelligence systems.

g. Alterations in the orbits of intelligence satellites.

h. Interviews with nongovernmental subject matter experts conducted by intelligence personnel.

i. Requests for maps and other topographic material.

6. General. The completed logistic profile presents a picture of logistic activities conducted in preparation for an impending operation. As in the administration function, the long lead

time for some preparations gives early warning of forthcoming operations if events are compromised.

7. Planned Event Sequence. See logistic annex to OPLAN.

8. Actual Event Sequence. Observation, interviews.

9. Analysis. As conducted for the intelligence functional areas.

10. Examples of Typical Indicators:

a. Special equipment issue.

b. Pre-positioning of equipment and supplies.

c. Increased weapons and vehicle maintenance.

d. Upgrading lines of communications.

e. Petroleum, oils and lubricants stockpiling.

f. Ammunition stockpiling.

g. Delivery of special munitions and uncommon munitions (discloses possible nature of operation).

h. Arrival of new logistic units and personnel.

i. Increased requisition of supplies.

j. Increased traffic on logistic communications nets.

k. Changes in normal delivery patterns.

11. General. In addition to presenting a picture of its own functional area, friendly communications also reflect all other functional areas. Communications surveillance and communications logs for all functional nets are important tools in evaluating this functional area as well as other functions involved.

12. Planned Event Sequence. OPLAN, OPORD, signal operation instructions or standing signal instruction.

13. Actual Event Sequence. Communications monitoring and communications logs.

14. Analysis. As conducted for the intelligence functional areas.

15. Examples of Typical Indicators:

a. Increased radio, teletype and telephone traffic.

b. Increased communications checks.

c. Appearance of new stations in net.

d. New frequency and call-sign assignments.

e. New codes and authenticators.

f. Radio silence.

g. Changing call up patterns.

h. Use of maintenance frequencies to test equipment.

i. Communications command post exercises.

j. Appearance of different cryptographic equipment and materials.

k. Unclassified network activity.

16. General. The completed profile of operational activities reflects events associated with units as they prepare for an operation.

17. Planned Event Sequence. OPLAN, operation order (OPORD), SOP.

18. Actual Event Sequence. Observations, reports, messages and interviews.

19. Analysis. As conducted for the intelligence functional areas.

20. Examples of Typical Indicators:

a. Rehearsals and drills.

b. Special-tactics refresher training.

c. Appearance of special-purpose units (bridge companies, forward air controllers, pathfinders, mobile weather units).

d. Pre-positioning of artillery and aviation units.

e. Artillery registration in new objective area.

f. Complete cessation of activity in area in which reconnaissance activity previously took place.

g. Appearance of new attached units.

h. Issuance of new equipment.

i. Changes in major unit leadership.

j. Repositioning of maneuver units.

21. General. The completed profile of administrative and support events shows activities taking place before the operation, thereby giving advance warning.

22. Planned Event Sequence. Derive from unit SOPs and administrative orders.

23. Actual Event Schedule. Observations and interviews.

24. Analysis. As conducted for the intelligence functional areas.

25. Examples of Typical Indicators:

a. Release of groups of personnel or complete units for personal affairs.

b. Runs on exchanges for personal articles, cleaning and other items.

c. Changes to wake-up and dining schedules.

d. Changes to mailing addresses.

e. New unit designators on mail.

f. Emergency personnel requisitions and fills for critical skills.

g. Medical supply stockpiling.

h. Emergency recall of personnel on leave and liberty.