UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION NEW RIVER
PSC BOX 21001
JACKSONVILLE, NC 28545-1001

ASO 3070.1D
OPS
SEP 26 2022

AIR STATION ORDER 3070.1D

From: Commanding Officer, Marine Corps Air Station New River
To: Distribution List

Subj: OPERATIONS SECURITY (SHORT TITLE: OPSEC)

Ref: (a) DoDD 5205.02E Ch 2 of 20 June 2012
(b) DoDM 5205.02 Ch 2 of 3 November 2008
(c) JP 3-13.3 of 4 January 2012
(d) SECNAVINST 3070.2A
(e) MCO 3070.2A
(f) NTTP 3-13.3M/MCTP 3-32B of September 2017
(g) MCIEAST-MCB CAMLEJO 3070.1A
(h) ASO 3440.1B
(i) 5 U.S.C. § 7532

Encl: (1) OPSEC Terms and Definitions
(2) The OPSEC Process
(3) The OPSEC Assessment
(4) Format for Final OPSEC Assessment Report
(5) Examples of Critical Information List
(6) Appointment as the Marine Corps Air Station New River Department/Section Operations Security Monitor
(7) Appointment as the Marine Corps Air Station New River Operations Security Program Manager

1. Situation

a. Today's security environment has evolved from one in which the threat from identifiable adversarial nation-states has been joined by the less identifiable transnational terrorist. These adversaries have the will and the ability to do harm to United States interests both at home and abroad. Rapid advances in available, affordable information technologies and the development of sophisticated, aggressive collection organizations, forces us to reconsider what information can be used to compromise ongoing military operations.

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

must be considered. Methods of collecting critical pieces of information may include signals intelligence, human intelligence, imagery intelligence, measurement and signature intelligence, and open-source intelligence. The majority of collection efforts by adversaries are directed toward open source, unclassified information. In most cases, classified information is no longer essential or necessary to build an accurate intelligence picture of what military forces are doing. Using an abundance of easily obtained, unprotected information and objectives can be ascertained, and an appropriate response developed to deny us those objectives. Each Marine, Sailor, civilian, contractor, and their families 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. Cancellation. Air Station Order 3070.1C.

3. Mission

a. Develop and sustain an Operations Security (OPSEC) Program to prevent adversaries or potential adversaries from obtaining specific facts about Marine Corps Air Station (MCAS) New River's intentions, capabilities, limitations, and activities.

b. Summary of Revision. This Order has been revised and should be thoroughly reviewed.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. Deny potential adversaries unimpeded access to information that could be useful in developing actions intended to be disruptive to MCAS New River and Department of Defense (DoD) operations. End State: denial of access to critical information by potential adversaries through the elimination or mitigation of existing vulnerabilities.

(2) Concept of Operations. OPSEC concerns will be communicated to reduce inadvertent disclosures, giving close

attention to internet-based capabilities. Communication conduits are the Commanding Officers OPSEC Program Manager, OPSEC Monitors, Antiterrorism Officers, and Communications Strategy Liaisons. To be successful, the OPSEC Program will require commanding officers, department heads, and supervisors at all levels, both military and civilian, to reinforce the importance of good OPSEC practices with their subordinates. All personnel must adhere to the OPSEC policies designed and implemented to protect information from exploitation.

b. Tasks

(1) Station Directorates and Special Staff

(a) Comply with the intent of the references and the contents of this Order and the enclosures.

(b) Ensure personnel requesting access to networks have completed approved OPSEC training including social media awareness, controlled unclassified information (CUI), and security review for public release in accordance with (IAW) reference (d).

(c) Appoint a department/section OPSEC Monitor utilizing enclosure (6). Provide point of contact information to the Station OPSEC Program Manager. OPSEC Monitors will be guided in the performance of their duties IAW the references and enclosures (1) through (5).

(d) Develop tailored department/section OPSEC procedures utilizing the OPSEC process in reference (c).

(2) Station S-1

(a) Monitor and update the check-in/check-out procedures to support the requirement that all personnel joining and departing the Command check-in/check-out with the Command's OPSEC Program Manager.

(b) Provide the Station OPSEC Program Manager a list of civilian personnel depicting the completion of OPSEC training in Total Workforce Management System no later than 1 September annually.

(3) Station Plans and Operations (S-3). OPSEC is an operations function.

(a) Develop and implement the Installation OPSEC Program.

(b) Serve as the staff advocate for OPSEC.

(c) Appoint a DoD civilian as the Station OPSEC Program Manager, utilizing enclosure (7), per reference (e).

(4) Mission Assurance Program Manager. Integrate OPSEC agenda items in the Mission Assurance Working Group (WG) and incorporate OPSEC in the Random Antiterrorism Measures (RAMs).

(5) Headquarters and Headquarters Squadron (HQHQRON)

(a) Appoint an OPSEC Monitor, utilizing enclosure (6), to coordinate OPSEC efforts with the Station OPSEC Program Manager.

(b) Provide OPSEC subject matter compliance and recommendations.

(c) Coordinate OPSEC education and training for military, civilian, and contracted members of HQHQRON; to include family member education.

(d) Coordinate and conduct periodic internal reviews and assessments, utilizing standardized checklists or audit tools, with the Station OPSEC Program Manager.

(e) Participate as a member of the OPSEC Assessment Team and OPSEC WG (OWG), when required.

(f) Ensure all HQHQRON personnel and family members are familiar with and adhere to this Order.

(g) Ensure all HQHQRON personnel authorized to review and/or release information for public accessibility have completed the required OPSEC training.

(h) Submit records of training to the Station OPSEC Program Manager upon request.

(i) Produce an annual report depicting the completion of the required OPSEC training for all new joins, upon accession to HQHQRON.

(6) Security Management Office

(a) Ensure the completion of approved OPSEC training and the review of the Command's Critical Information List (CIL) by all new-join personnel and those seeking revalidation of network access.

(b) Prior to validating the System Authorization Access Request (SAAR), DD Form 2875, confirm with the requestor's supervisor, the requestor has completed all required OPSEC training outlined in reference (d).

(7) OPSEC Program Manager

(a) Provide OPSEC subject matter expertise and recommendations to the CO, MCAS New River.

(b) Develop, coordinate, and maintain the Command OPSEC Program, to include writing policy and guidance documents, utilizing enclosures (1) through (5).

(c) Coordinate and conduct an annual assessment of the OPSEC Program utilizing the references and provide copy to Station Operations.

(d) Develop and sustain OPSEC Program and policy training for all applicable HQHQRON personnel.

(e) Establish an Interagency OPSEC Support Staff (IOSS) account within 30 days of appointment.

(f) Coordinate OPSEC surveys.

(g) Conduct an annual OPSEC review.

(h) Chair the OWG to address OPSEC matters among the staff, departments, and higher headquarters (HHQ). The OWG may be combined with other established WGs.

(i) Coordinate with other WGs on OPSEC related matters.

(j) Develop and maintain a CIL.

(k) Coordinate with the Marine Corps Installations East-Marine Corps Base, Camp Lejeune (MCIEAST-MCB CAMLEJ) OPSEC Program Manager for command assist visits, inspections, and support as needed.

(l) Ensure all personnel are provided access to OPSEC education and training awareness annually.

(m) Complete on of the following training courses within 30 days of appointment:

1. IOSS OPSEC Fundamentals Computer Based Training (OPSE-1301): https://www.iad.gov/ioss/.

2. OPSEC Fundamentals (IO-OP101.16): https://www.cdse.edu/catalog/elearning/IO-OP101.html.

(n) Complete one of the following training courses within 90 days of appointment:

1. OPSEC and Public Release Decisions (OPSE-1500): https://www.iad.gov/ioss/.

2. OPSEC Analysis Course (OPSE-2380 or equivalent): https://www.iad.gov/ioss/.

3. Resident OPSEC Program Management Course (OPSE-2390), Naval OPSEC Support Team Program Managers Course, Defense Security Service Academy DoD OPSEC Officers Course, or equivalent.

4. OPSEC and Internet Based Capabilities Course (OPSE-3500): https://www.iad.gov/ioss/.

(8) OPSEC Monitors

(a) Complete the required annual OPSEC training based on the requirements of the position and/or department.

1. OPSE-1301: https://www.iad.gov/ioss/.

2. IOSS Web OPSEC Awareness training: https://www.iad.gov/ioss/.

(b) Complete the following training based on the additional requirements of the position and/or department. The Station OPSEC Program Manager will make the final determination.

1. OPSE-1500: https://www.iad.gov/ioss/.

2. OPSE-3500: https://www.iad.gov/ioss/.

(c) Ensure department/section members complete required OPSEC education and training per the references.

(d) Coordinate OPSEC education and training within the department that also includes family members.

(e) Provide OPSEC subject matter support and recommendations to the department/section.

(f) Participate as a member of the OWG.

(g) Provide OPSEC related recommendations to the Station OPSEC Program Manager and OWG.

(h) Conduct an annual review of the CIL with personnel who have a valid need to know.

(i) Assist in conducting the annual Installation OPSEC review and perform department/section OPSEC reviews and assessments as required.

(j) Provide input to the Station OPSEC Program Manager for submission of OPSEC lessons learned to the Marine Corps Center for Lessons Learned/Joint Lessons Learned Information System.

d. Coordinating Instructions

(1) Annual OPSEC training requirements for all personnel include an overview of the OPSEC process, defining OPSEC and its relationship to the Command's security programs, review of the current CIL, review the list of the Command's personnel fulfilling OPSEC responsibilities for situational awareness, understanding OPSEC indicators, and defining and reporting OPSEC violations, discrepancies, and punitive repercussions for OPSEC violations. At a minimum, the following will be included as part of the OPSEC education program and training requirements:

(a) OPSEC Awareness for Military Members, DoD Employees, and Contractors: http://cdsetrain.dtic.mil/opsec/.

(b) Uncle Sam's OPSEC (OPSECUS001): https://www.marinenet.usmc.mil/.

(c) Civilian Cyber Awareness Training (CYBERC): https://www.marinenet.usmc.mil/.

(d) United States Marine Corps Cyber Awareness Training (CYBERM0000): https://www.marinenet.usmc.mil/.

(e) Navy OPSEC briefs: http://www.navy.mil/ah_online/OPSEC/briefs.asp.

(2) An annual OPSEC assessment ensures the program receives regular Command attention and is continually evaluated in order to remain relevant to Command needs.

5. Administration and Logistics

a. Service members who willfully or negligently compromise OPSEC Critical Information or violate OPSEC policy may be subject to administrative and/or punitive action pursuant to the Uniform Code of Military Justice and reference (d).

b. Civilian persons who willfully or negligently compromise OPSEC Critical Information or violate OPSEC policy may receive corrective, disciplinary and/or other adverse action per reference (i).

c. Recommendations concerning the contents of this Order shall be forwarded to Station Plans and Operations (S-3).

6. Command and Signal

a. Command. This Order is applicable to all MCAS New River personnel, service members, contracted personnel, and their families.

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

G. W. BURNETT

DISTRIBUTION: B

OPSEC Terms and Definitions

1. This enclosure contains common use terms and definitions associated with OPSEC and are provided for a more detailed understanding of OPSEC and to assist with the OPSEC Program creation process.

a. Critical Information. 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; the CO must evaluate each activity and operation and then balance required OPSEC measures against operational needs.

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

d. OPSEC Assessments. An 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. 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 five steps of the OPSEC Process.

(1) The five steps of the OPSEC process are usually applied in a sequential order:

(a) Step 1: Identification of critical information.

(b) Step 2: Analysis of threats.

(c) Step 3: Analysis of vulnerabilities.

(d) Step 4: Assessment of risk.

(e) Step 5: Application of OPSEC measures.

(2) In dynamic situations, the five steps may be revisited at any time to adjust to new threats or information. A detailed explanation of the OPSEC process is provided in enclosure (3).

g. OWG. Teams of personnel with representatives from the different elements of the Command's organization designed to assist the Command with OPSEC matters and the OPSEC Program.

h. Threat. Any individual or organization that seeks to do harm by interrupting ongoing military operations or activities.

(1) In order to be classified a threat, two conditions must be satisfied:

(a) An intent to do harm must exist.

(b) A capability to do harm must exist.

(2) If both conditions cannot be met, then a threat does not exist.

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

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

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

The OPSEC Process

1. General. Using the OPSEC process will help the CO assess the risk and apply appropriate OPSEC measures.

a. OPSEC is a Command responsibility.

b. OPSEC is an operations function vice security, intelligence, or counterintelligence (CI) function.

c. OPSEC is a process in identifing critical information, analyzing friendly actions concerning military operations and activities, vulnerabilities, exploiting the threat to gain information, and implementing measures to reduce vulnerabilities thereby protecting critical information.

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

a. Step 1: Identification of Critical Information. The CO and staff tries to identify the questions the enemy will need to know about friendly intentions, capabilities, limitations, and activities. These questions are the EEFI. Critical information is only part of the EEFI; it is the information vitally needed by the enemy and will often be similar to what you would want to know about the enemy. This serves to focus the OPSEC process on protecting the vital information, rather than attempting to protect all information.

b. Step 2: Analysis of Threats. This involves the research and analysis of intelligence information, CI or CI reports, and OSINT to identify who the likely enemy will be. The friendly CO will ask questions, such as:

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

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

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

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

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

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

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

(8) How does the enemy process and disseminate their collected data?

c. Step 3: Analysis of Vulnerabilities. This action identifies an operation's or activity's vulnerabilities. The analysis 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 taking appropriate and timely action. The CO will need answers to questions such as:

(1) What OPSEC indicators of critical information, not known to the enemy, will be created by friendly actions resulting 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; planners analyze the identified vulnerabilities and possible OPSEC measures against them, and then select specific OPSEC measures for execution based on the risk assessment.

(1) OPSEC measures can be used to:

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

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

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

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

(a) Concealment and camouflage.

(b) Deception across all aspects of operations and information operations.

(c) Intentional deviations from normal patterns providing a sense of normality.

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

(3) OPSEC measures are most effective when they provide the maximum protection while minimally effecting operational effectiveness.

(a) More than one OPSEC measure may be identified for each vulnerability, and one OPSEC measure can be identified for multiple vulnerabilities.

(b) Primary and secondary OPSEC measures can be identified for single or multiple OPSEC indicators.

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

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

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

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

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

(e) Will implementing a particular OPSEC measure create an OPSEC indicator?

(f) Will implementing a particular OPSEC measure create an OPSEC indicator that you want the enemy to see?

(g) 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. Solid staff functioning and planning will ensure OPSEC plans integrate with and support other programs and operations.

e. Step 5: Application of OPSEC Measures. The CO implements the OPSEC measures selected in the previous step. Planning and integrating OPSEC measures into the operations plan (OPLAN) is critical to ensure countermeasures are applied at the right time, place, and in the correct manner.

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

(a) If the OPSEC measure producing the desired effect or is it producing an undesired effect?

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

(c) Will continuing to execute the OPSEC measure still be effective or has it accomplished its task and been overcome by the tempo of operations?

(d) Will ceasing the OPSEC measure produce negative or unintended consequences or no observable results?

(e) Does the OPSEC measure need to be modified based on the result?

(f) Does a previously selected or secondary OPSEC measure(s) need to be implemented to replace ineffective OPSEC measures based on the results?

(g) Do new OPSEC measures need to be devised to replace ineffective OPSEC measures?

(h) Have we identified new requirements or unforeseen OPSEC indicators that will need new OPSEC measures?

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

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

The OPSEC Assessment

1. General. The purpose of the OPSEC assessment is to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists. The operation or activity being assessed uses OPSEC measures to protect its critical information. The OPSEC assessment is used to verify the effectiveness of OPSEC measures and will determine if critical information identified, during the OPSEC planning process, is being protected. An OPSEC 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. Any department or section may request a formal assessment after completion of their internal assessment. At a minimum, each department/section will conduct an annual assessment utilizing reference (h).

a. Each OPSEC assessment is unique due to the differing activities of varied units. Additional factors are the nature of the information to be protected, the enemy's intelligence collection capabilities, and the environment of the activity to be surveyed.

b. 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 and installations. However, assessment teams should also ensure security measures are not creating OPSEC indicators.

c. Assessments are not a punitive tool and should be conducted on a non-attribution basis to ensure better cooperation and honesty when surveying activities, plans, and operations.

3. Two Types of Assessments

a. Command Assessment. Concentrates on events within the department/section and is from within the Command. The majority of assessments will be this type. The scope of these assessments can vary depending on Command guidance. Recognizing that an all-encompassing assessment would levy a high burden, Commands are encouraged to develop an approach in which

which functions are routinely evaluated, but done so over a period of time. For example, a department and/or section could evaluate administrative OPSEC during one period, while evaluating website OPSEC during the next period.

b. Formal Assessment. Is composed and conducted by members from within and/or outside the Command. The formal assessment will often cross command lines and needs to be coordinated appropriately. Formal assessments are normally directed by HHQ 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.

4. Results of Assessments. Assessment results should be given to the department/section of the unit surveyed and forwarded to HHQ on a non-attribution basis to derive lessons learned that may be applied to other units within MCIEAST.

5. 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 functional areas could be evaluated: intelligence collection operations; logistics; communications; operations; and administration and support.

b. Select the Assessment Team Members. Select members from the various staff functions and other entities as needed to ensure an adequate breadth of expertise. OPSEC is an operations function; thereforen the team leader should be from Station Plans and Operations (S-3).

c. Understand the Operation or Activity to be Assessed. Team members must be thoroughly briefed on the OPLAN and any other matters effecting the operation. This will help team members develop a functional outline for the aspect of the operation the team members are responsible to survey.

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

e. Conduct Empirical Studies, if Possible. An example would be to review results of preparations for a major operation or activity such as support operations computer simulations, war games, sand table exercises, field exercises, and command post exercises. This may already be available from information used to complete step 3 of the OPSEC process. These reviews can help the team identify vulnerabilities that cannot be determined through observation of the operation and interviews of personnel.

f. Develop a Functional Outline. Functional outlines for each functional area to be surveyed will be completed. 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. by developing a timetable of events to occur and 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. Use the chronology to build a functional outline. The functional 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 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.

(2) Actual Event Sequence. Observe and record events as they actually occur while surveying activities. Be especially cognizant of the information listed in paragraph 6.

(3) Critical Information. List critical information the Command has identified in the OPSEC Program or OPLAN.

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

(5) OPSEC Measures. List the OPSEC measures developed in the OPSEC Program or OPLAN expected to see during the assessment.

(6) Analysis. Determine any OPSEC vulnerabilities through review of the OPSEC Program, command/staff briefs, and actual activities/operations observed. Look for OPSEC indicators revealing 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?

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 procedure needed, including coordinating for unimpeded access to units and personnel. Determine if any training is required or if members need familiarization with a particular functional area.

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

(1) Assessment purpose and scope.

(2) List of team members and clearances.

(3) List of required briefing and orientations.

(4) Timeframe involved.

(5) Administrative or logistical support requirements.

(6) Any other details deemed pertinent.

6. OPSEC Field Assessment 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 brief can be a formal presentation or informal discussion and include a summary of the hostile threat collection capabilities and the vulnerability assessment.

(1) The CO and staff brief the OPSEC Program or OPLAN to the assessment team. The assessment team should take this opportunity to clarify questions developed in the planning phase.

(2) The assessment team briefs the command on the assessment objectives and procedures. The department/section should be asked to comment on this to validate the assessment.

b. Refine the Functional Outlines. Using information from the 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 is a chronological record of what actually was done or happened, who did it, where it happened, and how and why it was done. The recordings should include an assessment of the identified vulnerabilities in light of the enemy collection threat and any OPSEC indicators generated by the activities or operations.

(4) If a finding is considered to have serious negative mission impact, the department/section 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.

7. Analysis and Reporting Phase. The assessment team correlates and assesses the collected field assessment data.

a. Identify Vulnerabilities. Correlate and assess the data to identify the previously developed vulnerabilities and those identified during the field assessment. Observed OPSEC indicators are identified as potential vulnerabilities.

(1) Vulnerabilities are conditions that the threat may be able to exploit to reveal critical information.

(2) The key characteristics of vulnerabilities are observable OPSEC indicators and the threat's ability to collect or observe the indicators.

(3) The ability of the threat to effectively exploit the vulnerability in a timely manner indicates the actual risk to friendly forces.

b. OPSEC Assessment Report. The report is generated, addressed, and delivered to the CO of the operation/ activity surveyed. Format for findings can be presented in chronological order, order of significance, or grouped into the different functional areas. The report should discuss:

(1) Observed OPSEC indicators.

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

(3) Vulnerabilities identified.

(4) Analysis of the vulnerability's risk to the department/section's operations.

(5) Recommended OPSEC measures or modification to existing OPSEC measures.

(6) How the critical information is being protected.

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

Format for Final OPSEC Assessment Report

1. Overview

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

b. Conduct of Assessment. Brief discussion of team composition, procedures used, the department/section visited, timeframes involved, and any problems encountered.

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

d. Threat. List the enemy intelligence collection capabilities.

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

a. Observation. List the observed OPSEC indicators that could reveal identified information. This will include previously identified indicators and indicators not previously identified but observed during the assessment.

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

c. Conclusions/Recommendations. Recommend OPSEC measures to counter the OPSEC indicators to protect the critical information. If the OPSEC assessment team does not have the expertise and knowledge to recommend an OPSEC measure, state it. The command can plan, develop, and apply appropriate OPSEC measures for future or current operations. The department/ section needs to determine if OPSEC lessons learned can be applied to other departments/sections and disseminate the information appropriately. Care must be taken to appropriately classify and handle the final OPSEC assessment report IAW the appropriate security directives.

Examples of Critical Information List

1. The CIL identifies types of information MCAS New River personnel shall use to identify unclassified, but sensitive information, requiring application of OPSEC measures. This is not an all-encompassing checklist which can be applied to all situations. Department/section and their staffs will use their judgment and experience and develop critical information unique to their mission.

2. The CIL provides nine relevant areas of information and examples of information which may fall under each category.

a. Personnel Information

(1) Privacy Act and personally identifiable information.

(2) Joint Personnel Adjudication System data.

(3) Standard Labor Data Collection and Distribution Application data.

(4) Defense Travel System data.

(5) Training records.

(6) Timecards.

(7) Vehicle registration data.

(8) Ranks/names of officers and staff noncommissioned officers on assigned base quarters.

b. Unit Information

(1) Appointment letters.

(2) Access rosters.

(3) Work schedules.

(4) Personnel strengths and shortfalls.

(5) Watch schedules and reaction times.

(6) Training data of units using MCAS New River facilities.

c. Facilities Information

(1) Identification of any open access entry control points.

(2) Geographical Information Services or other mapping sources with specific plain language identification of sensitive areas.

(3) Building schematics; even if available through open source or via contract bid.

(4) Specific CO office location within headquarter buildings.

(5) Mission essential vulnerable area lists.

(6) Critical infrastructure, assets, and Supporting Infrastructure Critical Assets (SICA) information, locations, and schematics to include: water systems, electrical grids, communications nodes.

(7) Critical infrastructure and SICA capabilities and/or limitations.

(8) Maintenance requests and contracts.

(9) Future construction project information.

(10) Contract information.

(11) Planned land use.

(12) Locations of sensitive storage and staging sites, maps, and text to include: hazardous material (HAZMAT), arms, ammunition, and explosives.

d. Equipment and/or Specialized Equipment Information

(1) Security camera locations and/or capabilities.

(2) Intrusion detection system locations and/or capabilities.

(3) Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) sensor locations and/or capabilities.

(4) Equipment capabilities, maintenance issues, and shortfalls.

(5) Antiterrorism and Physical Security devices and equipment.

e. Plans, Policies, and Procedures

(1) Mission Assurance plans.

(2) Integrated action sets.

(3) Special orders.

(4) Security plans.

(5) CBRNE response capabilities, guidelines, and procedures.

(6) Force protection condition security augmentation requirements.

(7) DoD Education Activity school critical incident plans.

(8) Installation and unit RAMs.

(9) Installation emergency management plan.

(10) Continuity of operations plans.

f. Information Technology and Communications Systems Information

(1) SAAR database.

(2) System Security Accreditation Agreement data with associated internet protocol addresses.

(3) Information assurance vulnerability program data.

(4) Interim approval to operate/connect data.

(5) Protected distribution system approvals.

(6) Common access card electronic data interchange personal identifier information.

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

(1) Security, risk, vulnerability, and criticality assessments.

(2) Physical Security and crime prevention surveys.

(3) Documents labelled law enforcement sensitive, such as, threat and location observation notices, Federal Bureau of Investigation alerts, etc.

(4) Security and Emergency Services Company, Headquarters and Support Battalion, MCIEAST-MCB CAMLEJ Provost Marshal Office, Fire and Emergency Services, and Brig incident reports, traffic accident reports, blotters, desk journals, and statistic sheets.

(5) Safety mishap reports and associated records.

(6) Completed or ongoing internal and criminal investigations.

h. Special Event Information

(1) Distinguished visitor information to include: transportation, special security, family, billeting, and movement itinerary.

(2) Security plans, schedules, strength, routes, and identification.

(3) Locations of visit events and stop locations.

(4) Special event letters of instruction.

i. Logistics Information

(1) Freight shipment data associated with particular exercises or operations.

(2) HAZMAT and ammunition shipments.

(3) Ammunitions requests.

(4) Billing and accounting data.

(5) Transportation Management Office personal property files.

(6) Transportation Operational Personal Property System data.

(7) Supply shortages.

ASO 3070.1D
SEP 2 6 2022

COMMAND LETTERHEAD

3070.4
CO
DD MON YYYY

From: Commanding Officer, Marine Corps Air Station New River
To: Rank First M. Last EDIPI/MOS USMC

Subj: APPOINTMENT AS MARINE CORPS AIR STATION NEW RIVER DEPARTMENT/SECTION OPERATIONS SECURITY MONITOR

Ref: (a) DoDD 5205.02E Ch 2 of 20 June 2012
(b) MCO 3070.2A
(c) SECNAVINST 3070.2A
(d) MCIEAST-MCB CAMLEJO 3070.1A
(e) ASO 3070.1D

1. Per the references, you are appointed as the Marine Corps Air Station New River Department/Section Operations Security (OPSEC) Monitor.

2. You will be guided in the performance of your duties per the provisions of the references.

3. You shall report directly to the Station OPSEC Program Manager in matters regarding OPSEC.

I. M. COMMANDER

Copy to:
OPSEC Program Manager
Station S-3

Enclosure (6)

ASO 3070.1D
SEP 2 6 2022

COMMAND LETTERHEAD

3070.4
CO
DD MON YYYY

From: Commanding Officer, Marine Corps Air Station New River
To: Rank First M. Last EDIPI/MOS USMC

Subj: APPOINTMENT AS MARINE CORPS AIR STATION NEW RIVER OPERATIONS SECURITY PROGRAM MANAGER

Ref: (a) DoDD 5205.02E Ch 2 of 20 June 2012
(b) MCO 3070.2A
(c) SECNAVINST 3070.2A
(d) MCIEAST-MCB CAMLEJO 3070.1A
(e) ASO 3070.1D

1. Per the references, you are appointed as the Marine Corps Air Station New River Operations Security (OPSEC) Program Manager.

2. You will be guided in the performance of your duties per the provisions of the references.

3. You shall report directly to the Station Operations Officer in matters regarding OPSEC.

I. M. COMMANDER

Copy to:
Station S-3

Enclosure (7)