UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE
PSC BOX 20005
CAMP LEJEUNE NC 28542-0005

MCIEAST-MCB CAMLEJO 3070.1A
G-3/5

FEB 1 2 2021

MARINE CORPS INSTALLATIONS EAST-MARINE CORPS BASE CAMP LEJEUNE
ORDER 3070.1A

From: Commanding General
To: Distribution List

Subj: OPERATIONS SECURITY (OPSEC)

Ref: (a) DODD 5205.02E Ch 1, "DOD Operations Security (OPSEC)
           Program," May 11, 2018
       (b) JP 3-13.3, Joint Doctrine for Operations Security
       (c) SECNAVINST 3070.2
       (d) MCO 3070.2A
       (e) CJCSI 3213.01D, Joint Operations Security
       (f) DON OPSEC, NTTP 3-13.3M/MCTP 3-32B, Operations
           Security (OPSEC)
       (g) CMC DCMS Washington DC R221834Z Feb 18, Headquarters
           Marine Corps (HQMC) Critical Information List
           (CIL) (NOTAL)
       (h) UCMJ
       (i) 5 U.S.C. Chapter 75
       (j) DoDM 5220.22 Ch1, Volume 2 "National Industrial
           Security Program," September 30, 2020
       (k) DoD 5200.39, "Critical Program Information (CPI)
           Protection within the Department of Defense," May 28,
           2015
       (l) Regulations of the National Archives and Records
           Administration (NARA) Code of Federal Regulations
           (CFR)

Encl: (1) Glossary
       (2) The OPSEC Process
       (3) Examples of Critical Information
       (4) Examples of OPSEC Indicators
       (5) Examples of OPSEC Countermeasures
       (6) OPSEC Assessment
       (7) Notional OPSEC Plan
       (8) Contract, Acquisition, and Procurement Requirements
       (9) OPSEC Continuity Book Format Example
       (10) OPSEC Assessment Procedures
       (11) MCIEAST-MCB CAMLEJ G-3/5 PLANS 1 OPSEC Review Form

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

1. Situation

a. Today's security environment has evolved from one in which the threat from identifiable nation-states has been joined by the less identifiable transnational and homegrown terrorist, as well as foreign allies and United States (U.S.) citizens. Regardless of status, these adversaries all seek access to information and have the will and ability to harm U.S. interests at home and abroad. Through a variety of means, whether it is sophisticated methods such as signals or imagery intelligence, or the more unsophisticated methods such as open source intelligence, the adversary seeks to gain an advantage and hinder the success of ongoing and future military operations.

b. While the protection of classified information is a priority, personnel must also focus on protecting unclassified, but sensitive, and open source materials used in day to day operations; hence "Operations Security," or OPSEC. Methods of collecting Critical Information include Signals Intelligence (SIGINT), Human Intelligence (HUMINT), Technical Intelligence, and Open Source Intelligence, to name only a few. With 90 percent of collection efforts by adversaries directed towards open source unclassified information, the application of the OPSEC process must be a part of day to day activities.

c. Classified information is no longer essential to build a fairly accurate picture of what military forces are doing and using the OPSEC Process will reduce the adversary's capability to obtain information on the command's Capabilities, Activities, Limitations, Intentions (CALI), and installation protection objectives. Using easily obtained, unprotected information, friendly force objectives can be ascertained and an appropriate adversary action developed to deny those objectives. Each Marine, Sailor, Civilian Marine and contractor 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. MCIEAST-MCB CAMLEJO 3070.1.

3. Mission

a. Marine Corps Installations East-Marine Corps Base Camp Lejeune (MCIEAST-MCB CAMLEJ) will maintain an OPSEC Program to

2

protect Critical Information from exploitation by adversaries.

    b. <u>Summary of Revision</u>. This Order updates the MCIEAST-MCB CAMLEJ OPSEC Order. It has been revised to update policies and procedures and should be reviewed in its entirety.

4. <u>Execution</u>

    a. <u>Commander's Intent and Concept of Operations</u>

        (1) <u>Commander's Intent</u>. To deny potential adversaries access to information that could be useful in developing disruptive actions to ongoing and future operations. This will be accomplished by the following actions:

        (a) Implementation of an OPSEC Program and policies within each command and organization within MCIEAST-MCB CAMLEJ. MCIEAST-MCB CAMLEJ headquarters, all MCIEAST installations, and subordinate commands/organizations, will establish an OPSEC Program and institute OPSEC policies in accordance with references (a) through (k) and this Order.

        (b) Provide OPSEC training as outlined in this Order and disseminate the Commander's OPSEC Critical Information List (CIL).

        (c) Continued education of users at all levels to raise awareness and to better control the information on the Commander's OPSEC CIL.

        (d) Commanders and supervisors at all levels continually reinforce good OPSEC practices and enforce the policies contained in references (a) through (f).

        (e) The desired end-state is denial of access to critical information by potential adversaries through the elimination or mitigation of existing OPSEC vulnerabilities. OPSEC shall be coordinated and integrated into all areas to include contracting, personnel, information, cyber, acquisition and procurement, industrial, law enforcement, antiterrorism/force protection (AT/FP), and physical security.

(2) Concept of Operations

(a) OPSEC is the responsibility of each Commander. MCIEAST installations and subordinate commands/organizations will develop and maintain OPSEC programs based on the references. An annual OPSEC assessment conducted on each installation's program will ensure that OPSEC programs receive command attention and are evaluated in order to remain relevant. By implementing this guidance, MCIEAST installations and subordinate commands/organizations will decrease vulnerabilities by degrading adversary abilities to collect Unclassified, but Sensitive and Critical Information.

(b) In order to reduce inadvertent disclosures, command leadership at all levels should ensure command's unclassified CIL and OPSEC concerns are shared with military Service Members, civilian employees, on-site contractors, and civilian family members. Leaders are encouraged to use family-oriented written media and briefs provided by the OPSEC Coordinator or Monitor, to inform family members of the need for OPSEC.

(c) Enclosures (1) through (11) should be used in conjunction with this Order.

b. Tasks

(1) MCIEAST-MCB CAMLEJ shall:

(a) The MCIEAST-MCB CAMLEJ Assistant Chief of Staff, G-3/5 is the office of primary responsibility for OPSEC matters and will develop and maintain the MCIEAST Regional OPSEC Program and MCB CAMLEJ OPSEC Programs.

(b) Commanders are responsible for their command OPSEC Program and will maintain an effective program that ensures coordination between Communications Strategy and Operations (COMMSTRAT) or media representative, Cybersecurity, Physical Security, Operations, Acquisition and Procurement, Intelligence, Naval Criminal Investigative Service (NCIS), AT/FP, Law Enforcement, Critical Infrastructure, Training, Contracting, and the command's leadership. Each OPSEC Program shall include processes to report and mitigate disclosures of OPSEC Critical Information and address the punitive and

potential disciplinary actions for those who violate OPSEC through negligence or disregard of policy. Each OPSEC Program shall include mechanisms for enforcement, accountability, and the highest level of leadership oversight.

       (c) Management of the Regional OPSEC Program can be delegated to an OPSEC Program Manager in accordance with references (c) and (d).

       1. Because continual training and "best practice" is vital to an OPSEC program, it is essential that appointed OPSEC Program Managers and Coordinators are provided the opportunity and resources to attend OPSEC-related training courses, conferences, working groups, and meetings in accordance with references (c) through (e) and this Order.

       2. Each OPSEC Program Manager or Coordinator must have command support and sufficient authority to manage the program.

       3. The Commander's OPSEC Program Manager or Coordinator shall have access to the Commander in accordance with references (c) and (d), to ensure the Commander is kept informed on the command's OPSEC program and any concerns.

       (d) To manage the MCIEAST-MCB CAMLEJ OPSEC Program, the Commanding General (CG) will appoint in writing a Regional OPSEC Program Manager/OPSEC Planner in accordance with references (c) and (d). In accordance with reference (c), the Regional OPSEC Program Manager must be a U.S. citizen and have a favorably adjudicated Single Scope Background Investigation that has been completed within five years prior to assignment.

       1. The Regional OPSEC Program Manager's primary duties include: develop, maintain, and execute the organization's OPSEC Program to include writing policy and guidance, provide OPSEC subject matter expertise, advise the CG on OPSEC matters, ensure OPSEC training is conducted, conduct OPSEC reviews and assessments, and coordinate OPSEC efforts with all security disciplines (cyber, physical, law enforcement and investigations, etc.), logistics, Contracting, and COMMSTRAT; and advise appropriate actions for OPSEC violations.

2.   The Regional OPSEC Program Manager (OPM) provides OPSEC expertise for operations, security (cyber, physical, etc.), exercises, AT/FP, law enforcement, command security management, logistics, media, and day to day activities of the command; conducts OPSEC planning in accordance with applicable policy; plans for, executes, and monitors countermeasures and coordinates their execution with other commands and agencies that cross command boundaries.

3.   The OPM shall maintain a working relationship with AT/FP, Critical Infrastructure Protection, NCIS, Intelligence and Counterintelligence (if available), Installation Law Enforcement (Marine Corps Police), Criminal Investigation Division (CID), Installation Physical Security, Regional Contracting Office (RCO), Emergency Management, Information Assurance, Cybersecurity, and the Marine OPSEC Support Team (MOST).

4.   The Regional OPSEC Program Manager will ensure OPSEC reviews are conducted and documented on contracts, acquisition and procurement documents, requirements documents, Freedom of Information Act (FOIA) requests, Foreign Disclosures (FDO), MCIEAST-MCB CAMLEJ Orders, Bulletins, Policy Letters, Letters of Instruction, COMMSTRAT releases, Exercise Orders, Open Skies Missions, information sent for Wide Area Network (WAN) e-mail release, and any other information subject to public release or which may affect Critical Information.

5.   Provide assistance to MCIEAST installations and MCB CAMLEJ OPSEC Coordinators as required.

6.   Serve as HQMC OPSEC and the MOST's local liaison to tenant commands. Upon request, and when possible, assist the tenant commands with their OPSEC Programs.

7.   The Regional OPSEC Program Manager conducts OPSEC assessments, reviews, and inspections in support of command operations; conducts annual OPSEC reviews or assessments of subordinate commands, and identifies areas requiring additional OPSEC guidance, assistance, interpretation, or clarification. The Regional OPSEC Program Manager provides OPSEC lessons learned to the MOST for inclusion in the OPSEC lessons learned database.

8. The Regional OPSEC Program Manager monitors OPSEC education and training for all MCB CAMLEJ personnel, assists subordinate command's OPSEC training programs, requires appropriate OPSEC training and accountability documentation for all individuals prior to granting access to any Department of the Navy (DON) Non-secure Internet Protocol Router Network (NIPR), Secure Internet Protocol Router Network (SIPR), or other information technology in accordance with references (c) and (d).

9. The Regional OPSEC Program Manager conducts an annual command OPSEC Assessment of each installation's OPSEC program and coordinates the MOST OPSEC triennial assessment for each installation.

10. The Regional OPSEC Program Manager will chair both the Regional OPSEC Work Group (OWG) which shall meet at least once each fiscal year (FY), and the MCB CAMLEJ OWG which shall meet at least semiannually. The OWG may be combined with other working groups to enable coordination between related disciplines. It is the mission of the OWG's to address specific OPSEC issues; promote and monitor OPSEC awareness; conduct OPSEC reviews and assessments; develop OPSEC policy and training; ensure procedures are in place to control critical information and indicators thereby protecting essential secrecy.

11. The MCIEAST-MCB CAMLEJ G-3/5 will host OWGs as required to coordinate OPSEC matters among installations, facilities, departments, and staff; assist in developing the OPSEC Program throughout MCIEAST; develop, coordinate, and maintain the command's OPSEC Program to include written policy and program guidance.

(2) MCIEAST-MCB CAMLEJ Command Inspector General (CIG) shall:

(a) In conjunction with the OPSEC Program Manager, utilize the OPSEC Functional Area Checklist 3070 found in reference (d). Checklist can be found at https://www.hqmc.marines.mil/igmc/Resources/Functional-Area-Checklists/.

(b) OPSEC is a CORE functional area of the Inspector General of the Marine Corps (IGMC) Inspection Program and shall

be inspected during scheduled Commanding General's Inspection Program inspections.

      (c) Appoint an OPSEC Monitor as part of the MCB CAMLEJ OWG to perform OPSEC functions as required for the Office of the CIG.

      (3) <u>MCIEAST-MCB CAMLEJ General and Special Staff Department Heads shall</u>:

      (a) Appoint in writing an OPSEC Coordinator or an OPSEC Monitor for each respective department and/or section. Those with a small number of personnel (+/-10), minimal OPSEC needs (no public release documents, limited budgetary footprint, and no active social media or website), may coordinate with the Regional OPSEC Program Manager for a determination if appointing an OPSEC Monitor is sufficient for organizational OPSEC needs. Size and responsibility of Divisions, Branches, and Sections may require additional OPSEC support to support Department needs. MCIEAST-MCB CAMLEJ OPSEC Coordinators and OPSEC Monitors at MCB CAMLEJ are members of the installation OWG. See training requirements in paragraph 4c below in this Order for specific requirements for OPSEC Coordinators and OPSEC Monitors.

      (b) Duties of the OPSEC Coordinator or Monitor are to:

      <u>1</u>. Provide OPSEC subject matter support and recommendations to the department/section and advise the department head to ensure compliance with OPSEC policy.

      <u>2</u>. Coordinate OPSEC matters with the MCIEAST-MCB CAMLEJ Regional OPSEC Program Manager.

      <u>3</u>. Coordinate OPSEC education and training for members of the department/section to include the tracking and reporting of an annual review of the Commanding General's Critical Information List (CIL) by each person assigned to the department. Each Monitor shall submit an annual CIL Review report to the Regional OPM no later than September 1st of each year.

      <u>4</u>. Conduct OPSEC reviews and assessments as required by the OPSEC Program.

<u>5</u>.   Serve as member of an OPSEC Assessment or Review Team in support of the command's OPSEC Program.

<u>6</u>.   Provide representation to the MCB CAMLEJ installation OWG.

(4) <u>MCIEAST Commanders shall</u>:

(a) Ensure each OPSEC program includes processes to report and mitigate disclosures of OPSEC Critical Information and address the punitive nature and potential disciplinary actions for those who violate OPSEC through negligence or disregard of policy.   Each OPSEC Program shall include mechanisms for enforcement, accountability, threat awareness, and leadership oversight.

(b) Provide OPSEC guidance to their command.

(c) Ensure OPSEC is a function of Operations.   For those without an operations department, their OPSEC Program Manager or Coordinator responsibilities shall be assigned to individuals within an office with significant authority in command operations.   Commands without an S-3 or Operations Section should collaborate with the Regional OPSEC Program Manager at (910) 451-5720 for acceptable alternatives.

(d) Appoint, in writing, an OPSEC Program Manager or OPSEC Coordinator, whichever meets the needs of their command, and an Alternate OPSEC Coordinator (AOC).   Appointed personnel must be familiar with the operational aspects of the command and complete recognized formal OPSEC training.

(e) Ensure subordinate commanders (i.e. Headquarters and Support Battalion and Headquarters and Headquarters Squadrons) appoint OPSEC Coordinators in accordance with references (a), (c), and (d) and develop OPSEC programs tailored to their organization; develop their OPSEC policy/order signed by the commander; develop and distribute a signed Commander's OPSEC CIL, and utilize the OPSEC Planning Process.

(f) Share unclassified CIL and OPSEC concerns with the Deployment Readiness Officer (DRO), military and civilian family members in accordance with reference (d), and provide

OPSEC briefs and/or OPSEC Family Guides to inform family members of the need for OPSEC in accordance with references (b) and (d).

(g) The appointed command OPSEC Program Manager or OPSEC Coordinator, and an Assistant OPSEC Coordinator shall:

1. Develop and maintain an OPSEC Order or Policy for the Command OPSEC Program and conduct, at a minimum, a quarterly OWG.

2. Develop and implement an OPSEC program.

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

4. Designate subordinate units or activities that require an OPSEC program.

5. Coordinate OPSEC matters with the MCIEAST Regional OPSEC Program Manager.

6. Develop, coordinate, and administer OPSEC education and training. Ensure all military, civilian, and contractors are provided both online and unit-specific OPSEC education and awareness training within 90 days of joining and annually thereafter; monitor the command's OPSEC education and training for all assigned personnel; assist subordinate command's OPSEC training programs; require appropriate OPSEC training and accountability documentation for all individuals prior to granting access to any DON NIPR, SIPR, or other information technology in accordance with references (c) and (d).

a. Unit specific OPSEC education and awareness training shall include a review of the command's CIL, Indicators List, OPSEC Policy awareness, and the punitive nature of OPSEC violations.

b. If the command has a DRO assigned, the DRO will coordinate with the OPSEC Program Manager or Coordinator to ensure the command's OPSEC education and awareness training program includes family members and stresses the importance and role of family in OPSEC.

7. Conduct an annual assessment of the OPSEC Program effectiveness utilizing the OPSEC Functional Area Checklist 3070 and the assessment format in enclosure (10) as a guide. Submit assessment results to the MCIEAST Regional OPSEC Program Manager before the end of each FY.

8. Ensure the completion of OPSEC reviews of the command's orders, policies, bulletins, contracts, and information for public view or public release. Commands are encouraged to make use of the MCIEAST-MCB CAMLEJ G-3/5 PLANS 1 Form enclosure (11) to ensure and track the OPSEC review of items intended for public release to meet this requirement.

9. Provide representation to the MCIEAST Regional OWG. For the Commanding Officer, Headquarters and Support Battalion: also provide representation to the MCB CAMLEJ OWG and the OPSEC Assessment or Review Team in support of the MCB CAMLEJ OPSEC Program.

(h) For a commander's OPSEC Program Manager or Coordinator to effectively manage the OPSEC Process, commanders must determine and document the level of OPSEC risk they will accept.

(i) Depending upon the command's structure, Department Heads, most Directorate and Division Directors and Branch Heads, and some Section Heads and Office Managers should appoint an OPSEC Coordinator or an OPSEC Monitor. Those who have a small number of personnel (+/-10), minimal OPSEC needs (no public release documents, limited budgetary footprint, and no active social media or websites), may coordinate with their command's OPSEC Program Manager or Coordinator for a determination if appointing an OPSEC Monitor is sufficient for their OPSEC needs.

c. Coordinating Instructions

(1) The following shall be included as part of OPSEC education programs for all OPSEC Program Managers, Planners, and Coordinators:

(a) The IOSS OPSEC Fundamentals course OPSE-1301 CBT available at https://www.iad.gov/ioss/ or the OPSEC Fundamentals IO-OP101.16 available at:

11

https://www.cdse.edu/catalog/elearning/IO-OP101.html and must be completed within 30 days of appointment.

(b) OPSEC and Public Release Decisions OPSE-1500 available at https://www.iad.gov/ioss/ and must be completed within 90 days of appointment.

(c) OPSEC and Internet Based Capabilities Course OPSE-3500 available at https://www.iad.gov/ioss/ and must be completed within 90 days of appointment.

(2) OPSEC Program Managers, Planners, and Coordinators shall attend a resident OPSEC Program Management Course and OPSEC Analysis Course within 90 days of appointment.

(3) An OPSEC Monitor's training will be specified by the OPSEC Program Manager but will require, at a minimum, completing the OPSEC Fundamental Course (OPSE-1301) Computer Based Training (CBT). The OPSE-1500 and OPSE-3500 will also be considered if consistent with the requirements of the position. All are available at https://www.iad.gov/ioss/.

(4) OPSEC Coordinators and OPSEC Monitors are members of their command's OWG.

Available courses are:

(a) OPSEC Analysis Course OPSE-2380 and the OPSEC Program Management Course OPSE-2390 at https://www.iad.gov/ioss/

(b) Navy OPSEC Course (equivalent to OPSE-2380/2390) and available at http://www.navy.mil/ah_online/OPSEC/#services

(c) Defense OPSEC Managers Course DOMC-2480 (equivalent to OPSE-2380/2390)

(d) Defense OPSEC Coordinators Course DOCC-2480 (equivalent to OPSE-2380/2390)

(e) OPSEC Program Managers, OPSEC Coordinators, and other personnel (when specified) must complete the following OPSEC training:

    1.   The OPSEC Fundamental Course (OPSE-1301) CBT (must be completed within 30 days of appointment), OPSEC and Public Release Decisions (OPSE-1500) and the OPSEC and Internet Based Capabilities Course (OPSE-3500) within 90 days.

    2.   OPSEC Program Managers and OPSEC Coordinators at the regional, installation, battalion, and squadron command level shall complete the OPSEC Program Management Course (OPSE-2390) and the OPSEC Analysis Course (OPSE-2380), or the Navy OPSEC Support Team's two-day OPSEC Officer's Course.

    3.   OPSEC Program Managers, OPSEC Coordinators, and OPSEC Monitors who have a contracting, acquisition and procurement, Marine Corps Community Services, or other offices with significant acquisition and procurement responsibility within their command; and all contracting or acquisition and procurement office personnel shall complete the OPSEC Contract Requirements (CLC107 Section 892) course at the Defense Acquisition University at: http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=422. The commander's OPSEC Program Manager or Coordinator will make the final determination for this requirement.

    (f) In addition to the online annual OPSEC training directed by higher headquarters (HHQ), the following will be included in annually required, unit-specific OPSEC training for all personnel:

    1.   An overview of the OPSEC 5-Step Cycle.

    2.   Defining OPSEC and its relationship to the command's security programs and day to day activities.

    3.   Reviewing the current Commander's CIL.

    4.   Reviewing the list of the command's personnel fulfilling OPSEC responsibilities for situational awareness.

    5.   Understanding OPSEC Indicators.

    6.   Defining and reporting OPSEC violations and discrepancies.

5. Administration and Logistics

   a. Administration

    (1) Provide command OPSEC Coordinator and OPSEC Monitor contact information to the MCIEAST Regional OPSEC Program Manager.

    (2) Provide a copy of all OPSEC assessments and reviews to MCIEAST Regional OPSEC Program Manager.

    (3) Submit OPSEC assessment and review results to the MCIEAST Regional OPSEC Program Manager when requested.

    (4) OPSEC Program Managers and Coordinators of commands immediately subordinate to MCIEAST-MCB CAMLEJ shall maintain an up to date OPSEC Continuity Book in accordance with reference (e). Refer to the example in enclosure (10), which may also act as Turnover Folder and/or Standing Operating Procedures (SOP).

    (5) Records created as a result of this Order shall be managed in accordance with reference (l) approved disposition instructions to ensure proper maintenance, use, accessibility, and preservation, regardless of format or medium.

    (a) Concept of Record. The concept of record shall be defined as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business" in accordance with the International Organization for Standardization (ISO) 15489-1:2001.

    (b) Punitive Nature. Per reference (c), service members who willfully or negligently compromise OPSEC Critical Information or violate OPSEC policy are subject to administrative and/or punitive action pursuant to reference (h). Civilian employees who willfully or negligently compromise OPSEC Critical Information or violate OPSEC Policy may receive corrective, disciplinary, and/or other adverse action per reference (i) and 5 CFR Parts 731 and 752.

   b. Logistics

14

(1) Active promotion of OPSEC is the responsibility of all levels of commands. Commanders are encouraged to develop local OPSEC promotional materials and suitable techniques of promotion consistent with the law and funds available.

(a) Appropriated funds may be used to buy items to inform personnel on the OPSEC program. Ideally, such items will be appropriate to the work environment or serve as a reminder of the benefits of participating in the program. Coffee mugs, key rings, lanyards, pens, trifolds, posters, cards, etc., are typical promotional items. To the greatest extent possible, commands should share good information with Marine Corps Information Operations Center with attention to the MOST.

(b) As part of informational efforts, commanders at all levels shall:

1. Advertise the OPSEC program through posters, billboards, bulletins, or other media which frequently reach Marines, Sailors, Civilian Marines, contractors, and their family members.

2. Develop slogans, logos, and materials designed to promote their OPSEC program.

(2) Capture all costs associated with the OPSEC Program for future budgetary adjustments. Cost records should include all costs incurred for travel, training, equipment, and paper media (posters, circulars, bulletins, etc.).

6. Command and Signal

a. Command. This Order is applicable to all personnel employed by, detailed, or assigned to MCIEAST-MCB CAMLEJ General and Special Staff Departments, all MCIEAST subordinate commands/organization, including active and reserve personnel, Government Civilians (appropriated and non-appropriated funds); contractor personnel, any expert or consultant performing services for MCIEAST-MCB CAMLEJ through personnel appointment or contractual arrangement; industrial or commercial contractor, licensee, certificate holder, or subcontractors.

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

b. <u>Signal</u>. This Order is effective on the date signed.

N. E. DAVIS
Chief of Staff

DISTRIBUTION: A/B/C

16

Glossary

Terms and Definitions

1. Common use terms and definitions associated with OPSEC are provided for a clearer understanding of OPSEC, as well as assisting with the OPSEC cycle.

    a. Adversary. An opponent in a conflict or dispute. For this order, adversary is also intended to mean antagonist.

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

    c. Critical Information List (CIL). A list of critical information within an organization approved by the commander, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures. Each commander specifies critical information to protect and publishes it in the Commander's OPSEC CIL, which is signed by the Commander. Reference (g) is the Marine Corps CIL.

    d. Deception in Support of OPSEC (DISO). A DISO is a military deception activity that protects friendly operations, personnel, programs, equipment, and other assets against intelligence collection. The intent of a DISO is to create multiple false indicators to make friendly force intentions harder to interpret by those who seek to do harm.

    e. Essential Elements of Friendly Information (EEFI). Key information about specific friendly intentions, capabilities, and activities that adversaries pursue and try to obtain.

    f. Essential Secrecy. The condition achieved from the denial of critical information to adversaries through the combined efforts of traditional security programs and the OPSEC process.

    g. Essential Secrets. Aspects of friendly operations that, if compromised, would lead to adversarial knowledge of

exploitable conditions and a potential failure to meet the Commander's objectives and/or desired end-state.

h. Excessive OPSEC. Excessive OPSEC can degrade operational effectiveness by interfering with activities such as coordination, training, and logistical support. Each commander must evaluate their operations and activities, and then balance required countermeasures against operational needs.

i. OPSEC Assessment. 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 countermeasures and determine if critical information is being protected. OPSEC assessments are different from security evaluations or inspections. An OPSEC assessment attempts to produce an adversary's view of the operation or activity being assessed.

j. Operations Security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. Operations Security is commonly referred to simply as OPSEC.

k. OPSEC Coordinator. An individual trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC Program Manager or primary representative.

l. OPSEC Countermeasures. Methods and means to gain and maintain essential secrecy about critical information. These are actions taken to reduce the probability of an adversary gaining the commander's critical information, collecting OPSEC indicators, or correctly analyzing their meaning.

m. OPSEC Indicators. Friendly actions such as operations, exercises, training, day to day activities, and open sources of information that adversaries can potentially detect or obtain and derive friendly critical information. An indicator can be looked at by itself or in conjunction with something else. Various measures may be implemented to reduce the visibility of indicators or vulnerabilities. OPSEC indicators must also be taken into account when developing the initial CIL. There are five major characteristics of an OPSEC indicator. They are

Enclosure (1)

identified as signature, profiles, associations, contrasts, and exposure, or SPACE.

(1) Signature is an indicator that makes something identifiable or causes it to stand out.

(2) Profile is the signatures plus the associations. Adversaries look for patterns and signatures to establish a profile. Patterns are the way things are done, arranged, or have occurred.

(3) Association is the relationship of an indicator to other critical information or activities.

(4) Contrast is the differences observed between an activity's standard profile and it's most recent or current actions.

(5) Exposure is when and how long an indicator is observed.

n. <u>OPSEC Monitor</u>. When the commander's OPSEC Program Manager or OPSEC Coordinator has determined that a department, division, branch, section, or office has few personnel (+/-10) and a small need for the management of OPSEC, they may recommend that an OPSEC Monitor be appointed. The commander's OPSEC Program Manager or OPSEC Coordinator will determine the training requirements of that appointee.

o. <u>OPSEC Planner</u>. A functional expert trained and qualified to plan and execute OPSEC.

p. <u>OPSEC Planning Guidance</u>. Guidance that defines critical information requiring protection from the adversary and outlines provisional measures to ensure secrecy.

q. <u>OPSEC Process</u>. OPSEC planning is accomplished through the OPSEC Five-Step Process and is 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 is most effective when fully integrated into all planning and operational processes. A detailed explanation of the OPSEC Process is contained in references (b), (d), and (f).

r. <u>OPSEC Program Manager</u>. A full-time representative assigned to develop and manage an OPSEC Program.

s. <u>OPSEC Vulnerability</u>. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary.

t. <u>Protect</u>. Actions taken to shield from exposure, damage, or destruction; to keep from harm, attack, injury, or exploitation; to maintain the status or integrity of.

u. <u>OPSEC Review</u>. This is a measure whereby the OPSEC Program Manager or an OPSEC Coordinator conducts reviews of orders, bulletins, contracts, official websites and command sponsored social websites, public announcements, public affairs releases, FOIA requests and releases, FDO releases, and any other information that could be released to or accessed by the public.

v. <u>OPSEC Working Groups (OWG)</u>. OWG are teams of personnel from their particular organization and trained OPSEC appointees. These personnel assist the command with OPSEC matters and its program.

w. <u>Risk Management</u>. The process of selecting and implementing countermeasures to achieve the minimum level of risk accepted in writing by the commander, at an acceptable cost, both monetary and informational. Commanders must assess the effect of possible adversary exploitation of vulnerabilities on the effectiveness of their operation, exercise, or activity. They must then decide to either implement corrective actions or accept the risk posed by the vulnerability.

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

(1) An intent to do harm must exist.

(2) A capability to do harm must exist. If both conditions cannot be met, then a threat does not exist. The intent to do harm to America and its military is an ongoing threat. Since many state sponsored, non-state sponsored, and

lone actors have the intent and capability to do harm, a presumed threat will be present well into the future.

y. <u>Vulnerability</u>. 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 a basis for effective adversary decision-making.

The OPSEC Process

1. <u>General</u>. OPSEC is not a security, intelligence, counter-intelligence, or an administrative specific function. It is a command-wide task regardless of functional area. OPSEC is a command responsibility and is a process by which the command identifies critical information, analyzing friendly actions concerning military operations and activities - to include day to day activities, vulnerabilities, and the countermeasures that can be implemented to protect critical information.

2. <u>OPSEC Process</u>. The OPSEC process is a five step process.

    a. <u>Step 1: Identify Critical Information</u>. The Commander and staff identify the questions the adversary will need answered in order to anticipate friendly intentions, capabilities, and activities. Knowing what information is to be protected serves to focus the OPSEC Process rather than attempting to protect all information.

    b. <u>Step 2: Analyze Threats</u>. This involves research and analysis of intelligence information, counterintelligence, reports, and open source information to identify who the likely adversary will be. The Commander will ask questions, such as:

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

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

        (3) What may be the adversary's strategy for opposing the planned operation or activity to include day to day activities?

        (4) What type of tactics, techniques, and procedures might the adversary employ to get critical information?

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

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

Enclosure (2)

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

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

NOTE: NCIS is tasked by reference (c) to ensure relevant installation or activity specific counterintelligence information is developed and made available to support commanders' OPSEC programs.

c. Step 3: Determine Vulnerabilities. This action identifies an operation's or activity's vulnerabilities. This requires identifying OPSEC indicators that could reveal critical information. Vulnerabilities exist when the adversary is capable of observing an OPSEC indicator, analyzing it, and then taking appropriate action or aggregating the information for future use. The Commander will need answers to questions such as these:

(1) What OPSEC indicators of critical information not known to the adversary will be created by friendly actions that result from the planned operation or activity?

(2) What OPSEC indicators can the adversary actually collect?

(3) What OPSEC indicators can the adversary actually use to our disadvantage?

d. Step 4: Assess Risk. This step essentially has two components. First, planners analyze the identified vulnerabilities and then identify possible countermeasures against them. Second, specific countermeasures are selected for execution based on the risk assessment.

(1) Countermeasures can be used to:

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

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

(c) Directly attack the adversary's collection capabilities.

(2) Besides physical destruction, countermeasures can include:

(a) Concealment and camouflage such as that, which may be required to protect from Open Skies missions.

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

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

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

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

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

(a) What is the risk to mission effectiveness if a countermeasure is taken?

(b) What is the risk to mission effectiveness if a countermeasure is not taken?

(c) What is the risk to mission effectiveness if a countermeasure fails to be effective?

(d) Will the cost of implementing a countermeasure be too much as compared to the adversary's exploitation of the vulnerability?

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

(f) Do installations and commands even have the capability/resources to implement the countermeasure? If so, can the assets under installation control accomplish this, or do additional assets from outside sources need to be requested?

(5) Planning for countermeasures may require coordination amongst multiple staff and supporting elements or assets outside the command. Particular care must be taken to ensure that countermeasures do not interfere with other operations such as deception plans. Solid staff functioning and planning will ensure OPSEC plans integrate with and support other programs, operations, and activities.

e. Step 5: Apply Countermeasures. In this step, the commander implements the OPSEC countermeasures selected in the previous step (Risk Assessment). Planning and integrating OPSEC countermeasures into a plan or applying them to observable indicators in day to day activities is critical to ensure countermeasures are applied at the right time, place, and manner.

(1) Whenever possible, the adversary's reaction to our OPSEC countermeasures should be monitored to determine effectiveness. Provisions and methods for feedback from intelligence and counterintelligence staffs such as NCIS will have to be planned for in OPSEC plans. This feedback will help determine the following:

(a) Is the countermeasure producing the desired effect, no effect, or is it producing an undesired effect?

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

(c) Does the command need to continue executing the countermeasure? Will it still be effective, or has it accomplished its task and been overcome by the tempo of operations?

Enclosure (2)

(d) Does the command need to cease the countermeasure because of no observable results, negative, or unintended consequences?

(e) Does the command need to modify the countermeasure based on the result?

(f) Does the command need to implement previously selected (secondary) countermeasures to replace ineffective countermeasures based on the results?

(g) Does the command need to devise new countermeasures to replace ineffective countermeasures?

(h) Have new requirements or unforeseen OPSEC indicators been identified that will require new countermeasures? This is a dynamic process, and previous steps may have to be revisited.

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

(3) The OPSEC Assessment is an excellent method and is the primary tool for determining the effectiveness of countermeasures.

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. Commanders and their staffs will use their judgment and experience to develop critical information unique to their mission and location. The MCIEAST Commander's OPSEC CIL is available by contacting the MCIEAST Regional OPSEC Program Manager at (910) 451-5720.

2. Political and Military Crisis Management

    a. Deployment timelines and 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 civilian economy

    c. Transportation capabilities

4. Military Intervention

    a. Intentions

    b. Military capabilities

    c. Forces assigned

    d. Time considerations

    e. Logistic capabilities and constraints

5. Peacetime Weapons and other Military Movements

    a. Unit movements

    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

6. Command Post and Field Training Exercises

    a. Participating units

    b. Operations Plan or other contingencies that are being exercised

    c. Command relationships

    d. Logistics capabilities and weaknesses

7. Noncombatant Evacuation Operations

    a. Forces involved

    b. Logistic capabilities and constraints

    c. Staging areas

    d. Time considerations

8. 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.   Logistics capabilities and constraints

9. <u>Counterterrorism Operations</u>

    a.   Forces

    b.   Contingency plans

    c.   Standing SOP

    d.   Time considerations

    e.   Staging locations

    f.   Tactics

    g.   Ingress and egress methods

    h.   Logistics capabilities and constraints

Examples of OPSEC Indicators

1. OPSEC Indicators are friendly actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information. Indicators have five characteristics: SPACE. Their definitions can be found in references (a) through (f). Provided below are examples to help understand them.

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 air field. Analysis of the emissions indicates it is ground equipment used for medium or large fixed-wing transport aircraft. The intelligence analysts had previously identified different emissions from ground support equipment (GSE) and identified them as belonging to a particular aircraft or type of aircraft. The analysts only need 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 adversary to anticipate future actions. Reducing the uniqueness or stability of the indicator's signature increases the ambiguity of the adversary'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. Profiles. Each functional activity generates its own set of unique signatures and associations. The sum of these signatures and associations is the activity's 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 installation has many unique indicators. Over a period of several years, an adversary may have cataloged enough of these indicators and created a standard picture, or profile of the indicators, that an installation creates.

(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 adversary observes indicators, compares them to information they already have, then can identify what type of units are aboard an installation and what they are doing. If the adversary has identified the profiles for company of tanks and a reinforced infantry battalion conducting training, they might conclude that there is a regimental-size unit preparing to conduct operations.

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

(1) Using an example for an air installation, the adversary knows that heavy GSE or "yellow gear" is used for fixed-wing transport aircraft. The adversary may also know that the length and composition of the landing strip will support not only rotary wing aircraft, but transport aircraft as large as a C-130. An adversary would likely take the GSE indicator and associate it with the previous information, and conclude that KC-130s are or will be operating in the area.

(2) Another aspect to associations involves the continuity of actions, objects, or other indicators that register as patterns to an adversary or 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 heavy

GSE units are observed at the same air facility. Past
repetitive practices observed indicated that three GSE units
signify a detachment of six KC-130s conducting operations or
training.

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

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 adversary or
analyst's attention. They will then focus more collection
efforts to find out what the contrast signifies. For example,
the adversary or analyst identifies a profile of what appears
to be an infantry unit in an installation's training area but
observes indicators that do not fit that standard profile.
The adversary or analyst then focuses collection efforts and
observes more indicators. Comparing these indicators to their
current information reveals that there are units there that
fit the profile for a Marine Expeditionary Unit.

e. Exposure. Exposure refers to when and for how long an
indicator is observed. The duration, repetition, and timing
of an indicator's 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. An example might be an
increase in the number of trucks the adversary knows to be
carrying ammunition on to an installation.

(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 adversary to detect and evaluate the indicator.

3. The following provides examples of indicators that are associated with military and supporting establishment activities and information. This list is not all-inclusive and is presented to encourage thinking about what kinds of action can convey indicators that could betray critical information for specific friendly operations, training, or other activities.

    a. <u>Indicators of General Military or Support Capabilities</u>

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

        (2) Friendly reactions to adversary activity or security probes on an installation.

        (3) Actions, information, or material associating reserve units 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 to an installation).

        (7) Movement of friendly ships, aircraft, and/or ground units in and around one of our installations.

        (8) Actions, information, or material revealing tactics, techniques, and procedures employed in an installation security breach.
        (9) Stereotyped patterns in performing the organizational mission that reveal the sequence of specific actions or when and how they are accomplished such as traffic patterns entering an installation.

b.   Indicators from Communications

(1) Many personnel seen using handheld radios or vehicle radios on the installation.

(2) Establishing and testing new communication nets. The sudden appearance of a new net may cause the adversary to increase collection efforts.

(3) Increasing, decreasing, or ceasing radio transmission when close to starting an operation, exercise, or test. Again, without conditioning to desensitize adversaries, unusual changes will catch the adversary's attention and prompt adversary intelligence collection efforts.

(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 adversary monitoring and adds to profiles.

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

c.   Indicators for Equipment and Systems

(1) Budget data that provides insight into the objectives and scope of system development efforts or sustainability of a fielded system (this often comes from public media).

(2) The equipment or system hardware itself.

(3) Information on test, exercise, and training schedules that allows adversaries to better plan the use of collection efforts.

(4) Use of unique units, targets, or sensor systems in training areas that support tests or training associated with particular equipment or systems.

(5) Unusual visible security imposed on particular locations, areas, or development efforts that could highlight their significance.

(6) Information indicating special manning of personnel with special skills from manufacturers known to be working on a particular contract, activity, or system.

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

(8) Use of advertisements that a company has a contract on a particular system or component of a system, or has applied special technologies to sensors on training ranges.

d. 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 for participating units or countries.

(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, fuels, weapons, and other types of supply items.

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

(6) Accommodating an increased number of linguists of a particular language or related group of languages.

(7) Unusual activity with foreign nationals for military or training support.

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

(9) Increasing the number of trips and conferences for installation personnel.

(10) NOTAMS and NTMs announcing airspace and seaport reservations/restrictions.

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

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

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

e. Indicators during the Execution Phase

(1) Unit and equipment departures from base/station.

(2) Visual detection of friendly units.

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

(4) Trash dumped by units or picked up by commercial vendors that might provide unit identifying data or other information.

(5) Alert of civilians in or around training areas.

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

(7) Changes in activity or volume over the WAN.

f. 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.

g. Indicators from Internet-based Capabilities

(1) Posting sensitive information on social networking sites.

(2) Posting unit rosters.

(3) Posting photos with sensitive information in the background.

(4) Not turning off geo-tagging when taking photos in billeting, training areas, and other sensitive areas.

(5) Posting filenames and file tags with sensitive data included in the name.

(6) Accepting friend requests from unknown persons.

(7) Not properly using privacy and security settings and failure to encrypt sensitive information.

(8) Out-of-date anti-virus software.

(9) Not ensuring there is active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

(10) Posting Personal Identifiable Information, For Official Use Only, and/or SBU on public facing websites or social networking sites.

(11) Using location-based social networking and applications that can turn on a device's microphone.

Enclosure (4)

Examples of OPSEC Countermeasures

1. The following OPSEC countermeasures are examples only and are provided in order to generate ideas as Marines develop their own OPSEC countermeasures. Development of specific OPSEC countermeasures is as varied as the specific vulnerabilities they are designed to offset. These include operational and logistic measures, technical measures, administrative measures, and operations and military deception measures.

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, identity, 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 as to conceal the location and identity of combat units.

3. Technical Measures

    a. Limit non-secure computer e-mail messages to nonmilitary activities. Do not provide operational information in non-secure e-mail messages.

    b. Prepare for computer network attack by ensuring patches are installed in a timely manner, data is backed up to devices not connected to the network, and redundant communication means and procedures are in place.

    c. Use encryption to protect voice, data, and video communications.

Enclosure (5)

d. Use radio communications emission control, low-probability-of-intercept techniques and systems, traffic flow security, secure phones, landlines, and couriers.

e. Maintain sound silence or operate at reduced power, proceed at slow speeds, turn off selected equipment.

4. <u>Administrative Measures</u>

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

b. Conceal budgetary transactions, supply requests 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 and that their families are sensitized to a potentially abrupt departure.

g. Limit non-secure telephone conversation with non-military activities.

h. Provide family OPSEC briefs to inform family members of the need for OPSEC.

i. Ensure personnel are aware of OPSEC vulnerabilities presented by online social networking and avoid posting information about changes in personal or unit routines that could indicate operational planning or other details. Operational details in online forums both during and after a deployment should also be carefully avoided so as not to put

personnel in current or future rotations or operations at risk.

j.   Ensure adequate policies and procedures are in place for shredding documents.

5.   Web Risk Assessment

a.   Ensure personnel understand the do's and don'ts of posting information on social network sites.

b.   Ensure personnel are aware of the privacy settings of their social network sites.

c.   Ensure administrators of the unit's public facing website is properly trained on public release and web risk assessment.

d.   Ensure administrators of the unit's public facing website are conducting periodic website assessments for critical information, photos with critical information, and postings that may contain critical information.

6.   Military Deception (MILDEC) in Support of OPSEC

a.   OPSEC used in conjunction with MILDEC can assist commanders in protecting key elements of operations and facilitate mission success. OPSEC, with MILDEC, can be used to:

(1) Cause adversary intelligence to fail to target friendly activity; collect against tests, operations, exercises, or other activities; or determine through analysis vital capabilities and characteristics of systems and vital aspects of policies, procedures, doctrine, and tactics.

(2) Create confusion about, or multiple interpretations of, vital information obtainable from open sources.

(3) Cause a loss of interest by foreign and random observers in test, operation, exercise, or other activity.

b. In accordance with Department of Defense (DoD) policy, commanders are authorized to conduct MILDEC, to support OPSEC during the preparation and execution phases of normal operations, training, exercises, and day to day activities provided that prior coordination is accomplished for actions that will affect other commanders.

OPSEC Assessment

1. <u>General</u>. 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 OPSEC Assessment verifies the effectiveness of countermeasures a unit or organization uses to protect its critical information. The assessment will determine if critical information identified during the OPSEC planning process is being protected. The results of assessments are considered Critical Information. If the results need to be sent to anyone via e-mail, they must be transmitted via encrypted e-mail only.

2. <u>Requirement</u>

   a. Each command, battalion/squadron level or higher should conduct an annual self-assessment but will, at a minimum, conduct an annual review using the current IGMC OPSEC Functional Area Checklist 3070.

   b. Any command may request a formal assessment from the Regional OPSEC Program Manager after completing an internal assessment.

3. <u>Two Types of Assessments</u>

   a. <u>Command Assessment</u>. Concentrates on events within the command and is normally performed using personnel assigned to the command being assessed. The majority of assessments will be this type, though 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 where functions are routinely evaluated over a period of time.

   b. <u>Formal Assessment</u>. A formal assessment is conducted by members from outside the command, normally by the MOST, or the MCIEAST Regional OPSEC Program Manager. A formal assessment can also be requested from the Naval OPSEC Support Team (NOST) or the Interagency OPSEC Support Staff (IOSS). The formal assessment will often cross command lines and need to be coordinated appropriately. Formal assessments are

Enclosure (6)

normally directed by HHQ, but may be requested by subordinate commands. These formal assessments are typically large scale endeavors requiring larger than usual numbers of personnel and lead times in excess of two months. Per references (b) and (f), MCIEAST subordinate commands may have an OPSEC Assessment conducted by the MCIEAST Regional OPSEC Program Manager. Each MCIEAST Installation and Headquarters and Support Battalion will have a formal OPSEC Assessment conducted triennially by the MOST.

Notional OPSEC Plan

Although OPSEC Plans are used in Operational Plans for tactical training exercises and combat operations, for installations, they may be less formal, but are still required as part of training exercise plans for AT/FP, Anti-Terrorism, Emergency Management, etc., regardless of the plan format.

Notional OPSEC Plan

(CLASSIFICATION)
Command Name
Command Address

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

( ) References:

    a.   MCIEAST-MCB CAMLEJO 3070.1A
    b.   Other references as needed

1. ( ) <u>Situation</u>. 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, stand-alone document.

    a.   ( ) <u>Adversary Forces</u>

        (1) ( ) <u>Current Adversary Intelligence Assessment</u>. State the estimated adversary's assessment of friendly operations, capabilities, and intentions. Specifically address any known adversary knowledge of the friendly operation covered in the basic plan.

        (2) ( ) <u>Adversary Intelligence Capabilities</u>. State the adversary's intelligence collection capabilities according to major categories (SIGINT, HUMINT, and so forth). Address all potential sources to include the capabilities of any non-belligerents, who may provide support to the adversary. Describe how the adversary's intelligence system works to include the time required for intelligence to reach key

decision makers. Identify major analytical organizations and key personalities. Discuss unofficial intelligence organizations, if any, that support the leadership. Identify strengths and weaknesses.

    b. ( ) <u>Friendly Forces</u>

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

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

    c. ( ) <u>Assumptions</u>. Identify any assumptions unique to OPSEC planning.

2. ( ) <u>Mission</u>. Provide a clear and concise statement of the OPSEC mission.

3. ( ) <u>Execution</u>

    a. ( ) <u>Concept of Operations</u>. Describe the general concept to implement OPSEC countermeasures; give it by phase and major activity (maneuver, logistics, communications, and so forth), if appropriate. Address OPSEC support to other elements of the Information Operations Plan, if applicable.

    b. ( ) <u>Tasks</u>. Identify specific OPSEC countermeasures 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. ( ) <u>Coordinating Instructions</u>. Identify requirements to coordinate OPSEC countermeasures 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.

d. ( ) <u>Feedback</u>. Describe the concept for monitoring the effectiveness of OPSEC countermeasures during execution. Identify specific intelligence requirements for feedback.

e. ( ) <u>OPSEC Assessments</u>. Address any plans for conducting OPSEC assessments in support of the basic plan.

f. ( ) <u>After-Action Reports</u>. Identify any requirements for after-action reporting.

4. ( ) <u>Administration and Logistics</u>. Give special OPSEC related administrative or logistical support requirements.

5. ( ) <u>Command and Control</u>

a. ( ) <u>Command Relationships</u>

(1) ( ) <u>Approval</u>. State approval authority for execution and termination.

(2) ( ) <u>Authority</u>. Designate supported and supporting commanders as well as agencies, as applicable.

(3) ( ) <u>Oversight</u>. Detail oversight responsibilities, particularly for measures by nonorganic units or organizations outside the chain of command.

b. ( ) <u>Command, Control, Communications and Computer Systems</u>. Address any special or unusual OPSEC-related communications system requirements. List all communications system-related OPSEC countermeasures in subparagraph 3b.

CLASSIFIED BY:
DECLASSIFY

Contract, Acquisition, and Procurement Requirements

1. Introduction

    a. OPSEC shall be incorporated into all acquisition and procurement programs, processes, and contracts. All military and civilian contracting personnel, contracting companies, defense contractors, and vendor personnel providing services or products aboard MCIEAST installations are responsible for safeguarding Sensitive and Critical Information under their control or within their authorized work area and shall abide by DoD and DON OPSEC requirements in reference (c). The extent of protection afforded this information should be sufficient to reasonably prevent the possibility of its loss, compromise, inadvertent or unauthorized disclosure, or modification.

    b. Commanders and Department Head shall ensure that contractors supporting Marine Corps commands use OPSEC to protect critical information for specified contracts and subcontracts. The MCIEAST organization, their Government Contracting Activity (GCA), (usually the RCO), and the Regional OPSEC Program Manager, shall ensure appropriate OPSEC instructions and countermeasures are included as contractual requirements.

    c. It is the GCA responsibility to:

        (1) Determine what OPSEC countermeasures are essential to protect critical information for specific contracts.

        (2) Identify OPSEC countermeasures in their Business Requirements Documents or Functional Requirements Documents.

        (3) Ensure the GCA identifies OPSEC countermeasures and requirements in the resulting solicitations and contracts.

2. Procedures. Commands shall establish procedures to ensure that contract requirements properly reflect OPSEC responsibilities and that those responsibilities are included in both classified and unclassified contracts. To accomplish this, each document requiring service, parts, equipment, etc. shall have with it a signed statement that the unit's OPSEC Program Manager or OPSEC Coordinator has conducted an OPSEC

Review. This statement will identify the unit OPSEC Program Manager or OPSEC Coordinator who conducted the review. The RCO OPSEC Coordinator will also sign that statement ensuring that the sending command conducted the review. The Regional OPSEC Program Manager will conduct periodic reviews to ensure compliance.

a. Commands must determine if there is critical information associated with the contract or activities involved in the contract that warrants the inclusion of OPSEC requirements. Consideration shall be given to the type of work being performed and the location, environment, and circumstances in which contract performance will occur. In some cases, contractors may simply be required to receive threat awareness briefings or basic security training for employees.

b. OPSEC reviews shall be conducted on the Statement of Work (SOW) and any requirements document for classified and unclassified contracts prior to the time the GCA releases the SOW to contract bidders. The SOW is a publicly released document that can reveal critical information or indicators of critical information.

c. OPSEC requirements must be included in the contract solicitation and resulting contract in sufficient detail to ensure complete contractor understanding of all OPSEC required provisions. OPSEC requirements levied on contractors may include, but are not limited to:

(1) Specific OPSEC countermeasures the contractor is required to follow.

(2) Specific OPSEC awareness training.

(3) Participation in the command or unit OPSEC program.

(4) Development of an OPSEC program with specific features based on command or unit approved OPSEC requirements.

d. For classified contracts, the Marine Corps command or unit, and GCA will specify OPSEC requirements on DD Form 254, Department of Defense Contract Security Classification

Specification. OPSEC requirements apply to National Industrial Security Program (NISP) contractors when it is determined that additional safeguards are essential for specific contracts; they are imposed in addition to the standard requirements of the NISP.

(1) The command or unit requesting action by the RCO or other contracting, acquisition and procurement, or vendor requests will state OPSEC requirements on the DD Form 254 in sufficient detail to ensure complete contractor understanding of the exact OPSEC provisions or countermeasures required. Full disclosure of these requirements is essential so that contractors can comply with and charge attendant costs to the specific contracts for which these measures have been directed. The failure of commands to conduct an OPSEC Review of these requests risks a delay in processing by the RCO until the document(s) is OPSEC compliant.

(2) If the Marine Corps command or unit requires the contractor to adhere to the command or unit OPSEC requirements, the DD Form 254 must have OPSEC checked as a requirement. The contractor must also be provided with a copy of the command or unit OPSEC requirements or plan.

(3) Marine Corps commands and units shall ensure contractors do not disclose classified or unclassified information pertaining to a contract to the public without prior review and clearance as specified in the requirements in block 12 of the DD Form 254.

(4) Marine Corps commands and units shall assist the Defense Security Service (DSS) in ensuring adequacy of industrial security efforts for OPSEC applied to classified contracts in accordance with reference (j).

3. DD FORM 254 Contract Security Classification Specifications

a. Classified contracts and contracts dealing with classified information require the completion of a DD Form 254. The DD Form 254 serves to further alert all parties to the contract's requirement for OPSEC countermeasures.

b.   For most contracts, item 11j of the DD Form 254 is marked "yes" to alert the reader to the fact that OPSEC requirements exist.   If item 11j is marked "yes", then box 14 of the form should contain local amplifying guidance for the contracting activity and the vendor such as the samples below:

(1) Compliance with security requirements imposed by documents generated in response to reference (k) and this Order is required.   Compliance with OPSEC countermeasures imposed by MCIEAST-MCB CAMLEJ OPSEC or by programs supported or by documents generated by RCO, may be necessary.   OPSEC program will be in accordance with references (a) and (d).   OPSEC plans shall be coordinated with and approved by the RCO OPSEC Coordinator or the MCIEAST Regional OPSEC Program Manager and shall also be imposed on subcontractors as appropriate.   Program protection measures shall be applied and approved by the Contracting Activity or Organization Program Protection Specialist at all locations where Critical Information is developed, produced, analyzed, maintained, transported, stored, tested, or used in training.

(2) The contractor shall research, develop and deliver an OPSEC plan in accordance with the DD Form 1423 (Contract Data Requirements List (CDRL)).

c.   In the case of procurements in support of a Special Access Program the following, or similar, text will also be inserted: 11 It may be necessary for OPSEC surveys and assessments to be conducted as a method to identify, define, and provide countermeasures to vulnerabilities in the performance of this contract in accordance with individual program requirements and/or DoD 5220.22-M-Sup 1, paragraph C11.4.   Specific guidance will be provided by [insert SAP POR]."

d.   All DD Forms 254, and applicable portions of the SOW referring to OPSEC, shall be provided to the MCIEAST Regional OPSEC Program Manager and the cognizant DSS Field Office and will be used by DSS in support of industrial security inspections.

OPSEC Continuity Book Format Example

Tab A: Table of Contents
Tab B: National Security Decision Directive 298
Tab C: DoD Directive 5205.02E Ch 1 & DoD Manual 5205.02-M
Tab D: SECNAVINST 3070.2_
Tab E: (your command) 3070
Tab F: (your higher headquarters command) 3070
Tab G: MCO 3070.2_
Tab H: OPSEC Policies (Commander's Accepted Risk, etc.)
Tab I: OPSEC Program Plan & OPSEC SOP
Tab J: Appointment Letters (OPM, OPC, OWG)
Tab K: OPSEC Working Group Membership Info
Tab L: OPSEC Working Group Meeting Minutes
Tab M: Threat Analysis
Tab N: Critical Information List, signed
Tab O: Vulnerability Analysis
Tab P: Risk Assessment
Tab Q: OPSEC Countermeasures
Tab R: Self-Assessment Reports/OPSEC Reviews
Tab S: OPSEC Training & Awareness Plan
Tab T: Unit Specific Training Briefs/Presentations
Tab U: Professional OPSEC Organizations memberships
        (e.g., OPSEC Professionals Society, etc.)
Tab V: OPSEC Library
Tab W: Points of Contact
Tab X: _____
Tab Y: _____
Tab Z: Miscellaneous

OPSEC Assessment Procedures

The steps listed below have been used at many DoD supporting establishments and forward deployed organizations with consistent, positive results. It is recommended that all the steps be read first to gain insight to the entire assessment process prior to its execution. Although no specific or unique training is required to conduct an OPSEC assessment, it is assumed that the organization's OPSEC Program Manager or Coordinator along with their working group members have completed basic OPSEC education and understand OPSEC fundamentals.

If training is required, OPSEC training sources are referenced in paragraph 4c of this Order. More information on training may be had by contacting the MCIEAST Regional OPSEC Program Manager.

Each step should be completed in the order listed.

1. Assemble the OWG to determine an appropriate execution timeline for this assessment. It is recommended the events include, but not restricted to:

    a. In-Brief - may be formal or informal.

    b. Threat Brief - what is the current threat(s) to the organization?

    c. Observations - is OPSEC practiced and what indicators are observed.

    d. Dumpster dives (don't forget office trash cans).

    e. Conduct OPSEC interviews with members of the organization to discover their understanding of, and practice of OPSEC.

    f. Web Risk Assessment - if they have a website or officially use social media.

    g. Command programmatic review using the OPSEC Functional Area Checklist 3070.

Enclosure (10)

h. Assessment wrap-up - may include an informal out-brief either written or oral, or a formal out-brief with the commander and staff

2. Prepare a timeline for a basic foundation of operations to support a plan of action. Due to in-briefs and out-briefs, personnel interviews, dumpster diving, and rooting around in office trash, a Letter of Instruction is recommended.

3. Present the commander with an in-brief prior to the assessment and obtain approval to proceed. The commander may have specific wishes with reference to the assessment and reporting of results as he/she may require stricter adherence to the command's Operations Security. Ensure everyone adheres to the Commander's wishes as this assessment is theirs.

4. If assisting and conducting an assessment outside of the chain of command, contact that commands Intelligence department (G-2 or S-2) or investigative organization, for installations, contact the service investigative branch (NCIS and/or CID) for a threat brief and an analysis of local threat intent and capabilities.

5. Assign team leads for designated portions of the assessment (trash review, interviews, observations, etc.).

6. Begin assessment in accordance with the event plan. Templates are available online and from the MCIEAST Regional OPSEC Program Manager and all can be edited to meet the organization's specifications. Add and or remove items as necessary.

7. Upon completion of the execution phase, and all information has been gathered, it is recommended the working group begin compiling a comprehensive report to present findings to the commander. It is recommended that a short Power Point brief reflecting these findings and recommendations for corrective action are presented.

For further assistance, contact the MCIEAST Regional OPSEC Program Manager, the MOST, the NOST, the IOSS, or the Joint OPSEC Support Staff (JOSE) - SIPR Only. All current contact information is easily found online.

CONTROLLED UNCLASSIFIED INFORMATION (CUI) // FOR OFFICIAL USE ONLY

SUBJECT: Operations Security (OPSEC) Review of Items for Public Release

1. Requestor

Name: _____

Title: _____

Installation: _____

Organization: _____

Phone Number: _____

Email: _____

2. Author: _____

3. Title of Material: _____

4. Information Type: _____

5. Geospatial Data (If Applicable): _____

Vector Geospatial Data:

Original or Derived Feature Type: _____

Feature Type Name: _____

Feature Type Definition: _____

Feature Attributes (Select "All" or Attach List

☐ All Associated Attributes

☐ Specify Attribute Name(s) or Attach List _____

Raster Geospatial Data:

Original or Derived Raster Product: _____

Raster Name: _____

Cartographic Product: _____

Title: _____

☐ Digital   ☐ Hardcopy   ☐ Both

Service Provider Name (e.g. ArcGIS Online) if geospatial data will be made available via web services:

_____

| MCIEAST - MCB CAMLEJ/G-3_5/PLANS/1 | (10/20) | PREVIOUS EDITIONS OBSOLETE | AEM DESIGNER |

CONTROLLED UNCLASSIFIED INFORMATION (CUI) // FOR OFFICIAL USE ONLY

6. Reason / Requirement for the public Release:

```

```

7. Requester must Check Yes or No after each question. Does this material contain:

a. Any classified Information? If yes, explain (page(s) and paragraph(s))

☐Yes ☐No _____

b. Any FOUO, Sensitive, or Controlled Unclassified Information (CUI)? If Yes, explain.

☐Yes ☐No _____

c. Information addressed in a Security Classification Guide? If Yes explain.

☐Yes ☐No _____

d. Information addressed in the latest Military Critical Technologies Listing or Critical Information List?

☐Yes ☐No

e. Any contract proposals, bids, or proprietary information that would prohibit release?

☐Yes ☐No

f. Any information on inventions/patent applications for which patent secrecy orders have been issued?

☐Yes ☐No

g. Any studies or reports containing advice, recommendations or vulnerabilities?

☐Yes ☐No

h. Any sensitive fielding/testing schedule information?

☐Yes ☐No

i. Information not published previously containing state-of-the-art, breakthrough or dual use technology?

☐Yes ☐No

j. Would release of this information allow development of countermeasures to the applicable system/technology?

☐Yes ☐No

k. Information protected by the Privacy Act such as SSN, DOB/POB, biography, photograph, etc

☐Yes ☐No

l. Does the US hold a significant lead in this technology that would be jeopardized by the release of this information?

☐Yes ☐No

m. Does this material reveal any security practices or procedures?

☐Yes ☐No

n. Would release of this information benefit a foreign entity, corporation or Government (militarily or economically)?

☐Yes ☐No

o. Information contrary to organizational OPSEC goals or on the Commander's CIL?

☐Yes ☐No

CONTROLLED UNCLASSIFIED INFORMATION (CUI) // FOR OFFICIAL USE ONLY

7. Requester must Check Yes or No after each question. Does this material contain: (cont)

p. Does this material contain sensitive information concerning an overall communication, electronics architecture of a tactical, strategic, or sustaining base application?

☐Yes ☐No

q. Does this information fall within the purview of your organization?

☐Yes ☐No

r. Is any information restricted from public dissemination by an international agreement?

☐Yes ☐No

8. I, the undersigned, am aware of the foreign intelligence interests in open source publications and in the subject matter of the information I have reviewed for OPSEC purposes. I certify that I have sufficient technical expertise in the subject matter of this date, paper, video, presentation, etc. and that, to the best of my knowledge, the net benefit of this public release outweigh the potential damage to the essential secrecy of all related USMC or other DoD programs of which I am aware. Based on my knowledge of this subject matter, the following required coordination is necessary (**Check all that apply**):

☐ Functional Data Set Lead   ☐ Critical Infrastructure Protection (CIP) Officer

☐ Command Security Officer   ☐ SJA / Legal Review Representative

☐ COMMSTRAT Office   ☐ Operations Security Officer / Coordinator

Additional Comments by the originating office / submitter:

I certify that I have reviewed this command's Critical Information List (CIL), and that the information contained within this document does not compromise, in any way, this command's classified or unclassified Critical Information, or information ab out critical infrastructure or, any other information that if released would be detrimental to this command, the Marine Corps, or the United States. A copy of this document shall be maintained by the originating office and an electronic copy of this completed form shall be sent via electronic mail to the organization's OPSEC practitioner.

Originating Office / Submitter

CONCURRENCES:

Functional Data Set Lead

Critical Infrastructure (CIP) Officer

Command Security Manager / Officer

Legal Reviewer

Operations Security Practitioner

COMMSTRAT Officer Representative