DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

MCO 3070.2A
PLI
02 JUL 2013

MARINE CORPS ORDER 3070.2A

From: Commandant of the Marine Corps
To: Distribution List

Subj: THE MARINE CORPS OPERATIONS SECURITY (OPSEC) PROGRAM

Ref: (a) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
(b) DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008
(c) ALMAR 007/04
(d) Joint Publication 3-13.3, "Operations Security," January 4, 2012
(e) MCWP 3-40.9
(f) SECNAVINST 5720.47B
(g) National Security Decision Directive (NSDD) 298, "National Operations Security Program," January 22, 1988
(h) SECDEF Information Security/Website Alert, DTG 090426Z AUG 06
(i) MARADMIN 365/10
(j) MARADMIN 181/10
(k) The Social Corps: The USMC Social Media Principles Handbook
(l) SECNAV M-5210.1

Encl: (1) The OPSEC Process
(2) Examples of Critical Information
(3) Examples of OPSEC Indicators
(4) Examples of OPSEC Countermeasures
(5) Notional OPSEC Plan
(6) OPSEC Assessments
(7) Functional Outlines and Profile Guidelines
(8) OPSEC Contract Requirements
(9) Inspector General Functional Area Checklist

Report Required: Annual Review of USMC Operations Security Program (Report Control Symbol DD-3070-01) External Report Control Symbol DD-Intel (A)2228), par. 4c(8) and encl (6)

1. Situation

a. References (a), (b) and (c) direct the Marine Corps to establish and maintain an Operations Security (OPSEC) program that promotes an understanding of OPSEC among all personnel. This Order provides policy, responsibilities, and procedures for OPSEC in the Marine Corps.

b. OPSEC shall be integrated into all day-to-day activities and operations that prepare, sustain, or employ Marine forces throughout the spectrum of warfare. The responsibility for OPSEC rests with leaders at all Marine Corps units or commands. OPSEC is not limited to operational units. All Marine units, activities, and commands have access to, and a responsibility to protect critical information.

c. OPSEC planning is accomplished through the five step OPSEC process. The process begins by identification of critical information. In dynamic situations, the steps may be revisited at any time to adjust to new threats or information. The five step process is:

(1) Identification of critical information

(2) Analysis of threats

(3) Analysis of vulnerabilities

(4) Assessment of risk

(5) Application of OPSEC countermeasures

d. A detailed explanation of the OPSEC process is contained in references (d) and (e) and enclosure (1). Additional information on critical information is contained in references (d) and (e) and enclosure (2). Additional information on OPSEC indicators is contained in references (d) and (e) and enclosure (3), and examples of OPSEC countermeasures are contained in references (d) and (e) and enclosure (4). Enclosures (2) through (5) are provided as examples only and should be altered to appropriately represent each command's specific OPSEC program.

e. Definitions

(1) Adversary. An individual, group, organization, or government that must be denied critical information.

(2) Adversary Intelligence Systems. Resources and methods available to and used by an adversary for the collection and exploitation of critical information or indicators thereof.

(3) OPSEC. A process of identifying unclassified critical information and subsequently analyzing friendly actions attendant to military operations and other activities (i.e., that prepare, sustain, or employ Marine forces during war, crisis, or peace) to:

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

(b) Determine indicators which adversary intelligence systems might obtain, that could be interpreted or pieced together to derive critical intelligence in time to be useful to adversaries.

(c) Select and execute OPSEC countermeasures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversarial exploitation.

(4) OPSEC Assessment. An evaluative process, conducted at least annually, of an organization, operation, activity, exercise, or support function to determine if sufficient OPSEC countermeasures are in place to protect from adversary intelligence exploitation. An OPSEC program assessment may include program reviews, Inspector General inspections, or higher headquarters assessments that specifically address OPSEC.

(5) OPSEC Coordinators. Personnel who have OPSEC duties as their responsibility on a part time basis.

(6) Countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity.

(7) OPSEC Countermeasures. Methods and means to gain and maintain essential secrecy about critical information.

(8) OPSEC Indicator. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

(9) OPSEC Program Manager/OPSEC Manager. Personnel who have OPSEC duties as their primary responsibility on a full time basis.

(10) Operations Support Element (OSE). An element responsible for all administrative, operations support and services support functions within the counterintelligence and human intelligence staff element of a joint force intelligence directorate.

(11) OPSEC Survey. A collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes.

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

(13) Critical Information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment.

(14) Essential Elements of Friendly Information (EEFI). Key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities necessary for adversaries to plan and act effectively against friendly mission accomplishment.

(15) Sensitive Information. Refers to unclassified information requiring special protection from disclosure that could cause compromise or threat to our national security, the Marine Corps, Marines, civilian Marines, DoD contractors, or family members.

2. Cancellation. MCO 3070.2.

3. Mission. Upon issuance of this Order, the Marine Corps Total Force develops and sustains an OPSEC program to protect critical information in order to prevent an adversary or potential adversary from obtaining specific facts about our intentions, capabilities, and activities.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) Purpose. Incorporate the OPSEC planning process into operations, exercises, activities, system development, and test and

evaluation in garrison and deployed environments as directed in reference (e).

(b) End State. A prudently formulated, practical, and timely systematic, Marine Corps-wide OPSEC program that includes organizational support, OPSEC training, assessments, and the development and incorporation of a critical information list.

(2) Concept of Operations. The Marine Corps will improve current OPSEC processes and promulgate them throughout the Marine Corps.

(a) Commanders will ensure their units appoint either an OPSEC Manager or Coordinator, develop OPSEC programs tailored to their commands, and utilize the OPSEC planning process.

(b) Commanders will communicate their OPSEC concerns with family members to reduce inadvertent disclosures, giving close attention to internet-based capabilities. Effective communication conduits are the commander's OPSEC Mangers/Coordinators, Anti-Terrorism Officers, Public Affairs Officers, and Family Readiness Officers.

(c) The Marine Corps Lessons Learned System shall be utilized in order to provide a repository for OPSEC lessons for use by all Marines.

b. Subordinate Element Missions

(1) Deputy Commandant, Plans, Policies and Operations (DC PP&O) shall:

(a) Establish and oversee the implementation of policies and procedures for the conduct of Marine Corps OPSEC.

(b) Serve as the lead office on OPSEC matters for the Marine Corps. Per reference (a), appoint a full-time OPSEC Program Manager to serve as the Service-level point of contact for all OPSEC matters.

(c) As required, coordinate OPSEC matters with the Joint Staff and other DOD and Interagency organizations.

(d) Submit the Annual United States Marine Corps (USMC) Operations Security (OPSEC) Report to Office of the Deputy Under Secretary of Defense for National Programs & Policy Support (NP&PS).

(e) Establish and maintain a USMC OPSEC working group (OWG) for the coordination and resolution of Marine Corps OPSEC issues.

(f) Designate an OPSEC manager who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this order.

(g) Director, Strategy and Plans Division (PL) shall:

(1) Coordinate with the Marine Corps Information Operations Center (MCIOC), the Navy Information Operations Center (NIOC) Norfolk or other appropriate commands to provide for OPSEC assessment, training and planning support to Marine Corps activities, installations, commands, units, and personnel.

(2) Coordinate with the Command, Control, Communications, and Computers (C4) Cyber Security Division for website content review and risk evaluation.

(3) Coordinate with the Division of Public Affairs (PA), Headquarters Marine Corps (HQMC), for policy guidance regarding official release of all command information to the public and the media.

(4) Assist in IGMC inspections as required. Provide OPSEC expertise to the Inspector General of the Marine Corps (IGMC) staff, for IG Functional Area (FA) 481. Update FA 481 checklist, as required.

(5) Appoint a HQMC OPSEC Program Manager to chair the OPSEC Working Group (OWG). The OWG will meet as required.

(6) Provide the H&S Bn OPSEC Manager/Coordinator with a copy of PP&O OPSEC plan.

(h) Commander, Marine Corps Information Operations Center (MCIOC) shall:

(1) Function as the Marine Corps OPSEC support element

(a) Provide operational and tactical level OPSEC expertise to all Marine Corps Forces (MARFOR), as required.

(b) Coordinate as needed with the NIOC Norfolk for OPSEC assessment, training and planning support to Marine Corps commands.

(C) Coordinate, in conjunction with Information Operations and Space Integration Branch (HQMC PP&O,PLI), at least annually, with Training and Education Command (TECOM) to ensure OPSEC training is incorporated into appropriate formal schools.

(d) Coordinate with TECOM, for the integration of OPSEC within training and exercises.

(2) Provide a permanent member to the OWG.

(3) Designate an OPSEC manager/coordinator, who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4b(17) of this Order.

(2) Director, Command, Control, Communications, and Computers (C4), shall:

(a) Ensure the Marine Corps Cyber Security Program supports the Marine Corps OPSEC program requirements.

(b) Coordinate C4 support to OPSEC assessments, as required.

(c) Continuously monitor Marine Corps websites for appropriate implementation of technical safeguards. Assist Marine Forces with the implementation of technical safeguards for websites that lack appropriate safeguards. Inform Marine Corps Network Operations Service Center (MCNOSC) of websites that violate technical standards or lack appropriate safeguards to enable further assessment of vulnerabilities.

(d) Provide a permanent member to the OWG.

(e) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this order.

(f) Provide the H&S Bn OPSEC manager/coordinator with a copy of C4's OPSEC plan.

(3) Director of Intelligence, (DIRINT) shall:

(a) Develop and disseminate policies regarding intelligence, to include counterintelligence.

(b) Provide a permanent member to the OWG.

(c) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this order.

(d) Provide the H&S Bn OPSEC manager/coordinator with a copy of Intelligence Department OPSEC plan.

(4) Director, Division of Public Affairs (PA) shall:

(a) In accordance with (IAW) SECNAVINST 5720.44C, ensure policy guidance regarding release of all information to the public and the media is coordinated with HQMC OPSEC Program Manager.

(b) Ensure that OPSEC is considered in the preparation of all public releases of information.

(c) Provide a permanent member to the OWG.

(d) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this Order.

(e) Provide the H&S Bn OPSEC manager/coordinator with a copy of PA's OPSEC plan.

(5) Inspector General of the Marine Corps (IGMC) shall:

(a) Ensure the OPSEC Functional Area is inspected at all commands as part of the Commanding General's Inspection Program.

(b) Provide a permanent member to the OWG.

(6) Headquarters and Service Battalion, HQMC (H&S BN) shall:

(a) Maintain copies of the OPSEC program plans for all HQMC divisions, to include Plans, Policies, and Operations (PP&O); Public Affairs (PA); Command, Control, Communications, and Computers (C4); Programs and Resources (P&R); Aviation (AVN); Installations and Logistics (I&L); Intelligence; Judge Advocate Division (JAD); Security Programs and Information Management Branch (ARS); Office of Counsel for the Commandant (CL); and Director, Marine Corps Staff (DMCS).

(b) Provide a permanent member to the OWG.

(c) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4b(17) of this Order.

(7) Director, Marine Corps Staff (DMCS) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4b(17) of this order.

(b) Provide a permanent member to the OWG.

(c) Provide the H&S Bn OPSEC manager/coordinator with a copy of DMCS' OPSEC plan.

(8) Commander, Marine Corps Systems Command (MARCORSYSCOM) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4b(17) of this Order.

(b) Ensure each separate Program Manager (PM) designates an OPSEC Coordinator to assist the MARCORSYSCOM OPSEC Manager in handling his or her separate PM/CO OPSEC issues.

(c) Confirm PMs/COs identify critical or sensitive information resident within their programs that should be protected and included on the command critical information list.

(d) Ensure program protection plans include OPSEC to protect critical information throughout the life cycle of Marine Corps acquisition systems and in all activities.

(e) Ensure all individuals who perform acquisition duties receive OPSEC training in support of program protection planning.

(f) Ensure Marine Corps contract requirements properly reflect OPSEC responsibilities and are included in contracts when applicable; see reference (b), enclosure (8) for additional information concerning contract requirements. Specifically ensure industrial partners implement OPSEC countermeasures when providing information to the public via websites and/or social media. When contacted by the Defense Security Service, support it in its role of ensuring contract industrial security efforts are adequate.

(g) Provide a permanent member to the OWG.

(9) Commanding General, Marine Corps Combat Development Command (CG MCCDC) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this Order.

(b) Establish guidelines for the integration of OPSEC into all activities to include capability demonstration plans, exercises, formal schools, Lessons Learned, and the Joint Staff's Lessons Learned Database.

(c) Develop and publish OPSEC concepts, studies, doctrine, and Tactics, Techniques & Procedures (TTP), as needed.

(d) Provide a permanent member to the OWG.

(10) Commanding General, Marine Corps Recruiting Command (CG MCRC) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this Order.

(b) Ensure that all Marine Corps recruiters consider OPSEC requirements when interfacing with the public.

(c) Provide a permanent member to the OWG.

(11) Deputy Commandant, Installations and Logistics (DC I&L) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this Order.

(b) Ensure information posted to DC I&L's public-facing websites does not, when taken in total, result in OPSEC vulnerabilities or security violations.

(c) Provide a permanent member to the OWG.

(d) Provide the H&S Bn OPSEC manager/coordinator with a copy of I&L's OPSEC plan.

(12) Deputy Commandant, Manpower and Reserve Affairs (DC M&RA) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this order.

(b) Provide a permanent member to the OWG.

(13) Deputy Commandant, Programs and Resources (DC P&R) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this Order.

(b) Provide a permanent member to the OWG.

(c) Provide the H&S Bn OPSEC manager/coordinator with a copy of P&R's OPSEC plan.

(14) Deputy Commandant, Aviation (DC AVN) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this Order.

(b) Provide a permanent member to the OWG.

(c) Provide the H&S Bn OPSEC manager/coordinator with a copy of AVN's OPSEC plan.

(15) Commanding Generals, Marine Corps Component Commands (All MARFORs) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4.b(17) of this Order.

(b) Maintain a POC listing for subordinate commands' OPSEC programs, updated at least semi-annually in October and March.

(c) Provide sufficient OPSEC support for subordinate units.

(d) Conduct an annual review of subordinate commands' OPSEC programs. The review will be the basis for a report which will be submitted to the Information Operations and Space Integration Branch (HQMC PP&O,PLI). The format and submission date for this report will be provided via separate correspondence, by HQMC PP&O,PLI in compliance with OUSD(I) guidance.

(e) Provide a permanent member to the OWG.

(f) Establish Command OPSEC teams as outlined in 4c(1)(a) of this Order.

(g) MARFORs receiving OPSEC support through regional COCOMs should follow the most restrictive regulations and measures.

(1) All training requirements will be carried out IAW with this Order.

(2) All annual reporting requirements will be carried out IAW this Order.

(16) Commander, Marine Corps Installation Command (MCICOM) shall:

(a) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed in paragraph 4b(17) of this Order.

(b) Ensure the OPSEC Functional Area is reviewed by inspection teams operating as part of the Commanding General's Inspection Program.

(c) Maintain a POC listing for subordinate commands' (MCI EAST/WEST/PAC and MCB Quantico) OPSEC programs, updated at least semi-annually in October and March.

(d) Provide sufficient OPSEC support to subordinate units.

(e) Conduct an annual review of the Regional MCI's and MCB Quantico's OPSEC programs. The review will be the basis for a report which will be submitted to the Information Operations and Space Integration Branch (HQMC PP&O, PLI). The format and submission date for this report will be provided via separate correspondence, by HQMC PP&O, PLI in compliance with OUSD(NP&PS) guidance.

(f) Provide permanent members to the OWG.

(g) Establish Command OPSEC Teams as outlined in 4c(1)(a) of this Order.

(17) All Commanding Generals and Commanding Officers (battalion/squadron and higher as well as base, station, activity and installation) shall:

Note. For purposes of this Order, an organization is at battalion/squadron or higher echelon when its head is a lieutenant colonel, a civilian grade GS-15, or a higher grade. This definition includes operating forces and the supporting establishment.

(a) Plan and implement OPSEC countermeasures to preserve essential secrecy in every phase of operations, exercises, tests, or activities that prepare, sustain, or employ Marine Forces.

(b) Designate an OPSEC manager/coordinator who will develop and implement an OPSEC program to fulfill the requirements listed below:

(1) Personnel appointed as the command OPSEC manager or coordinator should be familiar with all operational aspects of the command.

(2) Commanders at battalion/squadron level and higher shall appoint in writing an officer, staff non-commissioned officer, or equivalent Department of Defense civilian as the OPSEC manager or coordinator.

(a) Designate an OPSEC program manager or coordinator to fulfill their responsibilities.

(b) OPSEC program coordinators are encouraged but not required for units at or below the battalion/squadron level that are not geographically co-located with higher or that are assessed to have a high OPSEC risk.

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

(1) An OPSEC Order signed by the commanding officer.

(2) OPSEC training as outlined in paragraph 4c(3) of this Order.

(3) A Critical Information List (CIL).

(4) Sharing the CIL with the public affairs and family readiness officers and the Web Risk Assessment Cell (WRAC). If the CIL is classified, it will be provided only to personnel with the appropriate security clearance and access. OPSEC managers/coordinators will ensure the public affairs and family readiness officers receive current copies of their command's CIL in order to prevent inadvertent disclosure of this information via public affairs programs. The WRAC will use the CIL to monitor USMC websites for inadvertent disclosure of this information via public facing websites.

(5) Developing and executing OPSEC plans in support of operations and exercises in cooperation with the Anti-terrorism Officer, Physical Security Manager, Cyber Security, and the Intelligence Officer.

Reference (d) and enclosure (5) both contain examples of notional OPSEC plans.

(6) Ensuring contract requirements properly reflect OPSEC responsibilities and are included in contracts, when applicable. Specifically, ensuring industry partners take sufficient and appropriate action to protect sensitive government information throughout the contracting process. When contacted by the Defense Security Service (DSS), support them in their role of ensuring contract industrial security efforts are adequate.

(7) Ensuring all personnel posting information to official command web sites (to include command-sponsored social media) have completed OPSEC training per paragraph 4.c(3)(f) of this Order.

(8) Ensuring all official websites (to include command-sponsored social media) are reviewed quarterly by OPSEC-trained personnel to ensure they meet the OPSEC concerns listed in reference (f) and in paragraph 4.c(4) of this Order.

(9) Ensuring Public Affairs and Family Readiness Officers are trained in OPSEC as outlined in paragraph 4.c(3)(f) of this Order.

(10) Emphasize the importance of OPSEC with family members through pre-deployment training and at least semi-annual communication via official means.

(11) Each command will conduct assessments. Detailed information regarding assessments is contained in reference (d) and enclosures (6) and (7). At a minimum, every command will:

(a) Conduct an annual command level OPSEC assessment utilizing the Inspector General's Functional Area Checklist, enclosure (9).

(b) As per reference (a), establish an automated risk analysis tool that can be leveraged to facilitate the OPSEC process.

(d) Inspect the OPSEC Functional Area as part of the Commanding General's Inspection Program.

c. Coordinating Instructions

(1) OPSEC is an operations function. The operations officer is the staff advocate for OPSEC. The commander shall designate a staff officer to oversee OPSEC who is familiar with the operational aspects of the activity including the supporting intelligence, counterintelligence, and security countermeasures.

(a) Command OPSEC Teams. Effective OPSEC planning and execution requires input from all functional areas, therefore commands (battalion/squadron and higher) will create OPSEC teams with cross-command representation in order to achieve the requirements as listed in paragraph 4.b(17). OPSEC teams should, at a minimum, include representation from public affairs, family readiness, intelligence, operations, logistics, contracting, security, communications, and foreign disclosure. Additionally, attached and supporting elements and any joint and/or coalition forces should be included on the team.

(b) Commanders at the MARFORs, as well as MCCDC, MARCORSYSCOM, and MARCORLOGCOM, are highly encouraged to appoint a full-time OPSEC Program Manager vice a part-time coordinator.

(2) OPSEC is not a security, intelligence, or information assurance (IA) function.

(a) Security functions prevent unauthorized access to personnel, equipment, facilities, materials, and documents.

(b) Intelligence activities provide information on adversary forces, governments, and intentions. Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities. The Intelligence staff (G-2/S-2) is responsible for assisting commanders in planning, coordinating, and executing counterintelligence support during the drafting and reviewing of OPSEC plans. Commands without organic counterintelligence capability will coordinate with the Counterintelligence/Human Intelligence Officer at the next appropriate level of command for support.

(c) IA measures protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

(d) OPSEC and these activities often overlap and are mutually supportive. Close coordination must be maintained between all staff functions to ensure adequate OPSEC protection.

(3) Training Requirements

(a) Per references (a) and (g), all Commanding Generals and Commanding Officers shall establish an OPSEC program focused on training and education, and ensure that OPSEC awareness, training, and education are established and provided to OPSEC Program Managers or Coordinators.

(b) All courses are unit funded.

(c) All Marines, civilians, and contractors, who have authorized access to Marine Corps resources by virtue of employment or contractual relationship, will complete annual OPSEC training as outlined under 4.c(3)(g) and Table 1.

(d) All OPSEC program managers and coordinators must complete the OPSEC Fundamentals Course, OPSE 1301, within 30 days of appointment. The computer-based training DVD can be ordered by contacting the Naval Information Operations Center (NIOC) organizational mailbox, opsec@navy.mil. It can also be completed through the Interagency OPSEC Support Staff (IOSS) at http://www.ioss.gov/ listed under "Training." It is highly recommended to also attend the resident OPSEC Analysis Course (OPSE 2380). Registration is through IOSS listed under "Training."

(e) Command OPSEC program managers and coordinators at the Regimental/Group level and higher and supporting agencies/activities, to

include, but not limited to, HQMC, MCCDC, MARCORSYSCOM, MCWL, MARCORLOGCOM, MCRC, and MCIOC will also:

(1) Attend the Interagency OPSEC Support Staff (IOSS) OPSEC Analysis and Program Management resident course (OPSE 2500) or equivalent course, within 90 days of appointment.

(a) Registration for the OPSE 2500 course can be completed at http://www.ioss.gov/ or via email at ioss@radium.ncsc.mil.

(b) There will be a six month grace period to complete the IOSS OPSE 2500 course, following the publication date of this order.

(2) Current program managers and coordinators who have completed the Navy's OPSEC Course or the HQ Department of the Army's OPSEC Level II Course will have satisfied the requirements of 4.c(3)(c).

(f) Per reference (h), all command OPSEC managers and coordinators, public affairs officers, family readiness officers, webmasters, and any other personnel authorized to review information for public release via the internet, shall receive "web" OPSEC training.

(1) Training shall be completed within 90 days of appointment.

(2) Annual refresher training is required to maintain situational awareness of internet based capabilities and web based vulnerabilities.

(3) Training will be completed IAW Table 1.

(g) Annual OPSEC training requirements for command personnel are:

(1) A definition of OPSEC and its relationship to the command's security, intelligence and cyber security programs.

(2) An overview of the OPSEC process.

(3) OPSEC and social media.

(4) The command's current critical information list (CIL).

(a) To ensure command members do not inadvertently disclose critical information, an unclassified version of the CIL will be provided during annual training. The unclassified CIL may contain actual critical information and/or examples of notional types of critical information. Enclosure (2) provides examples of critical information which commanders can use for tailoring their training material.

(b) If the CIL is classified, it will be provided during annual training, but only to personnel with the appropriate security clearance and access.

(c) A portion of the annual training requirements can be completed through MarineNet at www.marinenet.usmc.mil, using training event code "AO" and course code "OPSECUS001" for Uncle Sam's OPSEC. To complete the requirement commands are required to provide a copy of the CIL and show

the command's OPSEC relationship to the security, intelligence and cyber security programs.

	Total Force to include CTR	Coord/Mgr	PAO	FRO	Webmasters
Annual OPSEC Training	Required	Required to provide 4c(3)(f)1 and 4c(3)(f)4 portion of annual training.	Required	Required	Required
OPSEC Fundamentals (IOSS 1301)	Optional	Required	Optional	Optional	Optional
OPSEC Analysis & Pgrm Mgmt (IOSS 2500)	Optional	Required for Reg/Group and Higher	Optional	Optional	Optional
OPSEC & Public Release Decisions (IOSS 1500)	Recommended	Required	Required	Required	Required
OPSEC & Web Risk Assessment (IOSS 3500)	Recommended	Required	Required	Required	Required

Table 1

(5) A listing of the command's personnel fulfilling OPSEC responsibilities will be maintained with the S-3 and made available upon request.

(h) All OPSEC program managers and coordinators will be compliant with the training requirements no later than six months from the publication date of this order.

(4) Unclassified Websites

(a) Unclassified, publicly available websites present a potential risk to personnel, resources, system development, and operations if inappropriate information is published on websites. OPSEC managers and coordinators will review their command's website to ensure there is no critical information published via text, graphics, or photographs. To obtain a website checklist, visit the NIOC Norfolk website at https://www.nioc-norfolk.navy.mil/. In addition, as directed in references (f), (i), (j), and (k) the following guidance is provided:

(1) Unclassified, publicly available websites shall not include classified material, "For Official Use Only" information, proprietary information, or information that could enable the recipient to infer this type of information. This includes, but is not limited to, lessons learned

or maps with specific locations of sensitive units, ship battle orders, threat condition profiles, activities or information relating to ongoing criminal investigations into terrorist acts, force protection levels, specific force protection measures being taken or number of personnel involved, Plans of the Day, or Plans of the Month, and RDT&E. When it is necessary to gain release authority from a senior in the chain of command, subordinate commands will submit material for clearance only after it has been reviewed and necessary amendments made to the fullest capability of the submitting command.

(2) Unclassified, publicly available websites shall not identify: family members of Department of the Navy personnel (military or civilian) in any way, except when cleared for release and published by authorized Public Affairs personnel; or the spouses of senior leadership who are participating in public events such as ship namings, commissionings, etc. Furthermore, family member information will not be included in any online biographies.

(3) Unclassified, publicly available websites shall not display personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers, or e-mail addresses which contain the individual's name. General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable. The names, telephone numbers, and personalized, official e-mail addresses of command/activity public affairs personnel and/or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories.

(4) Biographies of general officers, commanders, commanding officers, officers in command, executive officers or deputies, the civilian equivalents of those officers just listed, and Master Gunnery Sergeants or Sergeants Major may be posted to command unclassified, publicly available websites. However, biographies published on unclassified, publicly accessible websites will not include date of birth, current residential location, nor any information about family members.

(5) Reference (i) provides additional guidance for Marines who desire to make unofficial posts on the internet regarding Marine Corps related topics.

(6) Reference (j) authorizes official and limited personal use of internet-based capabilities via the Marine Corps enterprise network (MCEN). Access to internet-based capabilities, such as social media sites, from the MCEN presents a potential increase in OPSEC risk to the command. This increase in risk shall be mitigated through education, training and the promotion of awareness for the responsible and effective use of internet-based capabilities.

(7) Any further questions regarding website content should be forwarded to the MCIOC.

(5) Public Affairs. Through communication and engagement, public affairs plays a vital role in building understanding, trust and relationships with domestic, host-nation, and international publics critical to mission success. Therefore, public affairs personnel should be the first point of contact and must be included in the OPSEC planning process to ensure PA considerations are addressed and that critical information is safeguarded.

The need for OPSEC should not be used as an excuse to deny non-critical information to the public.

(6) Family Readiness. Commanders will discuss OPSEC concerns as part of their Family Readiness Program and stress the family's ability to contribute to the protection of the command's critical information. Family readiness officers, as a key component of the command team and the commander's military point of contact concerning unit family readiness issues, should be trained in OPSEC and social media, per Paragraph 4.c(3)(f).

(7) Inspections

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

(b) All units and activities at the regimental/group level and higher will conduct annual inspections of all subordinate commands using the FAC (enclosure 9).

(1) Inspectors must have attended the resident OPSEC training as prescribed in 4.c(3)(e) of this Order.

(2) Records of these inspections shall be retained for three years and will be an inspected item on the FAC. A copy of these inspections will also be provided to the inspected entity for their records. Inspected entities will retain a copy of the inspection for three years.

(c) All commands required to maintain an OPSEC program will conduct an internal inspection, utilizing the FAC, at least annually. During this annual inspection program, managers and coordinators shall review the command's critical information list, countermeasures, and threat statement for currency and relevance. Results from these inspections will be retained for three years and will be an inspected item on the FAC. Commands will normally utilize their own personnel to conduct an annual, command-level OPSEC assessment. Because formal assessments require support from organizations such as the Joint Information Operations Warfare Command or the Navy Information Operations Command, commands which desire a formal assessment will forward a request to Navy Information Operations Command Norfolk/CTF 1030 at opsec@navy.mil.

(8) Annual Reporting Requirement. Commanders will submit an annual calendar-year report, detailing their OPSEC program. Commanding Generals for the MARFORs, MARCORSYSCOM, MCCDC, MCRC, and other commands and activities, as directed by HQMC, will provide consolidated reports to HQMC. These consolidated reports will incorporate subordinate unit reports. Per reference (g), HQMC will submit a consolidated USMC report to the Office of the Deputy Under Secretary of Defense for National Programs & Policy Support (NP&PS). Guidance on the format and submission date for this report will be released via the Marine Corps Action Tracking System as it becomes available. Report Control Symbol DD-3070-01 (External Report Control Symbol DD-Intel(A) 2228) is assigned to this reporting requirement.

(9) Excessive OPSEC. Excessive OPSEC can degrade operational effectiveness by interfering with various day-to-day activities such as coordination, training, and logistical support. The commander must evaluate each activity and operation and then balance required OPSEC countermeasures

against operational needs. The OPSEC process will help commanders assess the risk and apply appropriate OPSEC countermeasures.

(10) Program Awareness and Training Product Promotion

(a) Active promotion of the OPSEC program is the responsibility of all levels of commands. All Commanding Generals, Commanding Officers, and installations are encouraged to develop their own OPSEC promotional materials and use all suitable techniques of publicity and promotion consistent with the law and within funds available.

(b) Appropriated funds may be used to buy items to promote 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 promotional ideas with the Total Force. Commands can share promotional products with MCIOC.

(c) As part of promotional efforts, commanders at all levels should:

(1) Advertise the OPSEC program through posters, billboards, inserts in bulletins, or other media which frequently reach Marines, civilians and contractors.

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

5. Administration and Logistics

a. Records created as a result of this Order shall be managed according to National Archives and Records Administration approved dispositions per reference (l) to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium.

b. Marine Corps Information Operations Center (MCIOC)

(1) Reference (a) directs each service to provide for an OPSEC support element.

(2) For the Marine Corps, this function is being provided by the MCIOC (http://www.marines.mil/unit/mcioc/Pages/index.aspx). Commands can receive additional assistance with OPSEC training support, advice for command-level OPSEC assessments and OPSEC aids such as posters. The MCIOC is the initial OPSEC POC for Marine Corps organizations. OPSEC matters that require higher level intervention will be coordinated with the PP&O OPSEC program manager via the MCIOC.

c. Naval OPSEC Support Team (NOST)

(1) The NOST can serve as an alternate support element.

(2) The NOST's Marine Liaison can be reached at (757) 417-7100.

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force. Contractors will implement OPSEC countermeasures as required by their contracts.

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

R. L. BAILEY
Deputy Commandant
Plans, Policies and Operations

DISTRIBUTION: PCN 10203112000

THE OPSEC PROCESS

1. The OPSEC Process involves five steps applied in a sequential order. In dynamic situations, these steps may be revisited at any time to adjust to new threats or information. These steps may or may not be used in sequential order but all elements must be present to conduct OPSEC analysis.

2. Step 1: Identification of Critical Information. Critical information is information about military activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources.

a. Essential elements of friendly information (EEFI). Critical information can be thought of as the answer to the EEFI; it is the information vitally needed by the adversary. This serves to focus the OPSEC Process on protecting the vital information, rather than attempting to protect all unclassified information. The EEFI is found in the OPLAN in Tab C to Appendix 3 to Annex C (Operations). This critical information will often times be similar to what you would want to know about the adversary.

b. Critical information that if obtained will either impact the success of the organizations or improve the likelihood of an adversary meeting their goals. For Example:

(1) **Military operations**: The adversary obtains information on the time and location of a planned attack. As a result, losing the element of surprise could lead to significant casualties.

(2) **Acquisition**: The adversary obtains information on a new missile in the development phase that cannot be detected by adversary capabilities. As a result, the adversary begins development of countermeasures to defeat the new technology.

(3) **Administration**: The adversary obtains information about force protection equipment being sent to a unit operating in theater. As a result, the adversary changes its tactics, techniques, and procedures to defeat the equipment.

c. From the examples listed above, there are many areas within a command where elements of critical information can be obtained. Working with or interviewing personnel in all areas of the command and even personnel not directly assigned may satisfy many portions of the command's critical information.

d. Once this list of critical information has been identified, it should be compiled in a Critical Information List, approved by the commander or director and disseminated so that a command's personnel know what information is critical and requires protection.

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

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

b. What are the adversary's intentions and goals? What does the adversary want to accomplish?

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

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

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

f. Who are the friendly intelligence and counterintelligence staffs, and will they provide or share this information?

4. Step 3: Analysis of Vulnerabilities. This action identifies an operation's or activity's vulnerabilities. This requires examining the parts of the planned operation and identifying OPSEC indicators that could reveal critical information. Vulnerabilities exist when the adversary is capable (with the available collection and processing assets) of observing an OPSEC indicator, correctly analyzing it, and then taking appropriate and timely action. Reviewing results of preparations (workups) to the operation such as computer simulations, war games, sand table exercises, field exercises, and command post exercises will help identify vulnerabilities not readily apparent. The commander will need answers to questions, so working continuously with intelligence personnel, the operations planners will gain answers to the following vulnerabilities questions:

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

b. What OPSEC indicators can the adversary actually collect?

c. What OPSEC indicators can the adversary actually use to our disadvantage? Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?

d. Will the application of OPSEC countermeasures introduce more indicators that the adversary will be able to collect?

5. Step 4: Assessment of Risk. This action has three components. First, **planners analyze the vulnerabilities** identified in the previous action and **identify possible OPSEC countermeasures** for each OPSEC vulnerability. Second, the commander and staff estimate the impact to operations such as cost in time, resources, personnel or interference with other operations associated with implementing each possible OPSEC countermeasure versus the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular OPSEC vulnerability. Third, the commander staff select **specific OPSEC countermeasures for execution** based upon a risk assessment done by the commander and staff. See reference (d).

a. OPSEC Countermeasures can be used to:

(1) Prevent the adversary from detecting an OPSEC indicator or exploiting vulnerabilities.

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

(3) Attack the adversary's intelligence collection system(s) directly.

b. Besides physical destruction, OPSEC countermeasures, among other actions, can include:

(1) Concealment and camouflage.

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

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

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

c. More than one OPSEC countermeasure may be identified for each OPSEC vulnerability; and one OPSEC countermeasure can be identified for multiple vulnerabilities. Primary and secondary OPSEC countermeasures can be identified for single or multiple OPSEC indicators. OPSEC countermeasures are most effective when they provide the maximum protection while minimally affecting operational effectiveness.

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

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

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

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

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

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

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

e. Planning for OPSEC countermeasures requires coordination amongst all staff elements, and supporting elements or assets outside the command. Particular care must be taken to ensure that OPSEC countermeasures do not interfere with other operations (e.g., deception plans, psychological

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

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

a. A general OPSEC countermeasure strategy should be:

(1) Minimize predictability from previous operations.

(2) Determine detection indicators and protect them by elimination, control, or deception.

(3) Conceal indicators of key capabilities and potential objectives.

(4) Counter the inherent vulnerabilities in the executive of mission processes and the technologies used to support them.

b. The adversary reaction to our OPSEC countermeasures will be monitored to determine effectiveness. Provisions and methods for feedback from combat units, intelligence and counterintelligence staffs, and other IO elements, will have to be planned for in the OPLAN. This feedback will help determine the following:

(1) Is the OPSEC countermeasure producing the desired effect or is it producing an undesired effect?

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

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

(4) Do we need to cease the OPSEC countermeasure because are no observable results, or there have been negative or unintended consequences?

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

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

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

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

c. During the execution of OPSEC countermeasures, OPSEC personnel should establish measures of effectiveness (MOEs) and measures of performance (MOPs) to assess if their OPSEC analysis is correct.

(1) MOE. **The adversary's reaction is monitored to determine the countermeasures' effectiveness and to provide feedback.** As it has been indicated above, implementing OPSEC countermeasures should not reveal additional critical information. As a corollary to that, if an OPSEC countermeasure is identified by the adversary, then that may be enough to alert the adversary that a military operation is imminent.

(2) MOP. Provides OPSEC personnel a way to determine if OPSEC countermeasures are being properly implemented.

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

e. The OPSEC Assessment is an excellent method and tool for providing feedback on the effectiveness of OPSEC 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. The below lists are not "cookie cutter" lists which can be applied to all situations, nor are they an all-encompassing checklist which can be robotically applied to all situations. Commanders and their staffs will use their judgment and experience and develop critical information unique to their mission.

2. Political and Military Crisis Management.

   a. Target selection and deployment destinations.

   b. Timing considerations.

   c. Logistical capabilities and limitations.

   d. Alert posture, Defense Condition, and response time.

3. Mobilization.

   a. Intent to mobilize before public announcement.

   b. Impact on military industrial base.

   c. Impact on civilian economy.

   d. Transportation capabilities and limitations.

4. Military Intervention.

   a. Intentions.

   b. Military capabilities.

   c. Strategy and tactics.

   d. Forces assigned and in reserve.

   e. Targets.

   f. Time considerations.

   g. Routes for combat units, support units, and resupply.

   h. Logistic capabilities and constraints.

   i. Third-nation or host-nation arrangements.

5. Open Hostilities.

   a. Force composition, disposition.

   b. Attrition and reinforcement.

c. Targets.

d. Time considerations.

e. Logistics capabilities and constraint.

6. Intelligence, Reconnaissance, and Surveillance.

a. Purpose of collection efforts.

b. Targets of collection.

c. Time considerations.

d. Types of and capabilities of collection assets.

e. Processing capabilities.

f. Units requesting intelligence data.

7. Peacetime Weapons and other Military Movements.

a. Fact of movement.

b. Origin and destination of units, personnel, and equipment being moved.

c. Capabilities of units, personnel, and equipment being moved.

d. Inventory of equipment being moved.

8. Command Post and Field Training Exercises.

a. Participating units.

b. OPLAN or other contingencies that are being exercised.

c. Command relationships.

d. Command, control, communications, and computer connections and weaknesses.

e. Logistics capabilities and weaknesses.

9. Noncombatant Evacuation Operations.

a. Targets.

b. Forces involved.

c. Logistic capabilities and constraints.

d. Safe havens or staging areas.

e. Routes.

f. Time considerations.

10. Counterdrug Operations.

a. Military forces involved.

b. Law enforcement agencies (LEAs) involved.

c. Military support to LEAs.

d. Host-Nation cooperation or involvement.

e. Capabilities of military forces/LEAs.

f. Time considerations.

g. Tactics to be used.

h. Logistics capabilities and constraints.

11. Counterterrorism Operations.

a. Forces.

b. Contingency plans.

c. Standing SOP.

d. Targets.

e. Time considerations.

f. Staging or basing locations.

g. Tactics.

h. Ingress and egress methods.

i. Logistics capabilities and constraints.

EXAMPLES OF OPSEC INDICATORS

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

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

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

(1) An indicator's signature stability implies constant or stereotyped behavior that allows an enemy to anticipate future actions. Reducing the uniqueness or stability of the indicator's signature increases the ambiguity of the 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. Associations. Association is the relationship of an indicator to other information or activities. Intelligence analysts compare their current observations with what has been seen in the past to identify possible relationships.

(1) Using the previous example, the intelligence analyst knows that the GSE is used for fixed-wing transport aircraft. The analyst also knows that the length and composition of the landing strip will only support transport aircraft as large as a C-130. Additionally, Marine Corps forces are the only units that have used this field in the last two years. An analyst would likely take the GSE indicator and associate it with the previous information, and conclude that KC-130s are operating in the area.

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

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

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

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

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

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

e. Exposure. Exposure refers to when and for how long an indicator is observed. The duration, repetition, and timing of an 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.

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

3. The following provides examples of indicators that are associated with military 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, acquisition programs, or activities.

a. Indicators of general military capabilities:

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

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

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

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

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

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

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

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

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

b. Indicators of general command and control capabilities:

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

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

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

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

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

consultations that occur with higher commands, and the types of actions initiated afterward.

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

(7) Using social media either personally or through the command, broadcasting movements, capabilities, locations, personnel, etc.

c. Indicators from communications:

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

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

(3) Increasing, decreasing, or ceasing (radio silence) radio transmission when close to starting an operation, exercise, or test. Again, without conditioning 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) Using stereotyped message characteristics that indicate particular types of activity allowing adversary's to monitor and evaluate friendly activity.

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

d. Indicators for equipment and systems:

(1) Unencrypted emissions during tests and exercises.

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

(3) The equipment or system hardware itself.

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

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

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

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

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

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

(10) Use of advertisements that a company has a contract on a classified system, or component of a system, possesses technology of military significance, or has applied particular principles of physics and special technologies to sensors and the guidance components of weapons.

(11) Public media, particularly technical journals.

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

(1) Provisioning of special supplies for participating elements.

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

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

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

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

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

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

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

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

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

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

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

(16) Imposing unusual off-limits restrictions.

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

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

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

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

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

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

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

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

(25) Setting up wide area network (WAN) over commercial lines.

f. Indicators during the execution phase:

(1) Unit and equipment departures from base.

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

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

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

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

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

(7) Alert of civilians in operational areas.

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

(9) Changes in oceanographic high frequency transmission.

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

g. Indicators of post-engagement operations or residual capabilities:

(1) Repair and maintenance facility schedules.

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

(3) Movement of supporting maintenance resources.

(4) Unusual medical activity.

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

(6) Assignment of new units to an area.

(7) Search and rescue activity.

(8) Personnel orders or reassignment.

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

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

h. Indicators from internet-based capabilities

(1) Posting sensitive mission related information on social networking sit.

(2) Posting unit rosters.

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

(4) Not turning off geo-tagging when taking photos in operational 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.

(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 (PII), For Official Use Only (FOUO), and/or Sensitive But Unclassified (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 (Foursquare, Gowalla, Color, and Shopkick).

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.

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

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

g. Use darkness to mask deployments or force buildup.

h. Approach an objective "out of the sun" to prevent detection.

i. Physical Attack and Electronic Warfare. During hostilities, use physical destruction and electronic attack against the adversary's ability to collect and process information. Military actions that are used in support of OPSEC include strikes against an adversary's satellites, SIGINT sites, radars, fixed sonar installations, reconnaissance aircraft, and ships. For more information, see JP 3-13.1, *Electronic Warfare*, and JP 3-60, *Joint Targeting*.

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.

d. Use radio communications emission control, low-probability-of-intercept techniques and systems, traffic flow security, padding, flashing light or flag hoist, ultra-high frequency relay via aircraft, burst

transmission technologies, secure phones, landlines, and couriers. Limit use of high-frequency radios and directional super-high-frequency transponders.

e. Control radar emission, operate at reduced power, operate radars common to many units, assign radar guard to units detached from formations or to air early warning aircraft, and use anechoic coatings.

f. Mask emissions or forces from radar or visual detection by use of terrain (such as mountains and islands).

g. Maintain sound silence or operate at reduced power, proceed at slow speeds, turn off selected equipment, and use anechoic coatings.

h. Use screen jamming, camouflage, smoke, background noise, added sources of heat or light, paint, or weather.

4. Administrative Measures:

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 is conducting periodic website assessments for critical information, photos with critical information, and postings that may contain critical information.

6. Military Deception 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 targeted 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.

(4) Convey inaccurate locating and targeting information to opposing forces.

b. In accordance with DoD policy, commanders are authorized to conduct MILDEC:

(1) To support OPSEC during the preparation and execution phases of normal operations, provided that prior coordination is accomplished for actions that will affect other commanders.

(2) When the commander's forces are engaged or are subject to imminent attack.

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

NOTIONAL OPSEC PLAN

(CLASSIFICATION)

Command Name
Command Address

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

( ) References:

a. MCO 3070.2A
b. Other references as needed

1. ( ) Situation. Refer to other annexes and paragraphs in the basic plan as much as possible to avoid duplication. When publishing the OPSEC annex separately from the basic order, however, it is necessary to copy the information here in detail that allows the OPSEC annex to be a useful, stand-alone document.

a. ( ) Enemy Forces

(1) ( ) Current Adversary Intelligence Assessment. 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) ( ) Adversary Intelligence Capabilities. 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. ( ) Friendly Forces

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

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

c. ( ) Assumptions. Identify any assumptions unique to OPSEC planning.

2. ( ) Mission. Provide a clear and concise statement of the OPSEC mission.

3. ( ) Execution

a. ( ) Concept of Operations. Describe the general concept to implement OPSEC 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. ( ) Tasks. 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. ( ) Coordinating Instructions. 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. ( ) Feedback. Describe the concept for monitoring the effectiveness of OPSEC countermeasures during execution. Identify specific intelligence requirements for feedback.

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

f. ( ) After-Action Reports. Identify any requirements for after-action reporting.

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

5. ( ) Command and Control

a. ( ) Command relationships

(1) ( ) Approval. State approval authority for execution and termination.

(2) ( ) Authority. Designate supported and supporting commanders as well as agencies, as applicable.

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

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

CLASSIFIED BY:
DECLASSIFY

OPSEC ASSESSMENTS

1. Assessments and Surveys

a. **General.** An OPSEC assessment is an intensive application of the OPSEC process to an existing operation or activity. Assessments are essential for identifying requirements for additional OPSEC countermeasures and for making necessary changes to existing plans. An OPSEC assessment is a good tool to validate OPSEC programs and organizational practices to protect critical information in operations and activities. In addition to using organic assets to conduct assessments, Commanding Officers can seek the support of external resources. An OPSEC survey is conducted by a team of external subject matter experts from multiple disciplines to simulate adversary intelligence processes.

b. **Purpose.** The purpose of an OPSEC assessment is to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists. Ideally, the operation or activity being assessed uses OPSEC countermeasures to protect its critical information. The OPSEC assessment is used to verify the effectiveness of OPSEC countermeasures. This assessment will determine if critical information identified during the OPSEC planning process is being protected. An assessment cannot be conducted until after an operation or activity has at least identified its critical information. Without a basis of critical information, there can be no specific determination that actual OPSEC vulnerabilities exist. The purpose of an OPSEC survey is to focus on the organization's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post execution phases of any operation or program.

c. **Uniqueness**

(1) Each OPSEC assessment is unique. Assessments differ in the nature of the information requiring protection, the adversary collection capability, and the environment of the operation or activity to be assessed.

(2) In combat, an assessment's emphasis should be on identifying vulnerabilities and indicators that signal friendly intentions, capabilities, and limitations and that permit the adversary to counter friendly operations or reduce their effectiveness.

(3) During non-combat operations, to include routine steady-state activities, assessments generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests, drills, practice alerts, and major exercises, are of great interest to a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and command and control (C2) capabilities that enhance that adversary's planning.

d. **Operations Security Assessments Versus Security Inspections**

(1) OPSEC assessments are different from security evaluations or inspections. An assessment attempts to produce an adversary's view of the operation or activity being assessed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

(2) Assessments are always planned and conducted by the organization responsible for the operation or activity that is to be assessed. Inspections may be conducted without warning by outside organizations.

(3) OPSEC assessments are not a check on the effectiveness of an organization's security programs or its adherence to security directives. In fact, assessment teams will seek to determine if any security measures are creating OPSEC indicators.

(4) Assessments are not punitive inspections, and no grades or evaluations are awarded as a result of them. Assessments are not designed to inspect individuals, but are employed to evaluate operations and systems used to accomplish missions.

(5) To obtain accurate information, an assessment team should try to create an environment that promotes positive cooperation and assistance from the organizations participating in the operation or activity being assessed. If team members must question individuals, observe activities, and otherwise gather data during the course of the assessment, they will inevitably appear as inspectors, unless this non-punitive objective is made clear.

(6) Although reports are not provided to the assessed unit's higher headquarters, OPSEC assessment teams may forward to senior officials the lessons learned on a non-attribution basis. The senior officials responsible for the operation or activity then decide to further disseminate the assessment's lessons learned.

(7) Lessons learned from the assessment should be shared with command personnel in order to improve the command's OPSEC posture and mission effectiveness.

e. **Assessments and Surveys**

(1) **OPSEC Assessment.** OPSEC assessments are conducted annually to evaluate an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence collection systems. An OPSEC assessment is normally run by the OPSEC program manager and performed by the unit's OPSEC working group. An assessment may be conducted with a small team of individuals from within an organization with or without assistance from subject matter experts. The scope of an OPSEC assessment is usually limited to events and activities within that organization.

(2) **OPSEC Survey.** A survey usually requires a team of external subject matter experts from multiple disciplines to simulate adversary intelligence processes. An OPSEC survey should focus on the organization's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post execution phases of any operation or program. These surveys may include telecommunications monitoring, radio frequency monitoring, network and computer systems assessment, and open-source collection. Survey teams should use collection techniques of known adversaries. A survey is required every three years. See Figure IV-1 of DoD 5205.2M for an assessment-survey comparison.

(3) **Requirements for Assessments and Surveys**

(a) At a minimum, each command will conduct an annual command assessment using the Inspector General's Functional Area Checklist.

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

2. Assessment Planning

a. **Introduction.** The required lead time to prepare for an assessment depends on the nature and complexity of the operation and activities assessed (combat operations, peacetime operational activity, or other type of operation). Allot sufficient time in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions, and for careful preparation of functional outlines. The following actions normally make up the planning phase:

b. **Determine the Scope of the Assessment.** The scope of the assessment is defined at the start of the planning phase and is limited to manageable proportions. Limitations are imposed by geography, time, units to be observed, funding, and other practical matters. There are two types of assessments: Command and Formal.

(1) A command assessment concentrates on events within the command and is normally performed by using only personnel assigned to the command being reviewed. The majority of USMC assessments will be this type of assessment. The scope of these assessments can vary depending on the commander's guidance. Recognizing that an all-encompassing assessment would levy a high burden on a typical command, commanders are encouraged to develop an approach in which functions are routinely evaluated, but done over a period of time. For example, a commander could evaluate administrative OPSEC during one field exercise, while evaluating website OPSEC on the next exercise. See **Enclosure (7) for examples of functional outlines and profile guidelines for assessments.**

(a) 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.

(b) The following areas could be evaluated: Intelligence Collection Operations; Logistics; Communications; Operations; and Administration and Support.

(2) A formal assessment is composed of and conducted by members from within and outside the command. The formal assessment will often cross command lines and needs to be coordinated appropriately. Formal assessments are normally directed by higher headquarters to subordinate echelons, but may be requested by subordinate commands.

c. **Select Team Members**

(1) Regardless of the assessment's external or internal focus, the team should contain multi-disciplined expertise. Assessment team members

should be selected for their analytical, observational, and problem-solving abilities.

(2) Since assessments are normally oriented to operations, the senior member should be selected from the operations (or equivalent) staff of the commander responsible for conducting the assessment.

(3) Typical team members would represent the functional areas of intelligence (to include CI), security, communications, logistics, plans, IA, PA, contracting, acquisition, and administration. When appropriate, specialists from other functional areas, such as transportation, will participate, and other entities as needed (e.g., engineering and supply) to ensure an adequate breadth of expertise. Team members are brought together early in the planning phase to ensure timely, thorough accomplishment of the tasks outlined below.

d. **Become Familiar with Assessment Procedures.** Designating team members with assessment experience is advantageous, but is often not possible. In such cases, team members will require familiarization with assessment procedures. This will help team members develop a functional outline for the aspect of the operation they are responsible to survey. Refer to DOD 5205.02-M, *DOD Operations Security (OPSEC) Program Manual,* Enclosure 4, for more information.

e. **Analyze the Adversary Intelligence Threat.** Because assessments are conducted from an adversarial perspective, it is important to conduct a comprehensive all-source threat assessment that addresses any updates to the adversary intelligence capability. Intelligence and counterintelligence staffs will normally provide this information (found in annex B of the OPLAN).

f. **Understand the Operation or Activity Assessed.** The team members' thorough understanding of the operation or activity to be assessed is crucial to ensuring the success of subsequent phases of the assessment. Team members should become familiar with the OPLANs, OPORDs, MILDEC activities, standard operating procedures (SOPs), or other directives bearing on the assessed operation or activity. This initial review familiarizes team members with the mission and concept of operations and identifies most of the organizations participating in the assessed activity (others may be identified as the assessment progresses).

g. **Review Empirical Studies.** Empirical studies, such as communications monitoring or CI reports, simulate aspects of the adversary intelligence threat and support vulnerability findings. An example would be to review results of preparations (workups) to the major operation such as, computer simulations, war games, sand table exercises, field exercises, and command post exercises. This may already be available from information used to complete step 3 of the OPSEC Process. These studies also help the assessment team identify vulnerabilities that cannot be determined through interviews or observation. The results of these studies are useful to the assessment team during the field or analytic phase of the assessment. These studies can help the team identify vulnerabilities that cannot be determined through observation of the operation and interviews of personnel. Arrangements for their use should be made as far in advance of the assessment as possible.

h. **Develop a Functional Outline**

(1) A basic OPSEC assessment technique involves the construction of a chronology of events that are expected to occur in the assessed operation or activity. Events are assembled sequentially, thus creating a timeline that describes in detail the activities or plans of an operation or activity.

(2) After the chronology is assembled, vulnerabilities can be identified in light of the known or projected threat. (See examples at Appendix B, "Functional Outlines and Profiles"). Collectively, the outlines project a time-phased picture of the events associated with the planning, preparation, execution, and conclusion of the operation or activity. The outlines also provide an analytic basis for identifying events and activities that are vulnerable to adversary exploitation.

i. **Determine Preliminary Friendly Vulnerabilities.** After the adversary intelligence threat and the OPSEC indicators are determined, a subjective evaluation must be made of the potential friendly vulnerabilities. A vulnerability (e.g., a detectable, exploitable event) may or may not carry a security classification at the time of its identification, but such preliminary vulnerabilities must be protected from disclosure by administrative or security controls. These preliminary friendly vulnerabilities are refined in later stages of the OPSEC assessment.

j. **Announce the Assessment**

(1) After team members are selected and are familiar with the operation or activity to be assessed, the organization conducting the assessment should inform its subordinate and supporting organizations an assessment will be conducted so that preparations can be made to support the team during the field assessment phase.

(2) The following information should be included:

(a) Assessment purpose and scope.

(b) List of team members and their clearances.

(c) List of required briefings and orientations.

(d) Timeframe involved.

(e) Administrative support requirements.

(f) All support requirements, such as COMSEC monitoring support requirements (if needed).

(g) Network vulnerability assessments requirements (as needed).

k. Example of a Functional Outline. The outline below can be applied to all the different functional areas such as intelligence, logistics, communications, operations, and administration and support.

(1) Planned Event Sequence. The OPLAN and command/staff briefs form the basis for this timeline. This can be formulated using a lineal listing, a matrix, or another suitable method as required.

(2) Actual Event Sequence. Observe and record events as they actually occur while assessing activities. Be especially cognizant of the information listed in paragraphs three through five below.

(3) Critical Information. List all OPSEC critical information that the command has identified in their OPLAN (annex B).

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

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

(6) Analysis. Determine any OPSEC vulnerabilities through review of the OPLAN (Annex B), command/staff briefs, and actual activities/operations observed. You are looking for OPSEC indicators that can reveal critical information. This condition creates a vulnerability that can be exploited by the adversary. Are the identified OPSEC countermeasures effective in protecting the critical information by preventing the adversary from collecting and accurately interpreting the OPSEC indicators?

3. Assessment Execution

a. **Introduction.** As noted previously, data collection begins in the planning phase with a review of associated documentation. During the assessment phase, interviews with personnel directly involved in the operation, together with observations and document collection, are the primary means of data collection. The following actions are normally accomplished during the assessment phase.

b. **Command Briefing on Operation to Be Assessed.** This briefing is presented to the OPSEC assessment team by the command directing the forces or assets involved in the operation or activity being assessed. The purpose of the briefing is to provide the assessment team with an overview of the operation from the command's point of view. Team members should use this opportunity to clarify remaining questions about the information developed in the planning phase. Include in the brief a summary of the hostile collection capabilities, threat, and the vulnerability assessment. The command should be asked to comment on this to validate the assessment. This brief to the command can be a formal presentation or informal discussion.

c. **Operations Security Assessment Team Briefing.** This briefing is presented by the chief of the assessment team to the commander and principal staff officers of the assessed organization. The briefing may be either a formal presentation or an informal discussion. The objective is to inform the commander and the staff of how the assessment will be conducted. The briefing includes a summary of the relevant threat and the vulnerability assessment developed during the planning phase. The staff should be asked to comment on the validity of this assessment. Results of previous OPSEC assessments of similar activities may be summarized.

d. **Data Collection and Functional Outline Refinement**

(1) During the assessment phase, data is collected through observation of activities, document collection, and personnel interviews. Data may also be acquired through concurrent ongoing empirical data

collection, such as COMSEC monitoring. Observe activities and operations using the functional outline as your guide.

(2) Team members must be alert to differences between what they have read, what they have assumed to be the situation, what they have been told in the command briefing, and what they observe and are told by personnel participating in the operation. Conflicting data are to be expected.

(3) While observations can verify the occurrence, sequence, and exact timing of events, much essential information must be gathered from interviews.

(a) Functional outlines should be reviewed before and after interviews to ensure that all pertinent points are covered. Specifics on how, when, and where people accomplish their tasks, and how these tasks relate to the planned and observed sequence of events, are recorded in order to document activities in a logical sequence.

(b) Team members should assure interviewees all sources of information are protected by a non-attribution policy.

(c) Interviews are best conducted by two team members.

(d) Facts to be recorded during or soon after the interview normally include:

1. Identification and purpose of the interview.

2. Description of the billets occupied by the individuals being interviewed.

3. Details of exactly what tasks the individuals perform and how, when, and where they perform them with a view toward determining what information they receive, handle, or generate, and what they do with it.

4. Whether the individuals' actions reflect an awareness of a hostile intelligence collection threat.

(4) Tentative findings will begin to emerge as data collection proceeds and information is reviewed and compared. The findings should be confirmed and fully documented as quickly as possible.

(5) If a finding is considered to have serious mission impact, it should be made known to the commander responsible for the operation in order to permit early corrective actions.

(6) Development of findings during the assessment phase ensures access to supporting data and eliminates the need to reconstruct evidence after the team has left the scene. Following this procedure, the basic findings and supporting data of the final assessment report are well developed before the end of the assessment phase. Final development and production of the assessment report can then proceed immediately upon the team's return to home station.

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

e. **Team Employment**

(1) The complexity, size, and duration of the assessed operation or activity will determine the general employment of the assessment team. Tentative locations for data collection, developed during the planning phase, provide initial indications of how and where to employ the team.

(2) It is rarely possible, however, to plan employment in detail before the assessment phase. A limited, short-duration operation with few participating elements may permit concentrating the team in one location, or a very few locations. Larger and longer operations may require complete dispersal of the team, movement of the entire team from one location to another, or both, over a substantial period of time. The most reliable guideline for the team chief in determining how to employ the team is to reassemble it daily, either physically or via a collaborative method, to assess progress, compare data, and coordinate the direction of the assessment.

(3) The duration of the assessment phase is established during the planning phase and depends on how rapidly data is collected. Many assessments have required 30 days or more. Less comprehensive ones might require a week to 10 days. The proximity of data collection locations to each other, number of such locations, transportation availability, and degree of difficulty experienced in resolving conflicting data are some of the factors affecting duration of the assessment phase.

f. **Operations Security Assessment Team Exit Briefing**

(1) An exit briefing should be presented to the commander before the team leaves a command, regardless of previous reports or tentative findings. Like the entrance briefing, the exit briefing can be an informal discussion with the commander or a formal briefing for the commander and the staff.

(2) The tentative nature of assessment findings should be emphasized. Even those that appear to be firm may be altered by the final data review as the assessment report is prepared. Because preparation of the written report may take some time, the exit briefing can serve as an interim basis for further consideration and possible action by the commander.

(3) The distribution of the final written report should be clearly stated during the exit briefing. Normally, the report is provided directly to the commander. Some commands have found it useful to forward an interim report to the assessed commander for comments before proceeding with the final version.

4. Analysis and Reporting. During this portion, the OPSEC team compiles the data acquired by individual members with information from any empirical studies conducted in conjunction with the assessment.

a. **Correlation of Data**

(1) **Correlation of Functional Outlines.** When the separate chronology outlines for each functional area are correlated, the chronology of events for the operation or activity as a whole will emerge. Review and compare assessment data to clarify any conflicts.

(2) **Correlation of Empirical Data.** In addition to correlating data acquired from the observations of individual team members, the assessment team may also use relevant, empirically-derived data to refine individual functional outlines. More important, this data can also verify vulnerabilities that would otherwise be exceedingly speculative or tenuous. Empirical data is extremely important to a comprehensive assessment.

b. **Identification of Vulnerabilities**

(1) The correlation and analysis of data help the team to refine previously identified preliminary vulnerabilities or isolate new ones. This analysis is accomplished in a manner similar to the way in which adversaries would process information through their intelligence systems.

(2) Indicators that are potentially observable are identified as vulnerabilities. Vulnerabilities point out situations that an adversary may be able to exploit. The key factors of vulnerabilities are observable indicators, an intelligence collection threat to those indicators, and capability to impact friendly operations.

(3) The degree of risk to the friendly mission depends on the adversary's ability to react to the situation in sufficient time to degrade friendly mission or task effectiveness.

c. **Operations Security Assessment Report**

(1) The report of the OPSEC assessment is addressed to the commander of the assessed operation or activity. Lengthy reports (more than 15 pages) should be accompanied by an executive summary.

(2) The report should provide a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis, and recommended OPSEC countermeasures to eliminate or reduce the vulnerabilities. Although some of the vulnerabilities may be virtually impossible to eliminate or reduce, they are included in the report to enable commanders to assess their operation or activity more realistically.

(3) Each report should contain a threat statement. Its length and classification need only be adequate to substantiate the vulnerabilities (or actual sources of adversary information) described in the report. The statement may be included in the main body of the report or as an annex. Portions of the threat that apply to a particular vulnerability finding are concisely stated as substantiation in a paragraph preceding or following the explanation of the observation. If the threat statement is classified at a level that impedes the desired distribution and handling, the statement, or parts of it, should be affixed as an annex that is included only in copies of the assessment report provided to appropriately cleared recipients.

(4) The section that delineates vulnerabilities can be presented in a sequence that correlates with their significance, in an order that coincides

with their appearance in the chronological progression of the assessed operation or activity, or grouped together according to functional area (logistics, communications, and personnel). A particular vulnerability can be introduced by a headline followed by an adequate description of the finding and accompanied by identification of that portion of the operation or activity that includes the vulnerability. As stated earlier, a vulnerability observation may also include relevant threat references.

(5) If possible, OPSEC teams should include recommendations for corrective actions in the report. However, the team is not compelled to accompany each of the identified vulnerability finding with a recommendation. In some situations, the team may not be qualified to devise the corrective action; in others, it may not have an appreciation of the limitations in resources and options of a particular command. It may sometimes be more effective for the team to present the recommendation informally rather than including it in the assessment report. Recommendations of the OPSEC team may be particularly valuable in situations in which any vulnerability crosses command lines. Ultimately, commanders or the responsible officials must assess the effect of possible adversary exploitation of vulnerabilities on the effectiveness of their operation or activity. They must then decide between implementing corrective actions or accepting the risk posed by the vulnerability.

(6) Appendixes and annexes to OPSEC assessment reports may be added to support the vulnerability findings and conclusions. Sections, such as a threat annex, may include empirical studies (or parts of them). Maps, diagrams, and other illustrative materials are some ways to substantiate OPSEC vulnerabilities.

(7) The report may end with a conclusion or summary of the assessment and its findings. The summary should not include judgments about compliance with standing security practices of the organizations. Such judgments are the purview of security disciplines.

(8) Distribution of the assessment team's report should be limited to the principal commands responsible for the assessed operation or activity. After the commands have had time to evaluate the report and take corrective actions, they can consider additional distribution. Abstracts from the report may be provided for lessons learned documents or databases on a non-attribution basis.

(9) Because they contain vulnerability information, OPSEC assessment reports must be controlled from release to unauthorized persons or agencies. Affected portions of the report are controlled in accordance with applicable security classification guides. For those portions of the report not controlled by security classification guides, administrative control of the release of assessment report information must be considered. Likewise, the notes, interviews, and raw data used to build an assessment report are subject to the same controls as the finished report

5. Example Format for a Final OPSEC Assessment Report.

a. Overview

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

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

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

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

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

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

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

(3) Conclusions/Recommendations. Recommend OPSEC countermeasures 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 countermeasure, then be honest and state this. The command can then plan, develop, and apply appropriate OPSEC countermeasures for future or current operations. The command needs to determine if OPSEC lessons learned can be applied to other commands and disseminate the information appropriately. Care must be taken to appropriately classify and handle the final OPSEC Assessment Report in accordance with the appropriate security directives.

FUNCTIONAL OUTLINES AND PROFILE GUIDELINES

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR INTELLIGENCE COLLECTION OPERATIONS

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

2. Planned Event Sequence. See the intelligence collection plan prepared by intelligence staff element.

3. Actual Event Sequence. Observe events in the joint intelligence center.

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

5. Examples of Typical Indicators:

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

b. Increased traffic on intelligence communications nets.

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

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

e. Increased activity of friendly agent nets.

f. Increased levels of activity by airborne intelligence systems.

g. Alterations in the orbits of intelligence satellites.

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

i. Requests for maps and other topographic material.

j. Appearance of OPSEC assessment team.

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR LOGISTICS

1. General. The completed logistic profile presents a picture of logistic activities conducted in preparation for an impending operation. As in the administration function, the long lead time for some preparations gives early warning of forthcoming operations if events are compromised.

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

3. Actual Event Sequence. Observation, interviews.

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

5. Examples of Typical Indicators:

a. Special equipment issue.

b. Pre-positioning of equipment and supplies.

c. Increased weapons and vehicle maintenance.

d. Petroleum, oils, and lubricants stockpiling.

e. Upgrading lines of communications.

f. Ammunition stockpiling.

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

h. Arrival of new logistic units and personnel.

i. Increased requisition of supplies.

j. Increased traffic on logistic communications nets.

k. Changes in normal delivery patterns.

l. Appearance of OPSEC assessment team.

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR COMMUNICATIONS

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

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

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

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

5. Examples of Typical Indicators

a. Increased radio, teletype, and telephone traffic.

b. Increased communications checks.

c. Appearance of new stations in net.

d. New frequency and call-sign assignments.

e. New codes and authenticators.

f. Radio silence.

g. Changing call-up patterns.

h. Use of maintenance frequencies to test equipment.

i. Communications command post exercises.

j. Appearance of different cryptographic equipment and materials.

k. Unclassified network activity.

l. Appearance of OPSEC assessment team.

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR OPERATIONS

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

2. Planned Event Sequence. OPLAN, OPORD, SOP.

3. Actual Event Sequence. Observations, reports, messages, interviews.

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

5. Examples of Typical Indicators:

a. Rehearsals and drills.

b. Special-tactics refresher training.

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

d. Pre-positioning of artillery and aviation units.

e. Artillery registration in new objective area.

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

g. Appearance of new attached units.

h. Issuance of new equipment.

i. Changes in major unit leadership.

j. Repositioning of maneuver units.

k. Appearance of OPSEC assessment team.

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR ADMINISTRATION AND SUPPORT

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

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

3. Actual Event Schedule. Observations and interviews.

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

5. Examples of Typical Indicators:

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

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

c. Changes to wake-up and dining schedules.

d. Changes to mailing addresses.

e. New unit designators on mail.

f. Emergency personnel requisitions and fills for critical skills.

g. Medical supply stockpiling.

h. Emergency recall of personnel on leave and liberty.

i. Increased activity at administrative/support offices, including processing of wills by legal department.

j. Appearance of OPSEC assessment team.

CONTRACT REQUIREMENTS

1. INTRODUCTION

a. Commanders and directors shall ensure that contractors supporting Marine Corps commands use OPSEC to protect critical information for specified contracts and subcontracts. The Marine Corps activity and their Government Contracting Activity (GCA) shall impose OPSEC countermeasures as contractual requirements when necessary.

b. It is the Marine Corps activity's responsibility to:

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

(2) Identify those OPSEC countermeasures in their requirements documents.

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

2. PROCEDURES. Heads of the Marine Corps 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 when appropriate.

a. Marine Corps 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 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 review shall be conducted of the statement of work (SOW) 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. It is important that GCAs work with their OPSEC program managers and coordinators to identify OPSEC requirements for the scope of work to be performed. The SOW should also undergo a formal content review prior to its release to the public.

c. Requirements for OPSEC must be included in the contract solicitation and resulting contract in sufficient detail to ensure complete contractor understanding of all OPSEC provisions required. 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 Marine Corps command or unit 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 ordered.

(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 classified 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 in ensuring adequacy of industrial security efforts for OPSEC applied to classified contracts in accordance with DoD 5220.22-R.

3. DD FORM 254 (Contract Security Classification Specifications)

a. Classified contracts and contract 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 requirement for OPSEC countermeasures.

b. For classified 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 DoD 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense, July 16, 2008, is required. Compliance with OPSEC countermeasures, if imposed by programs supported or by documents generated by [the contracting Activity or Organization], may be necessary. OPSEC program will be in accordance with DoD 5205.02-M, dated November 3, 2008. Program OPSEC plans shall be coordinated with and approved by [the Contracting Activity OPSEC Manager] and shall 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 Operations Security (OPSEC) plan in accordance with the attached 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 should also be inserted: "It may be necessary for OPSEC plans, surveys, and activities 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 cognizant Defense Security Service (DSS) Field Office and will be used by DSS in support of industrial security inspections.

DETAILED INSPECTION CHECKLIST

FA	SC	STMT	TEXT
481			OPERATIONS SECURITY (OPSEC) Functional Area Manager: PP&O, PL, PLI Point of Contact: JAMES J. SYDNOR (DSN) 222-4293 (COML) (703) 693-4293 E-mail: James.J.Sydnor@usmc.mil Date Last Revised: 18 June 2013
481	01		OPERATIONS SECURITY
481	01	001	How is OPSEC integrated into all day-to-day activities and operations? Reference MCO 3070.2A, PAR 1B
481	01	002	Provide documentation of how the OPSEC planning process is incorporated into operations, exercises, activities, system development, and test and evaluation in garrison and deployed environments. Reference MCO 3070.2A, PAR 4A (1) (A)
481	01	003	Provide a copy of each of the OPSEC Manager's and/or Coordinator's signed appointment letter/s Reference MCO 3070.2A, PAR 4A (2) (A)
481	01	004	Provide a list to include point of contacts for all subordinate commands one level below. Reference MCO 3070.2A, PAR 4B (15) (B)
481	01	005	Provide a copy of the command's annual review of all subordinate OPSEC programs. Reference MCO 3070.2A, PAR 4B (15) (D)
481	01	006	Provide a copy of the command's OPSEC order that is signed by the commanding officer and includes the command's Critical Information List (CIL). Reference MCO 3070.2A, PAR 4B (17) (C)
481	01	007	Where applicable provide a current copy of a DD254 that reflect OPSEC responsibilities. Reference MCO 3070.2A, PAR 4B (17) (C) 6
481	01	008	Provide supporting documentation of quarterly review of command sponsored social media and official websites. Reference MCO 3070.2A, PAR 4B (8)

481 01 009 Provide a copy of the annual command level OPSEC assessment.
Reference
MCO 3070.2A, PAR 4B (11) (A)

481 01 010 Conduct a demonstration of the command's automated risk assessment tool.
Reference
MCO 3070.2A, PAR 4B (11) (B)

481 01 011 Provide supporting documentation of the completion of annual training.
Reference
MCO 3070.2, PAR 4C (3) (C)

481 01 012 Provide supporting documentation that all program managers and coordinators have completed OPSEC fundamentals.
Reference
MCO 3070.2, PAR 4C (3) (D)

481 01 013 Provide supporting documentation that all program managers and coordinators at the Regimental/Group level and higher, to include supporting agencies/activities, have completed the Interagency OPSEC Support Staff's OPSEC Analysis and Program Management (OPSE 2500) resident course or equivalent.
Reference
MCO 3070.2, PAR 4C (3) (E)

481 01 014 Provide supporting documentation that all program managers and coordinators, public affairs officers, family readiness officers, webmasters, and any other personnel authorized to review information for public release via the internet have received "web" OPSEC training.
Reference
MCO 3070.2, PAR 4C (3) (F) and DoDD 5205.02E Encl 2,11.1

481 01 015 Does the command's unclassified publicly available website(s) display personnel lists, "roster boards", organizational charts, or command staff directories which show individuals' names, individual's phone numbers, or email addresses which contain the individual's names?
Reference
MCO 3070.2, PAR 4C (4) (A) 3

481 01 016 Provide 3 years of records of the unit's Command Inspection Program and the Commanding General's Inspection Program.
Reference
MCO 3070.2, PAR 4C (7) (B) 2

481 01 017 Show how OPSEC is being promoted throughout the command.
Reference
MCO 3070.2, PAR 4C (10)

481 01 018 How often is the Critical Information List (CIL) updated and what is the bases for updating the CIL?
Reference
DoDD 5205.02E Encl 2, 11.b

481 01 019 How is the CIL disseminated throughout the organization?
Reference
DoDD 5205.02E Encl 2, 11.b

481 01 020 Demonstrate, using the OPSEC process your organization's means for applying each of the five steps. Indicate how each of the five actions are applied or integrated within a related functional process.
Reference
MCO 3070.2A and DoDD 5205.02E

481 01 021 Provide a copy of the organization's most recent threat assessment. Demonstrate how the threat assessment was used to develop the CIL.
Reference
DoDD 5205.02E Encl 2, 11.g

481 01 022 Provide a copy of the organization's most recent risk assessment. Demonstrate how the risk assessment was used to determine appropriate countermeasures.
Reference
DoDD 5205.02E Encl 2, 11.g