UNITED STATES MARINE CORPS
COMMAND ELEMENT
II MARINE EXPEDITIONARY FORCE
PSC BOX 20080
CAMP LEJEUNE, NORTH CAROLINA 28542-0085

II MEFO 3070.1A
G-3
MAY 07 2019

II MARINE EXPEDITIONARY FORCE ORDER 3070.1A

From: Commanding General, II Marine Expeditionary Force
To: Distribution List

Subj: II MARINE EXPEDITIONARY FORCE OPERATIONS SECURITY STANDING OPERATING PROCEDURES

Ref: (a) MCO 3070.2A, Marine Corps Operations Security Program
(b) MFCO 3070.1A, Marine Corps Forces Command Operations Security
(c) Joint Publication 3-13.3, Operations Security, dated 4 January 2012

Encl: (1) OPSEC Terms and Definitions
(2) OPSEC Training Requirements
(3) OPSEC Working Group 7-Minute Drill
(4) Example Appointment Letter
(5) II MEF Critical Information List
(6) Unclassified Website OPSEC
(7) OPSEC Assessments and Program Reviews

1. Situation

a. Purpose. To establish policy and procedures for the Operations Security (OPSEC) Program within II Marine Expeditionary Force (MEF) and its Major Subordinate Commands and Elements (MSCs/MSEs), as well as any commands or units that may be assigned or attached to II MEF.

b. Background. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities by doing the following tasks:

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

(2) Determine potential OPSEC indicators that hostile intelligence systems might obtain which could be used to derive critical information in sufficient time to be useful to adversaries.

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

(4) Incorporate OPSEC during the planning, preparation, execution, and post-execution of operations and activities.

(5) Ensure OPSEC is a continuous process that contributes to the overall effort for mission success and allows each individual to participate in the process on a daily basis.

c. Terms and Definitions. See enclosure (1).

2. Cancellation. II MEFO 3070.1.

3. Mission. II MEF will implement an aggressive and effective OPSEC program that promotes education and awareness to ensure all II MEF personnel are responsible for and prepared to support OPSEC and safeguarding information in order to deny an adversary or potential adversary access to critical information that could be used to predict friendly intentions, capabilities, or activities.

4. Execution

a. Commander's Intent. II MEF maintains a systematic approach to OPSEC that uses established processes and methods to deny adversaries or potential adversaries access to critical information that facilitates the prediction of friendly intentions, capabilities, limitations or activities pertaining to our military situation. Endstate: All II MEF personnel are trained in OPSEC procedures, and the adversary is denied access to critical information through a proactive and aggressive culture of OPSEC.

b. Concept of Operations. In accordance with references (a) and (b), II MEF Command Element and MSCs/MSEs will ensure unclassified, sensitive information, is safeguarded and all Marines, Sailors, civilians, and contractors assigned to II MEF use proper OPSEC measures. This will be accomplished by:

(1) Appointing appropriate OPSEC coordinators;

(2) Maintaining an OPSEC plan;

(3) Exercising a rigorous education and awareness campaign;

(4) Conducting required training for key personnel as outlined in enclosure (2);

(5) Conducting annual command level assessments;

(6) Submitting annual reports to Headquarters Marine Corps (HQMC).

c. Tasks

(1) All II MEF Staff Sections. Designate an Officer, Staff Noncommissioned Officer (SNCO), or appropriate Department of Defense (DoD) Civilian to serve on and support the collective efforts of the II MEF OPSEC Working Group identified in enclosure (3).

(2) Assistant Chief of Staff G-1, II MEF

(a) Assist the Assistant Chief of Staff (AC/S) G-3 in planning, coordinating, and executing security support during the drafting and reviewing of OPSEC plans.

(b) Provide functional expertise, as required, in the planning, execution, and analysis of command OPSEC assessments of the II MEF Command Element.

(3) Assistant Chief of Staff G-2, II MEF

(a) Assist the AC/S G-3 in planning, coordinating, and executing counterintelligence support during the drafting and reviewing of OPSEC plans.

(b) Provide functional expertise, as required, in the planning, execution, and analysis of command OPSEC assessments of the II MEF Command Element.

(4) Assistant Chief of Staff G-3, II MEF

(a) Serve as lead agency and Program Manager on OPSEC matters for II MEF.

(b) Develop, maintain, and disseminate an OPSEC order and program for II MEF.

(c) Chair OPSEC Working Group as required. Working Groups shall consist of representatives from all Staff Sections including, Information Management Officer, Communication Strategy and Operations (COMMSTRAT), Security Manager, Naval Criminal Investagative Service (NCIS)and Information Operations (IO) OPSEC Working Group will:

1. Coordinate OPSEC matters amongst the II MEF staff and MSCs/MSEs.

2. Assist in development and implementation of the Command OPSEC program.

(d) Utilizing enclosure (4), designate an Officer, Staff Noncommissioned Officer, or DoD equivalent civilian as OPSEC Coordinator to perform the following duties:

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

2. Develop, coordinate, and maintain the command OPSEC program.

3. Serve as lead for OPSEC Working Group.

4. Develop and coordinate OPSEC education and training.

5. Coordinate command OPSEC assessment.

6. Conduct the annual OPSEC program review.

7. Submit annual OPSEC reports.

8. Provide assistance to MSC OPSEC coordinators as required.

(e) Appoint an Assistant OPSEC Coordinator to assist the OPSEC Coordinator with his duties as outlined in paragraph 4.c.(4)(d) above.

(5) Assistant Chief of Staff G-6, II MEF

(a) Assist the AC/S G-3 in planning, coordinating, and executing defensive cyber operations support during the drafting and reviwing of OPSEC plans.

(b) Provide functional expertise, as required, in the planning, execution, and analysis of command OPSEC assessments of the II MEF Command Element.

(6) Director, COMMSTRAT, II MEF

(a) Assist the AC/S G-3 in planning, coordinating, and executing Communication Strategy and Operations support during the drafting and reviewing of OPSEC plans.

(b) Receive and support application of the II MEF Critical Information List (CIL) and safeguarding of the data categories it contains.

(c) Ensure COMMSTRAT programs prevent inadvertent disclosure of CIL items.

(d) Execute activities and efforts as required to prevent the publishing of inappropriate information on public facing websites, social media, or other such information sources, per reference (a) paragraph 4.c.(4). Completion of reviews of such sites will be reported and documented quarterly to the II MEF OPSEC Coordinator. Inappropriate/unapproved information includes, but is not limited to:

1. For Official Use Only (FOUO) information;

2. Classified Information;

3. Critical Information;

4. Identity of family members;

5. Biographies that contain family information;

6. Personnel Rosters, Organizational Charts, and Staff Directories that contain individual names.

(e) Ensure completion of all required formal training for Communication Strategy and Operations and webmaster personnel per reference (a) and enclosure (2). Forward all training completion documentation to the II MEF OPSEC Coordinator.

(7) Information Management Officer, II MEF

(a) Support the development of threat assessments and their use in OPSEC process applications and the OPSEC program

generally, as vulnerability analysis, risk assessment, and identification of measures and countermeasures are conducted.

(b) Assist the AC/S G-3 in planning, coordinating, and executing information management support during the drafting and reviwing of OPSEC plans.

(c) Support activities and efforts to prevent the publishing of inappropriate information on public facing websites, social media, or other such information sources, per reference (a) paragraph 4.c.(4). Support will be directly to the II MEF OPSEC Coordinator who has direct responsibility, and to II MEF Communication Startegy who will take lead in executing these functions.

(8) Command Inspector General, II MEF

(a) Evaluate OPSEC as part of each unit's Command Inspection Program and the Commanding General's Readiness Inspection (CGRI) Programs. Inspection teams will review the OPSEC Functional Area of all commands visited by the Inspector General (IG) teams.

(b) The IG Marine Corps (IGMC) maintains an on line database of Functional Area Checklists (FAC). The website at which units will find the most recent OPSEC FAC (3070) is: http://www.hqmc.marines.mil/igmc/Resources/FunctionalAreaChecklists.aspx

(9) Security Program Manager, II MEF

(a) Support the development of Threat Assessments and their use in OPSEC process applications and the OPSEC program generally, as vulnerability analysis, risk assessment, and identification of measures and countermeasures are conducted.

(b) Coordinate Staff Security Training with the II MEF OPSEC Coordinator to ensure the inclusion of required OPSEC training topics and the maintenance of training completion/attendance records.

(10) All MSCs/MSEs Commanding Generals (CGs) and Commanding Officers (COs)

(a) Appoint in writing an Officer, SNCO, or equivalent Department of Defense civilian as the command OPSEC Coordinator at Battalion/Squadron and higher echelons to manage the OPSEC program. See enclosure (4) for example.

(b) Maintain OPSEC program at Battalion/Squadron Levels and higher echelons. At a minimum, the program shall consist of:

1. An OPSEC Order signed by the CG/CO.

2. OPSEC training as outlined in enclosure (2).

3. A CIL as in enclosure (5). OPSEC Coordinators will ensure the COMMSTRAT receive current copies of their command's CIL in order to prevent inadvertent disclosure of this information.

4. Develop and execute OPSEC plans in support of operations and exercises in cooperation with the Anti-terrorism Officer, Physical Security Manager, Cyber Security Manager, and the Intelligence Officer.

5. Ensure 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, and when contacted by the Defense Security Service (DSS), support them in their role of ensuring contract industrial security efforts are adequate).

6. Ensure the unit understands social networking concerns, periodically reviews unit operated web sites and meets the OPSEC responsibilities listed in enclosure (5) of this Order.

7. Conduct assessments and program reviews in accordance with enclosure (7), to include, at a minimum:

a. Conduct an annual, command level OPSEC assessment utilizing the Inspector General's Inspection Checklist.

d. Coordinating Instructions

(1) OPSEC is a command responsibility under the cognizance of the G-3. Per reference (c), if a command has an Information Officer or cell, the individual or group may be tasked

with managing the command's OPSEC program; however, the OPSEC program will be closely coordinated with other staff sections.

(2) All violations of OPSEC will be reported to the OPSEC coordinator who will then notify the chain of command.

5. Administration and Logistics

a. Administration

(1) Points of Contact. MSCs/MSEs will collect contact information on OPSEC Coordinators within II MEF and provide to the II MEF OPSEC Coordinator. The OPSEC Coordinator will be notified of any changes to contact information immediately.

(2) Inspections. Records of all assessments and program reviews will be retained for 3 years. Enclosure (7) outlines further detail.

(3) Report Submission. MSCs/MSEs will submit command OPSEC reports by unit OPSEC Coordinators with information consolidated from subordinates and submited to II MEF AC/S G-3 semi-annually. Reports are due at the end of June and December. The report will be a Microsoft Word document with the following information:

(a) OPSEC program status;

(b) Activities conducted during the reporting period that support the OPSEC program or command OPSEC posture (for example, training classes, working group meetings, assessments, program reviews, events, etc);

(c) Problem areas and recommendations;

(d) Lessons learned (as appropriate);

(e) Forecast of OPSEC activities during next reporting period;

(f) Updated roster of all II MEF MSC/E assigned OPSEC Coordinators down to the Battalion/Squadron level.

b. Logistics. As part of the quarterly and annual reports, identify any resource or funding requirements affecting the OPSEC program to the II MEF OPSEC Coordinator.

6. Command and Signal

a. Command. This order is applicable to all II MEF units and personnel to include DoD civilians and contract employees who are subject to military law or any unit that is established under this command in the foreseeable future.

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

B. N. WOLFORD
Chief of Staff

Distribution: A

OPSEC TERMS AND DEFINITIONS

1. All terms and definitions for this Order are derived from MCO 3070.2A.

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

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

4. OPSEC Assessments. An examination of an operation or activity to determine if adequate protection from adversary intelligence exploitation exists. The OPSEC assessment is used to verify the effectiveness of OPSEC measures and determine if critical information is being protected. An assessment cannot be conducted until after critical information has been identified. Without understanding critical information, which should be protected, there can be no specific determination that OPSEC vulnerabilities exist.

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

6. OPSEC Process. OPSEC planning is accomplished through the OPSEC process. The five steps involved in the OPSEC process are: identification of critical information, threat analysis, vulnerability analysis, risk assessment, and application of OPSEC measures.

7. OPSEC Program Managers and Coordinators. Program managers are personnel who perform OPSEC functions as their primary duty. Coordinators are personnel who perform OPSEC functions as an additional duty. Commanders will use their discretion in determining whether they require program managers or coordinators to fulfill their OPSEC responsibilities.

8. OPSEC Working Groups. These are teams of personnel with representatives from the different elements of the command's organization designed to assist the command with OPSEC matters and its program.

9. Threat. Any individual or organization that seeks to do harm by interrupting ongoing military operations or activities. In order to be classified as a threat, both of the following conditions must be satisfied:

a. An intent to do harm must exist.

b. A capability to do harm must exist.

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

OPSEC TRAINING REQUIREMENTS

1. OPSEC program managers and coordinators must complete 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."

a. All II MEF MSC/MSE OPSEC program managers/coordinators will:

(1) Attend the Interagency OPSEC Support Staff (IOSS) OPSE Analysis and Program Management resident course (OPSE 2500), 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/coordinators who completed the Navy's OPSEC Course or the Headquarters Department of the Army's OPSEC Course within six months prior to the publication date of this order will satisfy the requirements.

b. Per references (a), all command OPSEC managers/coordinators, COMMSTRAT Officers, Webmasters and any other personnel authorized to review information for public release via the internet, shall receive "web" OPSEC training. Completion of both OPSE-1500 and OPSE-3500 of the IOSS courses will satisfy this requirement.

(1) OPSEC and Public Release Decisions (OPSE 1500); register at http://www.ioss.gov/ or email ioss@radium.ncsc.mil.

(2) OPSEC and Web Risk Assessment Course (OPSE-3500); register at http://www.ioss.gov/ or email ioss@radium.ncsc.mil.

c. Annual OPSEC training will be conducted for all unit personnel. The web-based course "Uncle Sam's OPSEC," course code "OPSECUS001" located on MARINENET. Once completed, "Uncle Sam's OPSEC" will pass training code "AO" to the Marine Corps

Total Force System (MCTFS). However, unit personnel must complete all training for that calendar year (CY) for reporting and functional area inspection purposes. Civilian personnel will complete the web based course in Total Workforce Management System (TWMS).

d. Any II MEF request for contractual procurement that will bring civilian contract employees on base will include addressing OPSEC concerns. All statements of work will reference this order and require civilian contractors to conform to the II MEF OPSEC program.

OPSEC Working Group 7-Minute Drill

Purpose:

To coordinate OPSEC matters amongst the II MEF staff. Develop OPSEC plan for operations, training and COMREL events, rotational deployments, with II MEF equity by CCMD.

Location: II MEF G-3 Fires & Effects Coordination Cell (FECC) Conference Room

Day: TBD

Time: TBD

Frequency: As Needed

Attendees:

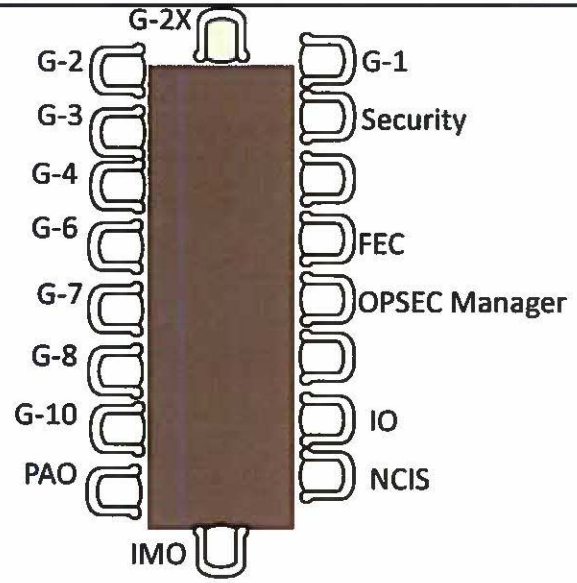
Chair: G-3 FEC (or designated appointee)

Facilitator: II MEF OPSEC Coordinator

Required: Representatives from all Staff Sections , including, Information Management Officer, Communication Strategy and Operations Officer , Security Manager, Information Officer (IO), NCIS

Secretary: II MEF OPSEC Coordinator

Others as required: TBD



Inputs:

- Potential or actual OPSEC issues or concerns.
- Input on future operations
- Updates on previous request for information (RFI) from last briefing.

Outputs:

- As required (based on CG II MEF guidance and requests for additional information).
- Verbal FECC guidance/decision regarding emergent issues concerns.

Lines of Operations:

05 Apr 19

UNITED STATES MARINE CORPS
COMMAND ELEMENT
II MARINE EXPEDITIONARY FORCE
PSC BOX 20080
CAMP LEJEUNE, NC 28542-0080

MAY 07 2019

IN REPLY REFER TO:
3302
FECC

From: Chief of Staff, II Marine Expeditionary Force
To: Major Devil D. Marine, 1234567890/0679 USMC

Subj: APPOINTMENT AS THE OPERATIONAL SECURITY OFFICER

Ref: (a) MCO 3070.2A

1. In accordance with the references, you are hereby appointed as the Operational Security (OPSEC) Officer for II Marine Expeditionary Force (MEF).

2. You are directed to familiarize yourself with the reference and all other pertinent or applicable directives and instructions pertaining to this appointment.

C. O. SEMPER

3302
FECC

FIRST ENDORSEMENT

From: Major Devil D. Marine, 1234567890/0679 USMC
To: Chief of Staff, II Marine Expeditionary Force

1. I have familiarized myself with the reference and have assumed all duties as the OPSEC officer for II MEF.

D. D. MARINE

Enclosure (4)

II MEF CRITICAL INFORMATION LIST

1. Current/future United States or Foreign Government operational activities as pertaining to operational employment of II MEF forces. For example, the strategic planning for Operation IRAQI FREEDOM is classified; a Combatant Commander Theater engagement plan maybe unclassified. (Mission, strategies and strategic planning, objective dates/times).

2. Scope of specific operations. (Movement of forces, force disposition/capabilities, limitations, tactics/techniques/procedures, command relationships, operation order details).

3. Intelligence, surveillance, and reconnaissance asset support of operations. (Collection techniques, capabilities/limitations, associated mission nicknames or CODE WORDS).

4. Detailed diagrams of camps/bases, photos showing layouts of bases, maps, and geospatial data, unit operating areas and boundaries. This is applicable to installations in a combat zone, or when deployed, such as the layout of Camp Leatherneck in Afghanistan.

5. Specific peripheral operational data pertaining to a specific operation or deployment common sense must be applied - for example, a meeting to discuss a Marine Expeditionary Unit pre-deployment training plan, and the resultant plan, is not critical information. However, the "sail date" is critical information. (Special duty rosters, itineraries/time tables, meetings, conferences, working groups, drivers/aides/Personal Security Details schedules).

6. Communications involved with or in support of the operation. (Capabilities/ limitations, call signs, frequencies, information network vulnerabilities, computer passwords, special equipment, and program details).

7. Administrative support to the operation. (Recall rosters, travel plans, planning rosters, joint manning documents, unit personnel strength/shortfalls, unit organizational charts, and personal data).

8. Personal protected information (PPI) of all personnel (U.S. contractors, and Foreign Government employees) involved in any operation or activity associated with II MEF operations.

UNCLASSIFIED WEBSITE OPSEC

1. Today's technology has led and is leading to many new forms of communication. Marines are responsible for the content they publish on social networking sites (SNS), blogs, or other unclassified, publicly available websites, as they present a potential risk to personnel, assets, and operations if inappropriate information is published. OPSEC Officers will review their command's website to ensure no critical information is published (data, graphics, or photographs).

2. Marines will take steps to ensure that all Marine Corps content is accurate and appropriate. Additionally, Marines will not post classified, controlled classified, sensitive information, and all information included in the Critical Information List. When in doubt, the Marine will consult the unit OPSEC Officer, Public Affairs Officer, Security Officer and or Intelligence Officer for guidance.

3. Unclassified, publicly available websites (Marines.mil, Facebook, Instagram) 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 Charge, Executive Officers or Deputies, the civilian equivalents of those officers 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. When creating or posting to official USMC social media sites and personal social media sites, refer to the Rules of Engagement/Standard Operating Procedure on the marines.mil website at: http://www.marines.mil/News/SocialMedia/SOPs.aspx this site provides the regulatory requirements for establishing, registering and operating SNS pages.

OPSEC ASSESSMENTS AND PROGRAM REVIEWS

1. Purpose. This SOP provides direction and guidance for the conduct of II MEF OPSEC assessments and program reviews. Assessments and program reviews will be tailored at the direction of the commander to meet the needs of II MEF organizations or specific operations.

2. General. OPSEC assessments and program reviews will be conducted annually to assess OPSEC in normal garrison routine, as well as for particular operations and deployments.

a. All MSCs/MSEs will conduct annual program reviews and assessments of all subordinate commands using the OPSEC Functional Area Checklist 3070.

(1) These annual reviews and assessments of subordinate commands must be conducted by an inspector who has been to the resident OPSEC training.

(2) Records of these reviews and assessments 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.

b. All commands required to maintain an OPSEC program will conduct an internal program review and assessment, at least annually. During this annual 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 this annual assessment. Commands which desire a formal assessment will forward a request to Navy Information Operations Command Norfolk/CTF 1030 at opsec@navy.mil.

3. Program Review Methodology. Program reviews will be conducted in accordance with the most recent Inspector General's Marine Corps OPSEC checklist (3070). This can be found at: http://www.hqmc.marines.mil/igmc/Resources/FunctionalAreaChecklists.aspx

4. Assessment Methodology

a. Planning

(1) In the planning phase, the scope of the assessment must be determined. Scope must be considered in terms of organization or operation size, complexity, geographic distribution and time available. Once the scope has been determined, an assessment team, comprised of individuals with appropriate skill sets, should be assembled. For smaller units, the assessment may be conducted solely by the OPSEC officer. Representatives who have expertise in areas to be reviewed are invaluable at identifying information protection shortcomings.

(2) A program review may include the following activities:

(a) Open Source Information Collection. Team members should review publicly available information (via articles, press releases, command websites, internet) on the organization or activity to determine the extent of information available to the adversary. The search should attempt to identify critical information available in the public domain.

(b) Personnel Interviews. Interviews must be conducted on a non-attribution basis. Assessment personnel should ask specific questions about the organization or operation that is being assessed and the individual's understanding of the threat, vulnerabilities, possible indicators, and how they exchange information. By standardizing interview questions, the team will be able to draw conclusions from trends that present against a cross-section of responses.

(c) Observation of Activities and Routines. By observing activities, team members are able to identify indicators first-hand associated with operations. By studying activities over time, patterns can be identified that require measures to mitigate the risk adversary exploitation.

(d) "Dumpster Diving". Information recovered during searches of trash containers and recycle bins can highlight the need for stricter paper disposal policies. Often, personnel do not realize the value of information placed in the trash. This information is often exploited by adversaries for its intelligence value.

b. Execution

(1) Prior to beginning a program review, the team should brief the command leadership of the organization or operation to explain the team's activities, expectations, and content and handling of the final report. The command being evaluated/assessed should provide an authorization letter to the team which permits team members to perform these activities. This letter is required in the event team members are challenged by security personnel.

(2) As the program review progresses, team members should begin compiling observations and findings in the form of a draft report. This report will be the basis of the command program review out-brief.

(3) At the conclusion of the program review, the team lead will provide an out-brief to command leadership. Initial analysis presented within the out-brief is subject to revision based on further study. However, general observations can be made at this point with a degree of accuracy. An overview of the team's findings should be presented with recommendations for improvement.

c. Program Review Report. After the assessment team has thoroughly reviewed the information collected, the team will produce a written report. The report may be classified, depending on the content and findings. The report will identify findings with proposed OPSEC measures or recommendations for improvement to protect critical information, vulnerabilities and indicators. The assessment report belongs to the organization requesting the evaluation. Other organizations, including higher headquarters, desiring a copy of the report must request the report from the assessed organization. The team will not provide the assessment report to other commands.