From: Commander, Navy Reserve Force

Subj: OPERATIONS SECURITY PROGRAM

Ref: (a) DoD Directive 5205.02E of 20 June 2012
(b) DoD 5205.02-M, DoD Operations Security Program Manual, November 2008
(c) OPNAVINST 3432.1A
(d) ALNAV 056/10

Encl: (1) Standard OPSEC Process
(2) Annual OPSEC Posture Assessment Report Format

1. Purpose. To establish policy and provide guidance for implementing and managing the Navy Reserve Operations Security (OPSEC) program per references (a) through (d).

2. Discussion

a. OPSEC is a systematic, proven process that identifies controls and protects generally sensitive but unclassified information about the command's mission and operations. When effectively employed, it enables mission success by preventing inadvertent compromise of sensitive or classified activities, capabilities, or intentions. The potential for exploitation of open source material including the internet, media and other generally unclassified but sensitive information is a significant challenge to providing adequate force protection, as well as safeguarding other sensitive or classified activities. As a result, OPSEC is vital in mitigating risks associated with all military operations.

b. The OPSEC program should focus on command functions where specific actions, such as planning, preparing, executing, supporting operations or other activities may convey indicators that an adversary could exploit and ultimately use to adversely affect Commander, Navy Reserve Force role in supporting Fleet missions.

c. OPSEC countermeasures should not be so excessive that they degrade operational effectiveness by interfering with activities
such as coordination, training and logistical support. Military operations are inherently risky and the Commander must evaluate each activity and operation, and then balance required OPSEC measures against operational needs. Using the OPSEC process will help Commanders assess the risk and apply appropriate OPSEC measures.

3. Policy. The goal of the command OPSEC Program is to increase operational effectiveness of planned and ongoing United States (U.S.) military activities by protecting unclassified indicators which convey intentions, capabilities or limitations of U.S. forces involved in protected activities.

4. Applicability. The provisions of this instruction are applicable to the Navy Reserve and all personnel conducting contracted services for the Navy Reserve effective on the date signed.

5. Responsibilities

a. N002 Inspector General and Echelon IV Commanders shall develop and implement a mission applicable OPSEC section for their inspection criteria for assessments of all command’s under their cognizance per reference (b).

b. Commanders shall:

   (1) Establish and implement an OPSEC program that meets all applicable requirements delineated in references (a) through (d) and enclosures (1) and (2).

   (2) Designate an OPSEC program manager and/or officer in writing.

   (3) Discuss OPSEC concerns with their Ombudsman as part of their Key Volunteer Program and stress the family’s ability to contribute to protection of the command’s critical information (CI).

c. The OPSEC program manager and/or officer is responsible for the overall coordination of the command OPSEC program and shall:
(1) Maintain the command’s OPSEC program per all applicable requirements delineated in references (a) through (d) and enclosures (1) and (2).

(2) For command’s with Secure Internet Protocol Router Network access, establish an account with the Operations Security Collaboration Architecture program within 90 days of designation.

(3) Attend the Navy OPSEC Course (J-2G-0966) and register on the Navy Information Operations Command OPSEC officer registration system.

(4) Coordinate the establishment of the Command’s Critical Information List (CCIL) and ensure command personnel are informed of CI. The CCIL shall be posted near phones, fax, copy machines and information systems processing unclassified information.

(5) Establish a command OPSEC Working Group Meeting, at a minimum quarterly, to discuss OPSEC matters, coordinate OPSEC assessments, surveys and develop OPSEC training plans and execution.

(6) Provide assistance in OPSEC planning, support, advice and training of the OPSEC working group and command personnel.

(7) Develop command OPSEC survey procedures and planning guidance for conducting informal and formal OPSEC surveys.

(8) Ensure that command website risk assessments are conducted, at a minimum, annually.

(9) Maintain liaison with organizations and personnel critical to the execution of a command level OPSEC program, such as Public Affairs Officer (PAO), other command OPSEC officers, intelligence and counter-intelligence communities, external inspectors and traditional security program officers.

(10) The OPSEC officer should utilize enclosure (1) when developing OPSEC plans to protect CI.

(11) Ensure each new command member receives orientation to the command OPSEC program as a part of the command check-in or command indoctrination program.
(12) Ensure all command members receive annual OPSEC awareness training through instructor training, Navy Knowledge Online (NKO) or Computer Based Training (CBT).

d. OPSEC working group members will be comprised of members from the command and shall:

(1) Attend working group meetings as required.

(2) Complete OPSE-1300, OPSE-1301 CBT or equivalent basic OPSEC classroom training.

(3) Promote continuing awareness of the command OPSEC program through OPSEC posters, Plan of the Week notices, All Hands notices via command e-mail distribution or web site.

e. Human Resources shall:

(1) Ensure the OPSEC process is incorporated throughout the hiring process and when a program’s CI or associated indicators are subject to adversary exploitation or unacceptable risk per references (a) and (b).

(2) Determine what OPSEC measures and requirements are essential to protect CI for job advertisement.

(3) Establish procedures to verify Position Descriptions (PDs) properly reflect OPSEC responsibilities and ensuring those responsibilities are included in the PD. CI should be determined using references (a) through (c).

(4) Ensure publicly released documents do not reveal CI or indicators of CI. OPSEC program managers should review the PD prior to public release.

f. COMNAVRESFOR N00CT/COMNAVAIRFOR N43 shall:

(1) Ensure the OPSEC process is incorporated throughout the contract acquisition process and when a program’s CI or associated indicators are subject to adversary exploitation or unacceptable risk per references (a) and (b). Ensure and verify that contractors supporting Department of Defense activities use OPSEC to protect CI for specified contracts and subcontracts.
(2) Determine what OPSEC measures and requirements are essential to protect CI for specific contracts.

(3) Identify OPSEC measures in requirements documents.

(4) Ensure the Government Contracting Activity (GCA) identifies those OPSEC measures and requirements in the resulting solicitations and contracts.

(5) Establish procedures to verify contract requirements properly reflect OPSEC responsibilities and ensure those responsibilities are included in contracts determined to have CI. CI should be determined using references (a) through (c).

(6) Ensure publicly released documents and Statements of Work (SOW) do not reveal CI or CI indicators. If OPSEC planning is necessary in a contract, reflect the OPSEC requirements in the SOW. OPSEC Program Managers should review the SOW prior to public release.

g. Public Affairs shall:

(1) Review all information for OPSEC concerns, have the OPSEC manager/officer review as necessary, prior to releasing information to the public.

(2) Ensure unclassified, publicly available web sites do not include classified material, "For Official Use Only" information, proprietary information or information that could enable the recipient to infer this type of information.

(3) Periodically remind personnel that all government information must be approved by the PAO for public release prior to posting to any internet site.

(4) Balance the need to publicly release information to garner public support, foster community relations and help with the success of the Navy Reserve with the need to protect CI and CI indicators. The need for OPSEC should not be used as an excuse to deny non-CI to the public.

h. All Hands shall:

(1) Be familiar with their command or unit’s OPSEC program and procedures through:
(a) Orientation training as a part of the command check-in or command indoctrination program.

(b) Annual training through instructor training, NKO or CBT.

(2) Protect all CI by ensuring they, through their individual or collective actions, do not unintentionally convey indicators of operational intentions, capabilities or limitations.

(3) Ensure CI is not posted to social media. Contact the Command OPSEC Officer and/or Public Affairs Officer with any questions regarding the appropriateness of information intended for placement on social media sites. Guidelines and recommendations for using social media technologies in a manner that minimizes risk are located at https://www.chinfo.navy.mil/socialmedia.html, and the Chief Information Office Guidelines for Secure Use of Social Media by Federal Departments and Agencies, version 1.0 (http://www.doncio.navy.mil/Download.aspx?AttachID=11)

(4) Ensure unclassified, publicly available web sites do 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 or activity public affairs personnel and or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories. Guidelines for official Internet posts can be found in reference (d).

6. Annual OPSEC Program Reviews and Reporting Requirements. Per reference (c) each command will complete an annual review and evaluation of its OPSEC program and submit a report to their Immediate Superior in Charge (ISIC) OPSEC officer by 30 September of each fiscal year, reflecting the command's OPSEC posture as of 1 October of that year. Annual assessments shall be maintained for a minimum of 3 years. Enclosure (2) provides format and guidance. OPSEC program reviews include:

b. Annual review and validation of OPSEC plans and policies.

c. OPSEC assessment for evaluation of the command’s compliance with OPSEC plans and programs in an effort to appraise its OPSEC posture. The OPSEC assessment may be conducted with a small team of trained personnel from the command’s OPSEC working group.

d. OPSEC Surveys conducted to self-evaluate the command’s ability to apply the OPSEC methodology to operations. This evaluation should focus on the command’s ability to adequately protect CI from adversary intelligence exploitation during command planning, preparation, execution and post execution phases of any command operation or activity.

e. Command’s will forward the results of annual OPSEC surveys to the ISIC’s OPSEC Officer.

R. R. BRAUN

Distribution:
Electronic only, via COMNAVRESFOR Web site
https://www.navyreserve.navy.mil
Standard OPSEC Process

1. OPSEC Action 1 - Identification of Critical Information

   a. While assessing and comparing friendly versus adversary capabilities during the planning process for a specific operation or activity, the commander and staff seek to identify the questions that they believe the adversary will ask about friendly intentions, capabilities and activities. These questions are the Essential Elements of Friendly Information (EEFI).

   b. Critical information (CI) is a subset of EEFI. It is only that information that is vitally needed by an adversary. The identification of CI is important in that it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all classified or sensitive information.

2. OPSEC Action 2 - Analysis of Threats

   a. This action involves the research and analysis of intelligence information, counterintelligence, reports and open source information to identify who the likely adversaries are to the planned operation.

   b. The operations planners, working with the intelligence and counterintelligence personnel and assisted by the OPSEC program personnel, seek answers to the following questions:

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

      (2) What are the adversaries’ goals? (What does the adversary want to accomplish?)

      (3) What is the adversaries’ strategy for opposing the planned operation? (What actions might the adversary take?)

      (4) What CI does the adversary already know about the operation? (What information? Is it too late to protect?)

      (5) What are the adversaries’ intelligence collection capabilities?
c. Detailed information about the adversaries' intelligence collection capabilities can be obtained from the command's counterintelligence and intelligence organizations. In addition to knowing about the adversaries capabilities, it is important to understand how the intelligence system processes the information that it gathers.

3. OPSEC Action 3 - Analysis of Vulnerability

   a. Vulnerability analysis identifies operation or activity OPSEC vulnerabilities. It requires examining each aspect of the planned operation to identify any OPSEC indicators that could reveal CI and then comparing those indications with the adversaries intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it and then taking timely action.

   b. Continuing to work with intelligence and counterintelligence personnel, the operations planners seek answers to the following questions:

   (1) What indicators (friendly actions and open source information) of CI not known to the adversary will be created by the friendly activities that will result from the planned operation?

   (2) What indicators can the adversary actually collect?

   (3) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision and take appropriate action in time to interfere with the planned operation?)

4. OPSEC Action 4 - Assessment of Risk

   a. Assessing risk has two components. First, planners analyze the OPSEC vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Second, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.

Enclosure (1)
b. OPSEC measures reduce the probability of the adversary either collecting the indicators or being able to correctly analyze their meaning.

c. OPSEC measures can be used to:

   (1) Prevent the adversary from detecting an indicator.

   (2) Provide an alternative analysis of an indicator.

   (3) Attack the adversaries' collection system.

d. OPSEC measures include, among other actions, cover, concealment, camouflage, deception and intentional deviations from normal patterns.

e. More than one measure may be identified for each vulnerability. Conversely, a single measure may be used for more than one vulnerability. The most desirable OPSEC measures are those that combine the highest possible protection with the least impact on operational effectiveness.

f. Risk assessment requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

g. OPSEC measures usually entail some cost in time, resources, personnel or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then the application of the measure is inappropriate. The decision not to implement a particular OPSEC measure requires command involvement to evaluate level of risk.

h. Typical questions that might be asked when making this analysis include:

   (1) What risk to effectiveness is likely to occur if a particular OPSEC measure is implemented?

   (2) What risk to mission success is likely to occur if an OPSEC measure is not implemented?

   (3) What risk to mission success is likely if an OPSEC measure fails to be effective?
i. The interaction between OPSEC measures must be analyzed. In some situations, certain OPSEC measures may actually create indicators of CI. For example, the camouflaging of previously unprotected facilities could be an indicator of preparations for military actions.

j. The selection of measures must be coordinated with the other components of Command and Control Warfare. Actions such as jamming of intelligence nets or the physical destruction of CI centers can be used as OPSEC measures. Conversely, deception and Psychological Operations plans may require that OPSEC measures not be applied to certain indicators in order to protect a certain message to the adversary.

5. OPSEC Action 5 - Application of Appropriate OPSEC Measures

a. In this step, the command implements the OPSEC measures selected in Step 4 or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

b. During the execution of OPSEC measures, the reaction of adversaries to the measures is monitored to determine measure effectiveness and provide feedback. Planners use that feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback must be coordinated with the command's intelligence and counterintelligence staffs to ensure the requirements to support OPSEC receive the appropriate priority. In addition to intelligence sources providing feedback, OPSEC surveys can provide useful information relating to the success of OPSEC measures.

6. Step process

a. Identify CI - consists of the "core secrets" about an operation or plan needed by adversaries to disrupt or prevent mission accomplishment.

b. Analyze the threat - know the adversaries, their capabilities and intentions and information they require to meet their objective.

c. Analyze vulnerabilities - require a system analysis of operations, programs, activities and facilities from the adversaries' perspective to identify weaknesses (vulnerabilities) susceptible to exploitation.

Enclosure (1)
d. Analyze the risk - necessitate comprehension of the adversary threats to existing vulnerabilities and deciding whether adversary exploitation of each particular vulnerability warrants the application of one or more countermeasures.

e. Apply countermeasures - include the development and implementation of methods to eliminate existing vulnerabilities and/or disrupt adversary multi-discipline information gathering and processing capabilities.
Annual OPSEC Posture Assessment Report Format

1. Overview. Summarize the overall OPSEC posture of the command. Highlight strengths and weaknesses that will be addressed in greater detail in the following paragraphs.

   a. OPSEC plans and activities conducted during the reporting period. Focus on how the OPSEC process was applied within the command. Avoid emphasizing traditional security measures (e.g., visits to cryptographic materials security custodians, telephone monitoring, procuring secure telephones or improving access control to sensitive areas). Appropriate activities to report include: conducting OPSEC surveys, conducting training about OPSEC and status of establishing command OPSEC programs per references (a) through (d).

   b. Miscellaneous problems and recommendations. Address problems not specifically related to matters reported under paragraph a, but which impact the command's OPSEC posture (e.g., designs and operating procedures that hinder effective OPSEC when systems are operated and deficiencies in the OPSEC awareness of personnel before they report to the command). Recommend Chain of Command actions needed to correct problems.

   c. Forecast of OPSEC activities and objectives for the next reporting period. Emphasize activities such as those reported in paragraph a.

   d. OPSEC Officer. Name, rank, organizational element, Defense Switched Network telephone number and secure telephone number.

   e. OPSEC lessons learned. Present concise case studies in the following format (as appropriate, "sanitize" information to allow wide dissemination):

      (1) Title.

      (2) Observation. Concisely state the problem.

      (3) Discussion. Answer the "who," "what," "where," "when," "why" and "how" questions about the problem. If the problem could not be solved, explain why?

      (4) Lesson learned. State what positive action was taken to avoid or alleviate the problem.

Enclosure (2)
(5) Recommended action. State how to permanently correct the problem or enter "none required".

(6) Comments.