DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

OPNAVINST 3432.1A
N2/N6
4 Aug 2011

OPNAV INSTRUCTION 3432.1A

From: Chief of Naval Operations

Subj: OPERATIONS SECURITY

Ref: (a) CJCSI 3213.01C
(b) DoD Directive 5205.02 of 6 March 2006
(c) JP 3-13.3, Operations Security, 29 Jun 2006
(d) NTTP 3-54M/MCWP 3-40.9 of March 2009
(e) DoD 5205.02-M, DoD Operations Security (OPSEC) Program Manual, 3 November 2008
(f) DUSD(CIS) Memo of 27 Aug 2007 (NOTAL)

Encl: (1) Navy OPSEC Program Management Responsibilities and Governance

1. Purpose. To establish policy, procedures and responsibilities for the Navy Operations Security (OPSEC) program.

2. Cancellation. OPNAVINST 3432.1.

3. Applicability. The provisions of this instruction are applicable to the U.S. Navy, all contractors assigned to Navy activities, and all personnel conducting contracted service for the Navy (e.g., research, development, test and evaluation agencies and their contracted agents), effective on the date signed.

4. Background

a. OPSEC is a critical process for all Navy activities. The Department of Defense (DoD) has reaffirmed OPSEC practices must be followed in the daily application of military operations. The practice of OPSEC enables mission success by preventing inadvertent compromise of sensitive or classified activities, capabilities, or intentions at the tactical, operational and strategic levels. OPSEC processes provide commanders with the ability to identify critical information (CI), current vulnerabilities, risks due to its vulnerabilities, and countermeasure decision criteria to mitigate risks.

b. OPSEC is a core competency within information operations (IO). For commands planning at the strategic and operational levels, OPSEC processes provide an integrated conduit for protecting CI while disrupting, denying, and degrading the adversary’s attempts to gain an advantage. For commands at the tactical level executing plans and carrying out operations, proper utilization of OPSEC planning, tracking, and execution provides an increased probability of success by preventing the timely aggregation and analysis of CI required for the adversary to disrupt friendly actions.

c. Reference (a) identifies OPSEC as one of three key components for achieving operational surprise. The other two elements are security programs and counterintelligence. The important distinction between OPSEC and the others is that OPSEC is an operations function, not a security function. Additionally, OPSEC focuses on unclassified activities, information and vulnerabilities, whereas security functions (physical security, information security systems, etc.) are primarily directed towards the protection of classified material. As an operations function, OPSEC belongs in daily activity planning and must continually be revisited as a command’s mission and plans transform.

d. Properly applied, OPSEC contributes directly to operational effectiveness by withholding CI from an adversary, thereby forcing an adversary’s decisions to be based on information friendly forces choose to release. Inadequate OPSEC planning or poor execution degrades operational effectiveness by hindering the achievement of surprise. Excessive OPSEC countermeasures, however, can degrade operational effectiveness by interfering with the required activities such as coordination, training and logistical support. The OPSEC process recognizes that risk is inherent to all military activities. Proper use of the OPSEC process will achieve a balance, maximizing information security, while minimizing the impact on operations and planning requirements. The command and OPSEC planner must evaluate each operation to determine the most effective countermeasure(s) for implementation as balanced against operational requirements, timelines and budget.

5. Policy. The goal is to establish and implement the best OPSEC policies, procedures, processes and guidance to enable sustained superior performance and cost effective protection of Navy CI, people, operations, technology and sustainment. All Navy activities, installations, commands, and units shall institute and manage an OPSEC program relevant to mission and resources per references (a) through (f) and enclosure (1).

6. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy Manual 5210.1 of November 2007.

J. M. BIRD
Vice Admiral, U.S. Navy
Director, Navy Staff

Distribution:
Electronic only, via Department of the Navy Issuances Web site
http://doni.daps.dla.mil

NAVY OPSEC PROGRAM MANAGEMENT RESPONSIBILITES AND GOVERNANCE

1. Assigned Personnel. Per reference (b), all military, government civilian, and contractor personnel assigned to Department of the Navy activities, installations, commands, and units are responsible for compliance with this governance.

2. Commanders and Officers in Charge (OIC). All commanders, OICs, program executive offices, and program managers shall appoint an OPSEC program manager and or officer in writing. The designee will have insight to the full scope of the command's mission and may manage the OPSEC program full time or as a collateral duty.

3. OPSEC Program Managers and Officers. OPSEC program managers and officers will assist commanders and OICs in identifying CI per references (c) and (d). Commands will establish a formal OPSEC program per references (b), (d), and (e).

4. Specific Responsibilities. In addition to the responsibilities outlined above, the following specific responsibilities apply:

a. Chief of Naval Operations (CNO). CNO shall advise the Chairman of the Joint Chiefs of Staff concerning U.S. Navy OPSEC matters per references (a) and (c).

(1) The Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) shall:

(a) Have overall responsibility for development of Navy OPSEC policy. Act as the echelon 1 reporting agent for annual OPSEC data call to the Under Secretary of Defense for Intelligence (USD(I)), per reference (c).

(b) Act as the Navy representative to the Office of the Secretary of Defense, USD(I), the joint staff, other services and other DoD agencies regarding Navy OPSEC matters.

(c) Maintain the central point of contact for Navy OPSEC program concerns, including access to the electronic messaging account OPSEC@navy.mil.

(2) The Deputy Chief of Naval Operations for Manpower, Personnel, Training and Education (OPNAV N1) shall be the resource sponsor for billet allocation, personnel requirements and training requirements.

(3) The Special Assistant for Naval Investigative Matters and Security (OPNAV N09N) will coordinate and direct the Naval Criminal Investigative Service to provide counterintelligence support to the Navy OPSEC Support Team (NOST) during the planning and execution of Navy OPSEC assessments and surveys.

b. Commander, U.S. Fleet Forces Command and Commander, U.S. Pacific Fleet shall:

(1) Coordinate fleet-wide OPSEC requirements.

(2) Enter OPSEC lessons learned into the Navy Warfare Development Command (NAVWARDEVCOM) Lessons Learned Database (https://www.jllis.mil/navy/), which will be available to all unit OPSEC officers.

(3) Establish and fund an OPSEC support capability for the Navy per reference (b).

c. Commander, U.S. Fleet Cyber Command (COMFLTCYBERCOM) shall:

(1) Coordinate and administer the Navy OPSEC program and provide oversight regarding the execution of Navy OPSEC policy, doctrine, instruction and organizational program implementation. Maintain an OPSEC support capability for the Navy per reference (b) to include the NOST. The NOST is a subordinate element of Navy Information Operations Command (NIOC) Norfolk.

(2) Assist in the identification of CI, review program and facility OPSEC plans, and offer CI and OPSEC plan endorsement to cognizant OPSEC program managers and officers.

(3) Develop and coordinate a Navy OPSEC training program, to include:

(a) OPSEC orientation training within 60 days of reporting for duty.

(b) OPSEC awareness training at least annually to include review of the five step OPSEC process, CI list(s), current threats and vulnerabilities, site OPSEC plan, and results of OPSEC assessments and surveys.

(c) OPSEC planner training for individuals with OPSEC planning responsibilities.

(d) OPSEC training for naval reservists assigned to mobilization billets.

(4) Assist in the conduct of OPSEC self-assessments or formal OPSEC surveys as directed.

(5) Provide OPSEC planning assistance and guidance to fleet units.

(6) Identify and submit appropriate OPSEC lessons learned into the NAVWARDEVCOM lessons learned database. Solicit community best practices for consolidation and updating appropriate policy and tactics, techniques, and procedures (TTP).

(7) Consolidate annual status reports per table (1) of reference (f) from echelon 2 and 3 OPSEC program managers no later than 7 November of each year. Analyze and forward results to echelon 1 no later than 15 November of each year.

(8) Submit at least one suitable Navy candidate for the annual national OPSEC awards program to the national Interagency OPSEC Support Staff (IOSS) no later than 1 December of each year. Instructions for submitting the awards packages are located on the IOSS Web site: https://www.iad.gov/ioss/department/national-opsec-awards-10021.cfm.

(9) Act as the point of contact for Navy OPSEC program concerns, including primary monitoring of the electronic messaging account OPSEC@navy.mil.

d. Commander, Navy Installations Command shall direct the establishment of an OPSEC program for each installation and maintain guidance on the use of OPSEC for installation security programs, training exercises, and assessments.

e. The commander of the Office of Naval Research and the commanders of naval systems commands shall:

(1) Establish OPSEC program requirements for all research, development, testing and evaluation and science and technology programs under their cognizance. Training requirements will include, at a minimum, completion of IOSS OPSE-1301 (OPSEC Fundamentals Course) for research and acquisition managers.

(2) Ensure contracts and acquisition agreements include OPSEC guidance (e.g., mandatory policies and measures) related to programmatic information that may be publicly released. The systems commands will conduct a regular review of information released in the public forum (e.g., Web sites) to ensure compliance with all Navy message (ALNAV) 056/10.

(3) Conduct regular reviews of publicly accessible processes and information on contractor and government sites to determine if the aggregation of information for major programs constitutes an OPSEC disclosure.

(4) Evaluate technological capabilities and solutions to reduce OPSEC vulnerabilities, prevent unclassified CI exploitation, employ aggregate OPSEC analysis, and generate relevant, cost effective countermeasures.

f. Commander, Operational Test and Evaluation Force shall establish procedures and maintain guidance on the use of OPSEC to protect U.S. systems, capabilities, and tactics during operational test and evaluation.

g. Navy Inspector General (IG), in coordination with the DoD IG, shall develop and implement an OPSEC section of its inspection criteria. Once completed and updated, submit the inspection criteria to OPNAV N2/N6 for inclusion as an appendix to this instruction.

h. COMFLTCYBERCOM, with its subordinate command, NIOC Norfolk, is the primary review authority for IO doctrine, and maintains the Warfare Center of Excellence for IO. COMFLTCYBERCOM, via NIOC Norfolk, shall coordinate with NAVWARDEVCOM to ensure Navy OPSEC TTP’s are effective, relevant, and responsive to fleet requirements.

5. Navy Activities, Installations, Commands, and Units. Navy activities, installations, commands, and units will establish an OPSEC program per references (b) and (e), and will incorporate the principles and practice of OPSEC focused on command involvement, planning, assessments, surveys, training, education, threat, resourcing, and awareness. The appointed OPSEC program manager and or officer will complete core competency OPSEC training and execute the applicable requirements in references (a), (b), (c), (d) and (e), and will be a dedicated, qualified OPSEC individual assigned to develop and manage the OPSEC program. Based on the mission requirements, commanders will determine the requirement for full or collateral duty OPSEC program managers and officers, responsible for the following:

a. Coordinate and administer their command OPSEC program and execute their command OPSEC instruction per references (b), (c), (d), (e), and (g).

b. For commands with Secure Internet Protocol Router Network (SIPRNET) access, establish an account with the Operations Security Collaboration Architecture (OSCAR) program. This program was developed as an interactive tool for conducting an OPSEC assessment and incorporates intelligence information with user-supplied settings that reflect the current command environment. Assessment results can provide the commander with a snapshot of the unit’s current OPSEC posture (e.g., susceptibility to open-source adversary intelligence collection). Use of OSCAR annually will satisfy the annual assessment requirements as set forth in reference (b). Pertinent Web sites:

(1) OSCAR: https://oscar.dtic.smil.mil/oscar.

(2) OSCAR registration: https://register.dtic.smil.mil/wobin/WebOjects/RegLite?SiteID=OSCAR.

c. Determine command CI per references (b), (d), and (e). CI that has been fully coordinated within an organization and approved by the senior decision maker will be visible and used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

d. Ensure classified and unclassified contract requirements properly reflect OPSEC responsibilities and that these responsibilities are included in contracts when applicable per references (b) and (e).

e. Conduct annual self-assessments and surveys per references (b), (c), and (e). All Navy activities, installations, commands, functions and units shall complete an OPSEC assessment annually. Report completion of an assessment to the immediate senior in command's (ISIC) OPSEC program manager and the NOST.

f. Maintain a turnover binder and ensure OPSEC programs and plans are exercised or evaluated through regular assessments.

g. Obtain and evaluate the OPSEC plan per references (b), (d), and (e) for each cognizant program prior to any outdoor testing to ensure the best OPSEC policies, procedures, processes, and guidance for the cost effective protection of the test are in place.

h. Generate and submit an annual OPSEC program status report to the ISIC's OPSEC program manager and NOST no later than 1 November each year. The report format is listed in table 1 of reference (e).

i. Coordinate with other OPSEC program managers located on the same facility and or base to implement OPSEC awareness, training and assessments.

j. Lead internal local OPSEC working group meetings. An internal OPSEC working group should consist of at least one representative entitled "OPSEC coordinator" from each directorate, department or division, especially the following representatives: administrative, budgeting, communications, information systems, intelligence, logistics, operations, planning, programs, research, and security.

k. Provide OPSEC orientation and awareness training to assigned personnel. Ensure OPSEC awareness training is conducted at least annually.

l. Submit at least one suitable Navy candidate for the annual national OPSEC awards program to IOSS no later than 1 December of each year. Instructions for submitting the awards packages are located on the IOSS Web site: https://www.iad.gov/ioss/department/national-opsec-awards-10021.cfm.

m. OPSEC is a requirement throughout the acquisition process and when a classified or unclassified program's CI or associated indicators are subject to adversary exploitation or unacceptable risk per references (b) and (e). Additionally, ensure and verify that contractors supporting DoD activities use OPSEC to protect CI for specified contracts and subcontracts. The Navy and government contracting activity (GCA) shall impose OPSEC measures as contractual requirements by:

(1) Determining what OPSEC measures and requirements are essential to protect CI for specific contracts.

(2) Identifying those OPSEC measures in their requirements documents.

(3) Ensuring the GCA identifies those OPSEC measures and requirements in the resulting solicitations and contracts.

(4) Establishing procedures to verify contract requirements properly reflect OPSEC responsibilities and ensuring those responsibilities are included in both classified and unclassified contracts determined to have CI. CI should be determined using references (c), (d), and (e).

(5) Ensuring publicly released documents and statements of work (SOW) do not reveal CI or indicators of CI. 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.

(6) Ensuring recommended contractual documentation language is provided on the NOST Web site: http://www.nioc-norfolk.navy.mil/ (go to the OPSEC pull-down link on the homepage).

n. Develop a command OPSEC instruction per references (b) and (d).

(1) The content for a command OPSEC instruction is flexible but must at least address the requirements listed in reference (d) as well as any additional requirements assigned. Integrate OPSEC plans into the operational planning, including continuity of operations planning and research and technology protection processes to minimize adversary insight into operations, research and technology.

(2) OPSEC cannot be effectively employed alone, especially if the mission involves collocated or geographically separate partner organizations. Potential relationship vulnerabilities exist between the inputs and outputs of each organization’s planning processes and other functional processes for each organization, facility, compound, station or base. An effective OPSEC instruction will promote OPSEC plans to address all relevant vulnerability concerns and propose practical, cost effective measures to mitigate them. References (c) and (d) outline procedures to create OPSEC plans.

(3) OPSEC instructions will also establish formal review procedures for relevant OPSEC concerns such as: proposed public releases, onsite treaty inspections, to include the Open Skies Treaty per the Open Skies Readiness Plan (http://www.ntip.navy.mil/open_skies/documents/readiness.pdf). Requests for proposals and contracts involving classified or controlled unclassified information.

o. Unclassified, publicly available media and Web sites present a potential risk to personnel, assets, and operations if inappropriate information is published on Web sites. Program managers and officers will review command products for the following concerns:

(1) Unclassified, publicly available Web sites 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. Personnel are reminded that all government information must be approved by the commanding officer or OIC for public release prior to posting to any Internet site.

(2) Unclassified, publicly available Web sites 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 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 ALNAV 056/10.

(3) Public affairs is an important tool in garnering public support, fostering community relations, and helping with the success of military operations. Public knowledge of military operations is inevitable because of advanced technology and instant media coverage. Therefore, publicly accessible information must be considered from an adversary’s perspective prior to publication where media attention is expected or desired. The need for OPSEC should not be used as an excuse to deny non-CI to the public.

(4) The use of social media for Federal services and interactions is growing tremendously, supported by initiatives from the administration, directives from government leaders, and demands from the public. This situation presents both opportunity and risk. Navy personnel are encouraged to responsibly engage in the use of social media and social networking sites in an unofficial and personal capacity. Guidelines and recommendations for using social media technologies in a manner that minimizes the risk are located in ALNAV 056-057/10, U.S. Navy Chief of Information Social Media Web page (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=1105). If personnel have any questions regarding the appropriateness of information they intend to place on social media sites, they should contact their command OPSEC officer and command public affairs officer.