DEPARTMENT OF THE NAVY

NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

IN REPLY TO

NAVSEAINST 3432.1
Ser 00P/0053
28 Oct 08

NAVSEA INSTRUCTION 3432.1

From: Commander, Naval Sea Systems Command

Subj: NAVAL SEA SYSTEMS COMMAND (NAVSEA) OPERATIONS SECURITY (OPSEC) PROGRAM INSTRUCTION

Ref: (a) JP 3-13.3, OPSEC of 29 Jun 06
(b) DoDDIR 5205.02, DoD OPSEC Program of 06 Mar 06
(c) DoDINST 5200.39, CPI Protection Within the DoD of 16 Jul 08
(d) DoDINST 5000.2C, Implementation and Operations of the Defense Acquisition System and the Joint Capabilities Integration and Development System of 19 Nov 04
(e) DUSD(CIS) Review of DoD Component OPSEC Programs Memo of 27 Aug 07
(f) DON ASN(RDA)Required Use of Standardized Process for the Identification of CPI in DON Acquisitions Programs Memo of 20 Feb 08
(g) OPNAVINST 3432.1, OPSEC of 29 Aug 95
(h) NTTP 3-54.3, OPSEC of 01 Aug 05
(i) NAVSEAINST 5510.1B, NAVSEA Security Program of 05 Oct 07

Encl: (1) NAVSEA OPSEC Manual

1. Purpose. To update OPSEC policy and provide guidance for planning and implementing effective OPSEC programs throughout NAVSEA Headquarters, affiliated Program Executive Offices (PEO), and NAVSEA Field Activities.

2. Cancellation. NAVSEAINST 3070.1 including CH-1, 20 Oct 1992.

3. Objective. To establish and implement the best OPSEC policies, procedures, processes and guidance to enable the cost effective protection of NAVSEA critical information, people, technology, essential functions, and equipment.

4. Applicability. This instruction is the basic NAVSEA regulation governing OPSEC programs. All NAVSEA organizations will institute an OPSEC program relevant to mission and

resources in accordance with enclosure (1). This instruction applies to all military, government and on-site contractor personnel assigned to NAVSEA Headquarters, affiliated PEOs and NAVSEA Field Activities.

5. Action. All military, government civilian and on-site contractor personnel assigned to NAVSEA Headquarters, affiliated PEOs and NAVSEA Field Activities shall comply with the latest versions of enclosure (1) and references (a) - (i). This instruction is effective immediately.

K. M. MCCOY

Distribution:
SNDL A1J1L
A1J1M
A1J1N
A1J1P
FKA1G
A1J1Q
FKP
C84

NAVAL SEA SYSTEMS COMMAND

OPERATIONS SECURITY MANUAL

September 2008

Published by:

Office of Security Programs and Continuity Planning

NAVSEA 00P

FORWARD

The purpose of this NAVSEA OPSEC Manual is to update all relevant NAVSEA OPSEC polices in compliance with higher authority and implement the associated policies and procedures in a consistent and cost effective manner. We have developed this new manual using a new lean and efficient approach to maximize the use of website hyperlinks and eliminate unnecessary redundant language.

All personnel assigned to NAVSEA headquarters, affiliated PEOs and NAVSEA Field Activities (military, government civilian and on-site contractors) are responsible for implementing the provisions of this manual. It should be read in its entirety. Subordinate activities and detachments should use this manual as the basis for implementing their own OPSEC guidance. While traditional security programs focus on protecting classified information, OPSEC is concerned with identifying, controlling, and protecting unclassified evidence related with operations and activities. When implementing the provisions of this manual, it is important to remember effective OPSEC programs and practices will help prevent adversary exploitation but excessive secrecy inhibits our ability to conduct our own operations. OPSEC and security programs should be closely aligned to ensure appropriate aspects of operations, research and technology are protected.

Patrick J. Geary, OCP
Director, Office of Security Programs and
Continuity Planning (SEA 00P)

NAVSEA OPSEC MANUAL

Section 1: Responsibilities

1. Assigned Personnel. All military, government civilian and on-site contractor personnel assigned to NAVSEA Headquarters, affiliated PEOs and NAVSEA Field Activities in accordance with (IAW) reference (b) [para 2.1-3 and 4.3.4] are responsible for compliance with this manual.

2. Deputy Commanders, affiliated Program Executive Officers (PEOs) and NAVSEA Field Activities. Deputy Commanders and affiliated PEOs at NAVSEA headquarters shall ensure their Assistant Security Manager identified in reference (i) [Encl 1, CH 1, para 2] appoint an OPSEC Program Manager. Commanding Officers of NAVSEA Field Activities shall appoint an OPSEC Program Manager.

3. OPSEC Program Managers. OPSEC Program Managers will assist Deputy Commanders, affiliated PEOs and NAVSEA Field Activities in identifying Critical Information (CI) IAW references (a) [Ch 1, para 5.e.11] and (h) [Ch 3.3]. Commands with CI will establish a formal OPSEC Program IAW references (b) [para 2.4 and 5.3.1.1], (g) [para 5(a) and (b)] and (h) [App E and F].

4. The Director, Office of Security Programs and Continuity Planning (SEA 00P). The Director, SEA 00P serves as the OPSEC Officer to the NAVSEA Commander and is delegated the authority and responsibility for the effective management of the command OPSEC program. The Director, SEA 00P acts as the Commander's representative on all matters pertaining to command OPSEC and establishes, administers, oversees, implements and evaluates policy required for the Navy OPSEC Program throughout NAVSEA Headquarters, affiliated PEOs, and NAVSEA Field Activities for all military, government and on-site contractor personnel. SEA 00P may assign a full time Command OPSEC Program Manager responsible for administering but not necessarily limited to the following areas of responsibility:

a. Coordinate and administer the NAVSEA OPSEC Program and provide oversight regarding the execution of the NAVSEA OPSEC instruction.

b. Assist in the identification of CI and/or Critical Program Information (CPI); review program / facility OPSEC plans and offer CI, CPI and OPSEC Plan endorsement to cognizant Deputy Commanders, affiliated PEOs and NAVSEA Field Activities.

c. Review for OPSEC concerns: proposed headquarters public releases, Requests for Proposals (RFPs), Procurement Requests (PRs), treaties to include Open Skies Treaty and contracts involving classified or Controlled Unclassified Information (CUI).

d. Develop and coordinate an OPSEC training program for all NAVSEA employees to include those working at NAVSEA Headquarters, affiliated PEOs, and NAVSEA Field Activities consisting of:

(1) OPSEC Orientation Training within 60 days of reporting for duty at NAVSEA.

(2) OPSEC Awareness Training at least annually to include review of the five step OPSEC process, site CI list, site specific threats and vulnerabilities, site OPSEC Plan and results of OPSEC assessments and surveys.

(3) OPSEC Planner Training for individuals with OPSEC planning responsibilities.

(4) OPSEC Training for Naval Reservists assigned to mobilization billets.

e. Assist in the conduct of OPSEC self-assessments or formal OPSEC surveys as directed.

f. Provide Program Managers and facility heads with OPSEC planning and acquisition program protection assistance and guidance.

g. Lead regularly scheduled NAVSEA HQ OPSEC Working Group meetings to coordinate headquarters action, training and support. Additionally, lead quarterly OPSEC Working Group meetings with all appointed NAVSEA Headquarters, affiliated PEOs, and NAVSEA Field Activity OPSEC Program Managers.

h. Request support from the Commander, Naval Criminal Investigative Service (COMNCISCOM), Navy OPSEC Support Team (NOST) and other relevant agencies during the planning and execution of NAVSEA OPSEC assessments and surveys.

i. Identify and submit appropriate OPSEC lessons learned into the Navy Lessons Learned System (NLLS). OPSEC Officers may also provide generic lessons learned and best practices to the

Navy OPSEC Support Team (NOST) for consolidation and updating appropriate Policy and Tactics, Techniques, and Procedures (TTP).

j. Consolidate annual status reports IAW reference (e) [Encl 1] from subordinate OPSEC Program managers no later than 30 November. Analyze and forward results to COMNAVSEA on 15 December beginning 2009.

k. Submit at least one suitable NAVSEA candidate for the annual National OPSEC Awards program no later than 31 December of each year beginning 2009.

5. The Director, Scientific/Technical Intelligence Liaison Office (SEA 00G). The Scientific/Technical Intelligence Liaison Office (SEA 00G) is responsible for ensuring all matters relating to OPSEC requirements are met for command sensitive compartmented information (SCI)/special assess program (SAP) programs. Although SEA 00P is not responsible for handling or controlling SCI, there is great need for cooperation and coordination, especially regarding contractual matters.

6. The Director, Naval Sea Systems Command Inspector General (SEA 00N). The Command Inspector General (SEA 00N) is responsible for ensuring all matters relating to OPSEC requirements are met via Naval Sea Systems Command Performance and Compliance Inspections (NPCI) using the reporting guidance in figure 1 of Section 3 of this manual.

7. The Director, Naval Nuclear Propulsion Office (SEA 08). The Naval Nuclear Propulsion Office (SEA 08) is responsible for ensuring all matters relating to OPSEC requirements are met for activities under their cognizance.

8. NAVSEA Field Activities. NAVSEA Field Activities with CI will establish an OPSEC Program IAW references (b) [para 5.3] and (g) [para 5(a) and (b)] to 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 will execute the applicable requirements in references (a) [Ch 1, para 5.e], (b) [para 5.3], (c) [Ch 6, para g and h], (d) [Encl 3, para 3.8], (g) [para 6.c] and (h) [Ch 4, 6, 9; App F.1, K and L]. An OPSEC Program Manager will be a dedicated, qualified OPSEC individual assigned to develop and manage the commands'/units' OPSEC program. OPSEC Program Managers are responsible for the following:

a. Coordinate and administer their Command OPSEC program and execute their command OPSEC instruction according to references (a) [Ch 1, para 5.c], (b) [para 5.3.1], (e) [Encl 1], (g) [para 6.c and Encl 1], and (h) [Ch 3].

b. Determine Command CI and/or CPI IAW references (c) [Encl 3, para 6.q], (f) [Encl 1], (g) [Encl 1, para 2.a] and (h) [Ch 3.3 and App B, C and D].

c. Ensure contract requirements properly reflect OPSEC responsibilities and are included in contracts when applicable per references (b) [para 5.3.6] and (d) [Encl 3, para 3.8].

d. Conduct annual self-assessments and surveys per references (a) [Ch 1, para 5.e.6], (b) [para 5.3.1], (g) [para 6.c] and (h) [Ch 4].

e. Maintain a copy of each tenant command or detachment OPSEC plan and ensure plans are exercised through regular assessments.

f. Obtain and evaluate the OPSEC plan IAW references (b) [para 4.2 and 4.3] and (g) [Encl 1, para 2.e.2] 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.

g. Generate and submit an annual OPSEC Program status report to SEA 00P no later than 30 November each year beginning 2009 IAW the annual report format listed in Figure 1 of Section 3 of this manual.

h. Coordinate with other OPSEC Program Managers located on the same facility / base to implement OPSEC awareness, training and assessments.

i. Lead internal local OPSEC Working Group meetings and participate in quarterly SEA 00P 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.

j. Provide OPSEC Orientation and Awareness training to assigned personnel using SEA 00P guidance. OPSEC Awareness

Training will be conducted at least annually to all assigned personnel.

Section 2: OPSEC Instruction and OPSEC Plan Guidance

1. NAVSEA Field Activities shall develop a command OPSEC instruction IAW references (b) [para 5.3.1.3], (g) [para 5.a] and (h) [App E and F].

2. The format for a command OPSEC instruction is flexible but must at least refer to the information listed in reference (h) [App F] as well as any additional requirements assigned in Section 1 of this manual. Generic or specific planning guidance should amend the command OPSEC guidance. OPSEC plans will be integrated into the operational planning (including Continuity of Operations Planning (COOP)) and RTP processes to minimize adversary insight to operations, research and technology.

3. OPSEC can not 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 (a) [Ch 3] and (h) [App E and F] outline procedures to create OPSEC Plans.

4. OPSEC instructions will also establish formal review procedures for relevant OPSEC concerns: proposed public releases, RFPs, PRs, treaties including Open Skies Treaty and contracts involving classified or CUI.

Section 3: Annual OPSEC Report

1. All OPSEC programs will be self-evaluated annually IAW reference (b) [para 5.3.1.4]. Findings will be submitted to SEA 00P5 via email no later than 30 November beginning 2009 in the format prescribed in figure 1 of this manual.

[Area intentionally blank to facilitate 1 page checklist format]

Figure 1. OPSEC Program Review Checklist

ALL PURPOSE CHECKLIST				PAGE 1 OF 2 PAGES
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA Operations Security (OPSEC) Program Review Checklist	OPR	DATE		
#	ITEM	YES	NO	N/A
1.	Has the organization appointed in writing an OPSEC program manager or coordinator at the appropriate level? (DoDD 5205.02, paragraph 5.3.1.1.; DoDM 5205.02, Encl. 3.)			
2.	Is the organization OPSEC manager or coordinator someone who is familiar with the operational aspects of the activity including the supporting intelligence, counterintelligence, and security countermeasures? (DoDD 5205.02, paragraph 2.2.)			
3.	Has the OPSEC manager or coordinator completed the appropriate training? (DoDM 5205.02, Encl. 7.)			
4.	Does the organization utilize the Navy OPSEC Support Team (NOST) capability that provides for program development, training, assessments, surveys, and readiness training? (DoDD 5205.02, paragraph 5.3.1.2.) [NOST website]			
5.	Has the OPSEC manager or coordinator developed local OPSEC guidance (regulations or operating procedures) for use of the OPSEC analytic process? (DoDD 5205.02, paragraph 5.3.1.3.)			
6.	Has the OPSEC manager or coordinator conducted an annual review and validation of the organization's OPSEC program? (DoDD 5205.02, paragraph 5.3.1.4.; DoDM 5205.02, Encl. 3.)			
7.	Does the OPSEC manager or coordinator submit an annual report? (DoDD 5205.02, paragraph 5.3.1.4.)			
8.	Does the OPSEC manager ensure OPSEC assessments and surveys are conducted? (DoDM 5205.02, Encl. 4.)			
9.	Does the OPSEC manager or coordinator provide sufficient support for subordinate units he or she has oversight for? (DoDD 5205.02, paragraph 5.3.1.5.)			
10.	Is the OPSEC manager or coordinator involved in the review process of information intended for public release? (DoDM 5205.02, Encl. 5.)			
11.	Has the organization ensured that critical information is identified and updated as missions change? (DoD 5205.02, paragraph 5.3.4.)			
12.	Has the OPSEC manager or coordinator established, implemented, and maintained effective OPSEC education activities to include initial orientation and continuing and refresher training for assigned members? (DoDD 5204.02, paragraph 5.3.5.; DoDM 5205.02, Encl. 7.)			
13.	Does the OPSEC manager ensure OPSEC is included in force protection planning and local exercises when applicable? (DoDD 5205.02, paragraph 4.2.)			
14.	Does the OPSEC manager work with CIP planners to identify critical information related to CIP? (DoDM 5205.02, Encl. 3.)			
15.	Are assigned personnel aware of the organization's critical information? (DoDM 5205.02, Encl. 3.)			
16.	Has the OPSEC manager supplemented DoDD 5205.02 and DoDM 5205.02 and issued procedures for:			
	a. Integrating OPSEC planning into the planning, development, and implementation stages of net-centric programs and operating environments? (DoDM 5205.02, Encl. 2.)			
	b. Conducting OPSEC assessments and surveys? (DoDD 5205.02, paragraph 5.3.2.; DoDM 5205.02, Encl. 4.)			
	c. Handling, safeguarding, and destroying critical information? (DoDM 5205.02, Encl. 5.)			
	d. A formal review of content for classification, sensitivity, sensitivity in the aggregate, determination of appropriate audience, and distribution and release controls when releasing information? (DoDD 5205.02, paragraph 5.3.3.; DoDM 5205.02, Encl. 5.)			
	e. Ensuring contract requirements properly reflect OPSEC requirements when appropriate? (DoD 5205.02, paragraph 5.3.6.; DoDM 5205.02, Encl. 6.)			

Section 4: Assessments and Surveys

1. OPSEC self-assessments and surveys enable an evaluation of OPSEC program effectiveness from an adversary's perspective. Self-assessments are internal examinations conducted by a command, using its own personnel. A formal survey involves formation of a survey team with members from inside and outside the command being surveyed. References (a) [App D], (g) [para 6.c.1], and (h) [Ch 4, 6 and 7] outline requirements and procedures for assessments and surveys.

2. A concise summary of the findings will be debriefed to the site Commander before the evaluation team departs. If required, a formal report will be provided within 14 days. Findings belong to the evaluated command and specifics are not forwarded except for security violations. Generic findings, i.e. need additional shredders, need OPSEC Program Manager to attend formal training, etc. will be reported via the annual OPSEC Report to capture NAVSEA performance metrics. Results and corrective "Plans of Action" from any self-assessment and/or OPSEC Survey, if not classified, meet the definition of sensitive unclassified information or CUI under exemption (b)(5) of the Freedom of Information Act. Findings will be safeguarded as FOR OFFICIAL USE ONLY information at a minimum IAW SECNAVINST 5720.42E.

3. Commands requesting self-assessment assistance and/or a survey will submit requests to SEA 00P5 via email. The request will include the purpose, scope, proposed dates and name of the appointed OPSEC Program Manager. SEA 00P will assist in scheduling and obtaining participating personnel from outside of the NAVSEA Command.

Section 5: OPSEC in Contracts

1. OPSEC will be considered throughout the acquisition process and is required when a program's CI or associated indicators are subject to adversary exploitation or unacceptable risk IAW references (b) [para 5.3.6], (d) [Encl 3, para 3.4.7.5 and 3.8] and (g) [para 6.j]. Deputy Commanders, affiliated PEOs and NAVSEA Field Activities shall ensure contractors supporting DoD activities use OPSEC to protect CI for specified contracts and subcontracts. The requiring NAVSEA organization and Government Contracting Activity (GCA) shall impose OPSEC measures as contractual requirements by:

a. Determining what OPSEC measures and requirements are essential to protect CI for specific contracts.

b. Identifying those OPSEC measures in their requirements documents.

c. Ensuring the GCA identifies those OPSEC measures and requirements in the resulting solicitations and contracts.

2. NAVSEA Deputy Commanders, affiliated PEOs and NAVSEA Field Activities shall establish procedures to verify contract requirements properly reflect OPSEC responsibilities and ensure those responsibilities are included in both classified and unclassified contracts determined to have CI. CI should be determined using references (a) [Ch 2, para 2.a and App A] and (h) [Ch 3.3].

3. Publicly released documents and SOW's can reveal CI or indicators of CI. If OPSEC planning is necessary in a contract, the OPSEC requirements shall be reflected in the SOW performed. OPSEC Program Managers should review the SOW prior to public release.

4. Recommended contractual documentation language is provided on the Navy OPSEC Support Team (NOST) website: https://www.nioc-norfolk.navy.mil/operations/opsec/main.shtml.

Section 6: OPSEC and the Research and Technology Protection Program

1. Identifying and ensuring protection of sensitive technologies and related information is vital to maintaining the US advantage against current and future potential adversaries. Reference (d) [Encl 3, para 3.4.7.5 and 3.9.1] requires all DoD acquisition Program Managers (PM) to identify Critical Program Information (CPI) in their respective program prior to Milestone (MS) A. Reference (f) [para 3] directs NAVSEA PMs to utilize the DON standardized CPI identification process.

2. After the CPI is determined, a Program Protection Plan (PPP) or Abbreviated PPP will be developed IAW reference (f), Encl 1.