



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

IN REPLY REFER TO

OPNAVINST 3432.1  
N513  
29 August 1995

OPNAV INSTRUCTION 3432.1

From: Chief of Naval Operations

Subj: OPERATIONS SECURITY

- Ref: (a) Joint Pub 1, 10 Jan 95, Joint Warfare of the US Armed Forces (U) (NOTAL)  
(b) CJCS MOP 30, 8 Mar 93, Command and Control Warfare (NOTAL)  
(c) CNO letter N513J/5S608233 dated 15 Feb 95 (NOTAL)  
(d) CJCSI 3213.01, 28 May 93, Joint Operations Security  
(e) Joint Pub 3-54, 22 Aug 91, Joint Doctrine for Operations Security (NOTAL)  
(f) DODI 5000.2, 23 Feb 91, Defense Acquisition Management Policy and Procedures (NOTAL)  
(g) DOD Manual 5200.1-M, 16 Mar 94, Acquisition Systems Protection Program (NOTAL)  
(h) OPNAVINST 3430.25, 1 Apr 94, Information Warfare and Command and Control Warfare (NOTAL)  
(i) OPNAVINST 3430.26, 18 Jan 95, Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W) (NOTAL)

Encl: (1) The OPSEC Process

1. Purpose. To issue Navy guidance for operations security (OPSEC).
2. Cancellation. OPNAVINST 3070.1A, OPNAVINST S3430.21A, and report symbol OPNAV 3070-1.
3. Scope. This instruction sets forth guidance on the conduct of U.S. Navy OPSEC by appropriate Navy commands.
4. Background
  - a. OPSEC is a critical component of U.S. Navy activities. Reference (a) states "maintaining the operations security of



29 AUG 1995

plans and gaining the fullest possible surprise" are essential to maintaining freedom of action. The practice of OPSEC prevents the inadvertent compromise of sensitive or classified activities, capabilities, or intentions at the tactical, operational, and strategic levels. OPSEC measures are required:

(1) For those operations and activities relating to the equipping, preparation, deployment, sustainment, and employment of the U.S. Navy in time of war, crisis or peace that require the maintenance of essential secrecy; and

(2) For the protection of the information contained in Operations Plans, Operations Orders, and supporting plans and orders.

b. OPSEC in Command and Control Warfare.

(1) Command and Control Warfare (C2W) is the integrated use of operations security (OPSEC), military deception (MILDEC) psychological operations (PSYOP), electronic warfare (EW), and physical destruction, all mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions. C2W is the action taken by the military commander to realize the practical effects of Information Warfare (IW) on the battlefield.

(2) C2W is a warfighting strategy that takes advantage of the synergistic effects achievable through the integrated use of the five C2W tools. Each C2W tool can be employed independently, but their integrated use gives a commander the ability to neutralize all elements of the adversary's C2 system simultaneously and in a coordinated manner. Each tool can be used to enhance the effectiveness of the other tools.

(3) While EW and destruction directly target an adversary's ability to command its forces, OPSEC seeks to degrade the quality of the adversary's decisions by hindering the ability of an adversary's intelligence system to gather critical information. By concealing one's own capabilities and intentions from the adversary, OPSEC creates the opportunity for surprise. MILDEC and PSYOP enhance the effectiveness of OPSEC when used to fill the information void created in the adversary's intelligence

29 AUG 1995

system by implementation of OPSEC. This synergism is a vital element of properly conducted information warfare (IW).

(4) Joint policy guidance for the integration of MILDEC, OPSEC, PSYOP, EW, and physical destruction into a C2W strategy is provided in reference (b). U.S. Navy Policy Planning Guidance on C2W is provided by reference (c), a joint Chief of Naval Operations/Commandant of the Marine Corps letter on IW/C2W.

c. OPSEC, Security, and Counterintelligence. As outlined in reference (d), OPSEC is one of three components that maintains the secrecy essential to achieving surprise. The other two elements are security programs and counterintelligence. The distinction between OPSEC and the other two elements is important. **OPSEC is not a security function, it is an operations function.** OPSEC and security programs are mutually supporting. Neither is exclusively responsible for maintaining secrecy, and both must be successful for secrecy to be preserved.

(1) The OPSEC process identifies and controls critical information that indicates friendly intentions, capabilities, and activities.

(2) Security Programs deny classified information to adversaries. These programs include physical security, personnel security, information security, and information systems security (INFOSEC).

(3) Counterintelligence programs support both security and OPSEC programs by identifying intelligence threats and methods of an adversary. Counterintelligence can also assist OPSEC planners by emulating foreign intelligence collection capabilities to assess OPSEC vulnerabilities. This is especially important where counterintelligence analysts assemble a coherent picture from indicators, profiles and patterns that may compromise a program, plan, or operation.

d. OPSEC and Operational Effectiveness. Properly applied OPSEC contributes directly to operational effectiveness by enhancing the probability that an adversary is surprised or makes bad decisions due to a lack of critical information on friendly forces and equipment.

29 AUG 1995

(1) Inadequate OPSEC degrades operational effectiveness by hindering the achievement of surprise. Excessive OPSEC can degrade operational effectiveness by interfering with required activities such as coordination, training, and logistic support.

(2) Proper use of the OPSEC process will minimize the conflicts between operational and security requirements. The OPSEC process recognizes that risk is inherent to all military activities. The commander or program manager must evaluate each operation and determine the balance between OPSEC measures and operational needs.

e. OPSEC and the Public. The requirement for the practice of OPSEC must be balanced against what reference (a) states is the responsibility of the Armed Forces to account for their actions "with the American people whom we serve." The need to practice OPSEC should not be used as an excuse to deny noncritical information to the public.

5. Policy. Essential secrecy for friendly intentions, capabilities, technologies, plans, and activities will be maintained by naval forces through the use of OPSEC measures prior to, during, and after operations and other potentially vulnerable activities. OPSEC measures will also be applied to research and system development, testing, evaluation, and acquisition programs from the establishment of a requirement through initial operational capability to maintain essential secrecy of friendly developments, capabilities, and tactics. An OPSEC program will be required for those commands or programs that have critical information, but will not be required for commands or programs that do not possess such information. This instruction allows Echelon 2 commanders to determine where OPSEC programs are required in subordinate commands and where they are not required. Echelon 2 commanders will be able to delegate this determination responsibility to subordinates where appropriate. The intention is to create an OPSEC program everywhere it is required, while avoiding an administrative burden on those commands for whom an OPSEC program is unnecessary.

a. OPSEC Program. Each Navy command and staff that possesses critical information in accordance with enclosure (1), as determined by their Echelon 2 commander, will establish a formal OPSEC program. This program will support the commander by ensuring that the command or staff actively practices OPSEC to

29 AUG 1995

deny critical information to any potential adversary. Those organizations involved in joint operations will consider joint OPSEC in the development of their programs. An OPSEC program provides for planning, training, education, threat identification, evaluation, and correction of vulnerabilities. The commander must be actively involved in OPSEC, particularly in defining OPSEC goals and planning guidance, and in making decisions regarding the balance of operational and security needs.

b. Navy operational OPSEC programs will incorporate, but are not limited to, the elements of the OPSEC process outlined in enclosure (1). Reference (e), from which enclosure (1) is extracted, describes in detail joint doctrine on OPSEC. Command programs should be prepared, where appropriate, to implement that doctrine. Navy research, development, testing, evaluation, and acquisition programs shall incorporate, but are not limited to, the OPSEC applications referred to in references (f) and (g).

## 6. Responsibilities

a. CNO will advise the Chairman of the Joint Chiefs of Staff concerning U.S. Navy OPSEC matters in accordance with references (d) and (e). Specifically, in accordance with references (h) and (i):

(1) The Deputy CNO (DCNO) (Plans, Policy and Operations) (N3/N5) will:

(a) Have overall responsibility for development of service OPSEC policy.

(b) Act as the Navy representative to the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff (JCS)/Joint Staff, the other Services, and other agencies regarding Navy OPSEC matters.

(c) Serve as the Navy-wide joint OPSEC program officer.

(d) Coordinate Navy participation, when required, in joint OPSEC Executive Groups (OEG) established by the Joint Staff.

29 AUG 1995

(2) The Director of Space and Electronic Warfare (N6), in his capacity as the primary Service coordinator and point of contact for Information Warfare/Command and Control Warfare (IW/C2W), is the resource sponsor for Service INFOSEC equipment.

(3) The Director of Naval Intelligence (N2) will act as focal point for intelligence support to all aspects of OPSEC training, planning, execution, and feedback. His responsibility as focal point includes coordinating and directing Office of Naval Intelligence support to Navy OPSEC, and coordinating national intelligence community support for Navy OPSEC.

(4) The Special Assistant for Naval Investigative Matters and Security (NO9N) will coordinate and direct Naval Criminal Investigative Service (NAVCRIMINVSERV) counterintelligence support to Navy OPSEC programs, and will coordinate national intelligence community counterintelligence support for Navy OPSEC.

b. Navy Echelon 2 Commands are assigned responsibility for determining which of their subordinate commands possess critical information, and will direct those subordinate commands to establish formal OPSEC programs and conduct OPSEC surveys as required. This authority may be delegated to subordinate commands.

c. Navy commands directed to establish a formal OPSEC program will:

(1) Conduct OPSEC surveys as required in support of command operations.

(2) Conduct annual OPSEC program reviews.

(3) Incorporate OPSEC into all operations and operational planning activities.

(4) Provide OPSEC training to all personnel.

d. Naval Component Commanders. Naval Component Commanders, in addition to the requirements on all Echelon 2 Commands, will:

(1) support OPSEC programs of their Unified CINCs; and

29 AUG 1995

(2) provide guidance to fleet units on OPSEC considerations during training evolutions which use methods, equipment or tactics that require special consideration.

e. Commander, Naval Doctrine Command. Commander, Naval Doctrine Command (COMNAVDOCCOM), in coordination with the CNO and the Naval Component Commanders, is assigned responsibility for development of Service doctrine for OPSEC that meets the requirements of the Naval Component Commanders.

f. Fleet Information Warfare Center. The Fleet Information Warfare Center (FIWC) is assigned responsibility for providing OPSEC assistance to Naval Component Commanders in accordance with reference (i).

g. Office of Naval Intelligence. The Office of Naval Intelligence (ONI) will, in coordination with the Navy Criminal Investigative Service (NAVCRIMINSERV), support Navy OPSEC programs. ONI and NCIS will conduct analysis of the intelligence collection threat from foreign nations and organizations for use in OPSEC planning and for monitoring the effectiveness of implementing OPSEC measures.

h. Naval Criminal Investigative Service. The Naval Criminal Investigative Service (NAVCRIMINSERV) will support Navy OPSEC programs through the conduct of counterintelligence operations to detect, deter, neutralize or exploit foreign intelligence collection activities against Navy organizations and activities.

i. Commander, Operational Test and Evaluation Force. The Commander, Operational Test and Evaluation Force (COMOPTEVFOR) will establish guidance on the use of OPSEC to protect U.S. systems capabilities and tactics during operational test and evaluation.

j. The Systems Command's Acquisition Systems Protection Working Group (SASPWG), in its role as the coordinating group for OPSEC protection efforts in the Navy acquisition community, shall advise the CNO (N3/N5) as needed on matters concerning the application of OPSEC in the Navy research, development, testing, evaluation, and acquisition programs environment.

29 AUG 1995



**T. C. LYNCH**

**DIRECTOR, NAVY STAFF**

Distribution:

SNDL A2A (Department of the Navy Staff Offices) (Chief of Naval Research and Department of the Navy Program Information Center, only)

A6 (Headquarters, U. S. Marine Corps (15))

B2A (Special Agencies, Staffs, Boards, and Committees) (DIA, JCS, and DIRNSA, only)

B3 (College and University) (Armed Forces Staff College, only)

B5 (U. S. Coast Guard)

21A (Fleet Commanders in Chief)

22A (Fleet Commanders)

23 (Force Commanders)

24 (Type Commanders)

26A (Amphibious Group)

26F (Operational Test and Evaluation Force and Detachment)

26H (Fleet Training Group)

26J (Afloat Training Group and Detachment)

26YY (Fleet Ocean Surveillance Information Center and Facility)

26HHH (Command and Control Warfare Group and Detachment)

26KKK (Tactical Training Group)

28A (Carrier Group)

28B (Cruiser Destroyer Group)

28C (Surface Group and Force Representatives)

28D (Destroyer Squadron)

28J (Combat Logistics Groups, Squadrons and Support Squadrons)

28K (Submarine Group and Squadron)

28L (Amphibious Squadron)

29 AUG 1995

Distribution (Continued):

SNDL 29 (Warships)

31 (Amphibious Warfare Ships)

32A (Destroyer Tender) (AD)

32C (Ammunition Ship) (AE)

32G (Combat Store Ship) (AFS)

32H (Fast Combat Support Ship) (AOE)

32Q (Replenishment Oiler) (AOR)

32KK (Miscellaneous Command Ship) (AGF)

42A (Fleet Air Commands)

42B (Functional Wing Commanders)

42D (Fleet Aviation Specialized Operational Training Group)

42E (Type Wing Commanders)

42J (Carrier Air Wing) (CVW, CVWR)

42N (Sea Control Squadron)

42P (Patrol Wing and Squadron)

42X (Fleet Air Reconnaissance Squadron) (VQ)

42Z (Tactical Electronic Warfare Squadron)

42CC (Helicopter Anti-Submarine Squadron, Light)

42DD (Carrier Airborne Early Warning and Squadron)

45A (Fleet Marine Force Commands and Marine Expeditionary Force)

45B (Marine Division)

45O (Light Antiaircraft Missile Battalion + Headquarters + Services Battery)

45R (Communication Battalion)

45V (Expeditionary Brigade and Unit)

45FF (Radio Battalion)

46 (Fleet Marine Force-Aviation) (46B, 46C, 46D, 46F, 46H, 46M, 46P, 46T, 46U, 46V, 46Y, only)

50A (Unified Commands) (USCINCPAC, USCINCLANT, and USCINCCENT only)

50D (Components of Unified Commands) (CINCUSNAVEUR, COMUSNAVCENT)

50G (Activities of Unified Commands) (LANTJIC (2) and JICPAC (2), only)

C3 (To Naval Personnel at DoD or other Government agencies) Officer in Charge Navy Element Joint Electronic Warfare Center, and U. S. Navy Element USEUCOM Joint Intelligence Center, only)

D3A (Navy International Programs Office)

E3A (Laboratory ONR) (Naval Research Laboratory, only)

OPNAVINST 3432.1

29 AUG 1995

Distribution (Continued):

SNDL FA30 (Weapons Training Facility)  
FE1 (Security Group Headquarters)  
FE4 (Security Group Activity) (Naples, IT, Kami Seya,  
JA, and Charleston, SC, only)  
FF42 (Navy Postgraduate School)  
FF44 (Naval War College)  
FKA1A Air Systems Command  
FKA1B Space and Naval Warfare Systems Command  
FKA1C Facilities Engineering Command  
FKA1F Supply Systems Command  
FKA1G Sea Systems Command  
FKA8 Activities Under the Command of DIRSSP  
FKM Shore Activities Under the Command of  
COMNAVSUPSYSCOM  
FKN Shore Activities Under the Command of  
COMNAVFACENCOM  
FKP Shore Activities Under the Command of  
COMNAVSEASYSYSCOM  
FKQ Shore Activities Under the Command of  
COMSPAWARSYSCOM  
FKR Shore Activities Under the Command of  
COMNAVSPACECOM  
FS Shore Activities Under the Command of ONI  
FT1 (Chief of Naval Education and Training)  
FT Shore Activities Under the Command of CNET  
FU Shore Activities Under the Command of the Military  
Assistant to the President  
FX Shore Activities Under the Command of MSC  
W Department of the Navy Echelon 2 Activities

Copy to:

OPNAV (N2, N3/N5, N51, N513 (25), N64, N091)  
SNDL C25A (OPNAV Support Activity Detachment) (Ft. Ritchie,  
only)

SECNAV/OPNAV Directives Control Office  
Washington Navy Yard Bldg 200  
901 M Street SE  
Washington DC 20374-5074 (3)

OPNAVINST 3432.1

**29 AUG 1995**

Order from:  
Naval Inventory Control Point  
Cog "I" Material  
700 Robbins Avenue  
Philadelphia, PA 19111-5099

Stocked: 50 copies

29 AUG 1995

The OPSEC Process1. General

a. OPSEC planning is accomplished through the use of the OPSEC process. This process provides the information required to write the OPSEC section of any plan or order. OPSEC planning is done in close coordination with the overall C2W planning effort and with the planning of the other C2W components.

b. The OPSEC process consists of five distinct actions. These actions are applied in a sequential manner during OPSEC planning. In dynamic situations, however, individual actions may be revisited at any time. New information about the adversary's intelligence collection capabilities, for instance, would require new analysis of threats.

c. An understanding of the following terms is required before the process can be explained:

(1) Critical information: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

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

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

2. The OPSEC Process

a. OPSEC Action 1--Identification of Critical Information.

(1) 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

Enclosure (1)

29 AUG 1995

friendly intentions, capabilities, and activities. These questions are the essential elements of friendly information (EEFI). In an operation plan or order, the EEFI are listed in Appendix 3 (Counter-intelligence) to Annex B (Intelligence).

(2) Critical information is a subset of EEFI. It is only that information that is vitally needed by an adversary. The identification of critical information 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.

(3) Critical information is listed in the OPSEC portion of an operation plan or order. Examples of critical information are provided in reference (d).

b. OPSEC Action 2--Analysis of Threats.

(1) 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.

(2) The operations planners, working with the intelligence and counterintelligence staffs and assisted by the OPSEC program personnel, seek answers to the following questions:

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

(b) What are the adversary's goals? (What does the adversary want to accomplish?)

(c) What is the adversary's strategy for opposing the planned operation? (What actions might the adversary take?)

(d) What critical information does the adversary already know about the operation? (What information is it too late to protect?)

(e) What are the adversary's intelligence collection capabilities?

(3) Detailed information about the adversary's intelligence collection capabilities can be obtained from the command's counterintelligence and intelligence organizations. In addition to knowing about the adversary's capabilities, it is important to understand how the intelligence system processes the information that it gathers. Reference (d) discusses the general characteristics of intelligence systems.

c. OPSEC Action 3--Analysis of Vulnerability.

(1) This action identifies an operation's or activity's OPSEC vulnerabilities. It requires examining each aspect of the planned operation to identify any OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's 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.

(2) Continuing to work with the intelligence and counterintelligence staffs, the operations planners seek answers to the following questions:

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

(b) What indicators can the adversary actually collect?

(c) 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?)

(3) Reference (d) contains a detailed discussion of OPSEC indicators.

d. OPSEC Action 4--Assessment of Risk.

(1) This action has two components. First, planners analyze the OPSEC vulnerabilities identified in the previous

Enclosure (1)

29 AUG 1995

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.

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

(a) 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 adversary's collection system.

(b) OPSEC measures include, among other actions, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the adversary's intelligence system.

(c) More than one possible 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.

(d) Reference (d) provides examples of OPSEC measures.

(3) 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.

(a) 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

Enclosure (1)

29 AUG 1995

inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires command involvement.

(b) 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?

(c) The interaction of OPSEC measures must be analyzed. In some situations, certain OPSEC measures may actually create indicators of critical information. For example, the camouflaging of previously unprotected facilities could be an indicator of preparations for military actions.

(4) The selection of measures must be coordinated with the other components of C2W. Actions such as jamming of intelligence nets or the physical destruction of critical intelligence centers can be used as OPSEC measures. Conversely, deception and PSYOP plans may require that OPSEC measures not be applied to certain indicators in order to project a specific message to the adversary.

e. OPSEC Action 5--Application of Appropriate OPSEC Measures

(1) 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.

(2) During the execution of OPSEC measures, the reaction of adversaries to the measures is monitored to determine their effectiveness and to 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

Enclosure (1)

OPNAVINST 3432.1

**29 AUG 1995**

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 successes of OPSEC measures.

Enclosure (1)