DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
914 CHARLES MORRIS CT SE
WASHINGTON NAVY YARD DC 20398-5540

REFER TO:

COMSCINST 3070.1A
N3/5
17 July 2000

COMSC INSTRUCTION 3070.1A

Subj: OPERATIONS SECURITY (OPSEC) PLAN

Ref: (a) OPNAVINST 3432.1
(b) DoD 5220.22-M, National Industrial Security Program Operating Manual
(c) Joint Pub 3-54, Joint Doctrine for Operations Security

Encl: (1) Operations Security Guidance for Contractors
(2) Essential Elements of Friendly Information
(3) The OPSEC Process

1. Purpose. To update the Operations Security (OPSEC) plan for Military Sealift Command (MSC) in accordance with references (a) and (b). This instruction is a complete revision and should be read in its entirety.

2. Cancellation. COMSCINST 3070.1.

3. Scope. The provisions of this instruction apply to the MSC organization, world wide, including ships of the MSC Force. To ensure integrity of operations, Naval Fleet Auxiliary Force (NFAF), Special Mission ships, Prepositioned ships and Strategic Sealift ships while under the operational control of other commands, will operate under the provisions of that Commander's OPSEC Plan.

4. Policy

a. MSC will conduct an aggressive OPSEC Program designed to improve mission effectiveness through the identification and elimination of potential OPSEC vulnerabilities. OPSEC is not a security function; it is an operations function. The practice of OPSEC prevents the inadvertent compromise of sensitive or classified activities, capabilities or intentions at the tactical, operational and strategic levels. In order to conduct an effective OPSEC Program, all assigned personnel and contractors must understand the concept of OPSEC and apply that knowledge and awareness in their day-to-day performance of assigned tasks. Therefore, it is essential that all military and civilian personnel receive appropriate OPSEC training.

b. All MSC and contractor personnel will undergo OPSEC training in accordance with references (a) and (b) and enclosure (1).

c. OPSEC measures will be employed at all times to preserve essential secrecy. Enclosure (2) contains a list of Essential Elements of Friendly Information (EEFI) which may require security protection depending upon the existing situation.

d. All MSC commands shall appoint in writing a designated OPSEC Officer. For MSC Headquarters, this function is performed by the Intelligence Officer (N311D).

5. Responsibilities

a. MSC commands will:

(1) Appoint an OPSEC Officer, normally from their Operations Directorate.

(2) Conduct annual OPSEC plan reviews.

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

(4) Provide OPSEC training to all personnel.

b. MSC Area Commanders will:

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

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

6. Action

a. Each MSC Area Commander will establish an OPSEC plan in accordance with reference (c) and as outlined in enclosure (3). A copy of plans will be provided to COMSC N3/5.

b. The COMSC Contracting Officer and MSC Area Command Contracting Officers will ensure OPSEC requirements are stated in requests for proposals (RFPs) and classified contracts in accordance with reference (c). The development and submission to the Contracting Officer of OPSEC requirements for inclusion in RFPs/contracts is the responsibility of the code originating the contractual requirement. Enclosure (1) discusses OPSEC measures required of DoD contractors.

c. The COMSC Comptroller will program funds for the conduct of formal OPSEC surveys of MSC commands and operations.

d. COMSC and MSC Area Commanders will conduct periodic OPSEC surveys of subordinate units, ashore and afloat.

e. All newly assigned/employed military/civilian personnel will receive an OPSEC orientation briefing conducted by the appropriate MSC Security officer (MSCHQ/Area Command) within 60 days after reporting to duty at MSC.

f. All MSC personnel are required to attend annual OPSEC orientation/ familiarization in accordance with this instruction. The OPSEC Officer will provide/ arrange this training.

g. Area Commanders, Commanding Officers, Officers in Charge and Headquarters Program Managers/Functional Directors/Special Assistants will ensure compliance with the provisions of this instruction.

"Signed"
G. S. HOLDER

Distribution:
COMSCINST 5215.5
List I (Case A, B, C)

SNDL	41B	(MSC Area Commanders)
	41C	(NFAF East/West)
	41D	(MSC Offices)
	41E	(APMC)
	41J	(OICMILDEPTs)
	41K	(APSRON FOUR)
	41L	(COMPSRONs)
	41M	(MSC TAGOS Project Office & Det)
	T-100	(Masters, civil service manned ships)
	T-102	(Masters & Operators, Fast Sealift Ships)
	T-103	(Masters & Operators, TAGOS)
	T-104	(Masters & Operators, MPS)
	T-105	(Masters & Operators, LMSRs)
	T-106	(Masters & Operators, Prepo Ships)

MSC Reserve Units
MSC Reps
All MSC Chartered Ships

OPERATIONS SECURITY GUIDANCE FOR CONTRACTORS

1. OPSEC measures are required of contractors when:

a. Administrative, technical and physical actions they may execute incident to a classified contract may result in indicators in open sources of information and detectable activities, and

b. Foreign intelligence collection against those open sources of information and detectable activities may result in foreign countries obtaining indicators that permit them to derive classified information.

2. The existence of the above situation must be determined prior to issuance of requests for proposals (RFPs) or contracts. To accomplish this, an OPSEC estimate will be prepared (by the requestor with the assistance of that organization's OPSEC Officer) when a requirement to issue an RFP or contract involving classified information is identified, with the exception of contracts that are limited to classified materials, such as:

a. Contracts to process or evaluate information and produce classified documents, pictures, computer programs, training materials and other similar matters.

b. Contracts for classified consultant services.

c. Contracts for library or ADP services related to classified materials.

d. Contracts for printing classified documents.

3. Care must be taken not to confuse requirements for OPSEC measures with requirements for information, physical, communications or personnel security contained in reference (b). Industrial Security Manual measures are automatically required of all contractors executing classified contracts.

4. A contract effort that requires the use of OPSEC measures may result in classification requirements additional to those of other contracts. These additional requirements may include such things as:

a. Indications of when and where activities will occur (such as tests) that can be targeted by foreign intelligence to obtain indicators that must be protected (collection opportunities).

b. The duration of a contract and indications of results (such as in ads, status reports and brochures).

c. The existence of a contract, services involved and what is being developed in U.S. press releases, stock prospective, etc.

d. Pictures indicating classified design features or approaches.

e. The lettering of contracts and identity of sub-contractors.

5. To ensure uniformity in the way OPSEC requirements are presented to industry, the following guidance shall be followed:

a. Guidance will be appended to basic RFPs or contracts and labeled: "OPSEC Requirements."

b. OPSEC guidance will include:

(1) EEFI pertinent to contractual activities.

(2) Essential secrecy to be maintained and statement of harm if adversaries derive accurate estimates.

(3) Specific OPSEC measures:

(a) Controls over administrative actions in addition to those in the Industrial Security Manual to keep indicators from appearing in open sources of information.

(b) Controls over technical and physical actions, in addition to encryption and TEMPEST (electronic security measures program), to keep indicators from appearing in detectable activities, such as electromagnetic or acoustic emissions and observable physical matters.

(c) Covers or other deceptive methods to explain indicators that result from actions necessary to execute contracts.

(d) Countermeasures against collection systems.

(4) Requirements for an OPSEC plan for activities that will occur at contractor owned facilities.

(5) Requirements for coordinated DON-contractor OPSEC planning for activities that will occur at DON or other DOD facilities, indicating who is responsible for preparing plans.

(6) Support for DON in providing upon request, help to contractors preparing OPSEC plans and executing OPSEC measures, including multi-disciplinary counterintelligence threat information and OPSEC survey support.

(7) Specific OPSEC measures Defense Investigative Service should examine during periodic security investigations. The project security officer will inspect all contracts for contractor compliance.

6. Contractors shall provide all cleared employees with security training and briefings commensurate with their involvement with classified information.

a. Contractors may obtain defensive security, threat awareness and other education and training information and material from the appropriate MSC Security Officer or other DoD sources.

b. Contractors shall be responsible for ensuring that personnel performing security duties, complete security training deemed appropriate by the Cognizant Security Administrative (CSA) office. The CSA is responsible for providing initial security briefings and for ensuring that other briefings required for special categories of information are provided.

c. Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

(1) A threat awareness briefing;

(2) A defensive security briefing;

(3) An overview of the security classification system;

(4) Employee reporting obligations and requirements; and

(5) Security procedures and duties applicable to the employee’s job.

d. The contractor shall conduct periodic refresher briefings for all cleared employees. As a minimum, the refresher briefing shall reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. The use of audio/video materials and issuance of written materials on a regular basis may satisfy this requirement.

e. Contractors shall debrief cleared employees at the time of termination of employment (discharge, resignation or retirement) or when an employee’s security clearance is terminated, suspended or revoked.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

1. The following list of Essential Elements of Friendly Information (EEFI) is provided as a guideline in the development of specific EEFIs for a given operational activity. This list is not all inclusive and should be changed and updated whenever necessary.

a. Information which reveals the specific capabilities or operational readiness of MSC Force ships.

b. Information which reveals a weakness of a specific ship, activity, etc., which could represent a compromise of the ship or activity mission.

c. Information regarding scheduling and routing of ships.

d. Information that reveals manifest data or loading/discharge ports.

e. Information which reveals security weakness within MSC or organizational activities.

f. Information which reveals security classification of various projects, operation or exercises.

g. Associations of a particular cover name or nickname with a classified project, operation or exercise.

h. Information which reveals special requirements for specific duty which could indicate deployment location or mission, such as:

(1) Special immunization requirements;

(2) Specific language requirements;

(3) Other than routine security procedures;

(4) Additional survival or mobility training;

(5) Special passport, visa and other foreign clearance requirements; and

(6) Special or civilian clothing requirements.

i. Information which reveals a special ship operation.

j. Effectiveness of MSC Command and Control Information System under stress; its vulnerabilities to countermeasures.

k. MSC Command and Control Information System interfaces with other commands and its effectiveness.

l. MSC Force size.

m. MSC Force ships' ability to support U.S. Navy theater commanders during crisis/ hostilities.

2. The EEFI should be used for the following purposes:

a. To assist in assigning the proper classification to specific items and to provide guidelines for downgrading when appropriate.

b. For guidance to staff agencies responsible for document, communications, electronic and physical security in their respective areas and for protecting mission sensitive data.

c. By OPSEC officers to analyze the significance of each planned action and activity in the operational, intelligence, administrative, logistics, communications and maintenance areas.

THE OPSEC PROCESS

1. 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 Command and Control Warfare (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 indications 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 friendly intentions, capabilities and activities. These questions are the 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.

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.

c. OPSEC Action 3 - Analysis of Vulnerability

(1) 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 critical information and then comparing those indications 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?)

d. OPSEC Action 4 - Assessment of Risk

(1) 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.

(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 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.

(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 inappropriate. The decision not to implement a particular OPSEC measure requires command involvement to evaluate level of risk.

(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 between 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 Psychological Operations (PSYOP) plans may require that OPSEC measures not be applied to certain indicators in order to protect a certain 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 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.