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

REFER TO:

COMSCINST 4385.1C
N00I
26 March 2003

COMSC INSTRUCTION 4385.1C

Subj: DETECTION AND PREVENTION OF FRAUD, WASTE AND MISMANAGEMENT

Ref: (a) SECNAVINST 5430.92A
(b) SECNAVINST 5370.5A
(c) COMSCINST 5040.2D
(d) COMSCINST 5200.9
(e) COMSCINST 5000.22
(f) SECNAVINST 7700.7
(g) SECNAVINST 5200.34D
(h) COMSCINST 5730.2E

Encl: (1) Operational and Business Risk Management (ORM)

1. Purpose. To affirm command support for Department of the Navy (DON) policy to detect, deter and counteract fraud, waste and mismanagement within the service. Reference (a) assigns program responsibility. This instruction is a complete revision and should be read in its entirety.

2. Cancellation. COMSCINST 4385.1B.

3. Background. In 1978, the President's Council on Integrity and Efficiency took the initiative to improve government operations and eliminate inefficiencies. DON responded to this program by reemphasizing existing programs of audit, inspection and internal review, reaffirming the traditional chain of command structure and by assigning authority, responsibility and accountability to Commanding Officers ashore and afloat. Concerted efforts by all personnel to actively support integrity and efficiency programs continue in this era of significant fiscal constraints.

4. Policy. It is Military Sealift Command (MSC) policy to effectively manage assigned resources, free from fraud, waste and inefficiency. MSC personnel at all levels, ashore and afloat, shall take aggressive action to manage these resources, take the initiative to improve procedures when necessary and promptly correct identified problems. Top level managers shall set the example for the staff. Abuses of authority, misconduct, fraudulent use of resources and mismanagement will result in prompt corrective action.

5. Discussion

a. Fraud, waste and mismanagement of resources divert already limited assets from essential programs and initiatives, increase operating costs and reduce the effectiveness of support provided to our forces ashore and afloat. All personnel must maintain high standards of conduct to ensure the special public trust and confidence placed in them continues.

b. Some incidents of fraud and mismanagement may be blatant and obvious. Other cases may only be detected through the systematic review and audit of programs or activities. Therefore, every employee must be vigilant when conducting day-to-day business. Reference (b) provides information on the hotline referral program.

6. Action

a. COMSC shall:

(1) Establish an aggressive assessment program to ensure a periodic review of operations aboard ship and at subordinate activities ashore.

(2) Establish a proactive Management Control Program (MCP) to provide continuous self-assessment of programs and procedures to include a risk management assessment of work processes using the guidance found in enclosure (1).

(3) Establish clear, attainable objectives for the Annual Management Guidance and long-range strategic plans.

(4) Establish and conduct a program to emphasize Standards of Conduct and personal accountability, in accordance with reference (a).

(5) Maintain a Command Evaluation Program (CEP) to provide prompt positive recognition of material weaknesses and management control shortfalls and to take swift corrective action when employees are not meeting established standards of performance and conduct.

b. COMSC Inspector General shall:

(1) Implement and administer references (b) through (e) for COMSC.

(2) Provide semi-annual reports (reference (f)) and semi-annual follow-up reports (reference (g)), as applicable.

(3) Coordinate with COMSC Comptroller (N8/N85) to ensure compliance with reference (h) on the release of specific information.

c. Program Managers/Functional Directors/Special Assistants/Area Commanders shall take action and/or support the actions outlined in subparagraphs 6a and 6b to include

(1) Provide semi-annual reports on audits, internal reviews and inspections to COMSC Inspector General, when directed.

(2) Complete and report corrective action recommended in assessments, inspections, audits and investigations when tasked. Report management control shortfalls as material or non-material weaknesses in accordance with reference (d).

7. Reports. The reporting requirements described in this instruction are exempt from report control in accordance with OPNAVINST 5214.7.

//S//
J. M. STEWART
Vice Commander

Distribution:
COMSCINST 5215.5
List I (Case, A, B, C)
SNDL 41B (MSC Area Commanders)

Copy to:
NAVINSGEN

OPERATIONAL AND BUSINESS RISK MANAGEMENT (ORM)

1. MSC military personnel and civil servants assess operational risk as defined in OPNAVINST 3900.39A in their daily routine. ORM is process oriented and is flowcharted in OPNAVINST 3900.39A.

2. In order to optimize MSC business practices, especially to control loss from fraud, waste and mismanagement, MSC personnel must incorporate business risk management into daily routine.

3. COMSCINST 5200.9 (MCP) provides for incorporation of ORM into all work processes.

4. To ensure business risk management is included in ORM at MSC, all personnel will use the following definition for "Hazard" when applying OPNAV ORM guidance:

> Hazard - any event or occurrence with the potential to cause personal injury or death, property damages or jeopardizes the achievement of the organization's mission.

5. At a minimum, consider these ORM Risk types in Assessable Unit management:

a. Safety as emphasized in ALNAV 063/02 and ALNAV 001/02.

b. Financial risk defined as loss of assets including loss through fraud or waste through inefficient use of resources, or available operating or capital budget.

c. Technological risk to achieving work process entitlement because systems and technology tools through design or operation does not allow optimum achievement of mission.

d. Human Resources risk evaluated to determine if management and staff are sufficient to meet the needs of the process.

e. Operational risk considered from the perspective of policies/laws constraining process improvement or instructions insufficient to understand how to properly execute a process.

f. Reputation risk assessment will consider the level of public interest and if execution of a process will negatively affect public opinion.

g. Strategic risk assessment as ORM will deconflict and prioritize a given process with the executing of other processes and ensure DON objectives are met in execution of the process.