Report No. D-2007-040 January 2, 2007

Inspector General

United States
Department *of* Defense

The General and Application Controls over the Financial Management System at the Military Sealift Command

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

BIA	Business Impact Analysis
CCR	Configuration Change Request
CM	Configuration Management
COMSC	Commander, Military Sealift Command
COMSCINST	Commander, Military Sealift Command Instruction
DITSCAP	DoD Information Technology Systems Certification and Accreditation Program
FMR	Financial Management Regulation
FMS	Financial Management System
IA	Information Assurance
ICCR	Internal Configuration Change Request
IT	Information Technology
MCDC	Military Sealift Command Corporate Data Center
MCP	Mission Continuity Plan
MSC	Military Sealift Command
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
SSAA	System Security Authorization Agreement

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

January 2, 2007

MEMORANDUM FOR THE NAVAL INSPECTOR GENERAL

SUBJECT: Report on the General and Application Controls over the Financial Management System at the Military Sealift Command (Report No. D-2007-040)

We are providing this report for review and comment. In preparing the final report, we considered the comments received from the Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller).

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) comments were partially responsive (see the Management Comments Required table at the end of the finding sections). As a result of management comments, we revised recommendations E.3. and H.1.b. to clarify the intent of the recommendations. Therefore, we request that the Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) provide comments on the final report to include corrective actions and milestones by February 1, 2007.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to **AUDCLEV@dodig.mil**. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Edward A. Blair at (216) 706-0074 ext. 226 or Gregory M. Mennetti at (216) 706-0074 ext. 267. See Appendix B for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Paul J. Granetto, CPA
Assistant Inspector General and Director
Defense Financial Auditing Service

Department of Defense Office of Inspector General

Report No. D-2007-040 **January 2, 2007**
(Project No. D2005-D000FC-0247.000)

The General and Application Controls over the Financial Management System at the Military Sealift Command

Executive Summary

Who Should Read This Report and Why? DoD personnel who manage and use the Financial Management System will find this report of interest. DoD information assurance program supervisors may also find the report useful. It discusses whether the Financial Management System's general and application controls were adequately designed and operating effectively.

Background. To support the Department's goal to achieve auditability, the Department of Defense Office of Inspector General launched a long-range strategy to conduct audits of DoD financial statements. The reliability of information in Military Sealift Command Financial Management System directly impacts the Military Sealift Command and the Department of the Navy's ability to produce reliable, and ultimately auditable, financial statements, which is key to achieving the goals of the Chief Financial Officers Act of 1990 (Public Law 101-576). This audit was conducted to assist the Military Sealift Command and the Department of the Navy in identifying and strengthening controls over Military Sealift Command Financial Management System to improve the reliability of financial information.

The Financial Management System is an accounting information system that accumulates and reports financial data for the Military Sealift Command. The Financial Management System provides support for fund and obligation control, budget execution and expenditure accounting, reimbursable accounting, miscellaneous accounting (disbursements and collections), general ledger control, and financial reporting.

Results. We identified several internal control weaknesses that were critical to the operations of the Military Sealift Command. The weaknesses found were related to entity-wide security program planning and management (finding A), access controls (finding B), software development and change controls (finding C), system software (finding D), segregation of duties (finding E), service continuity (finding F), authorization (finding G), and accuracy (finding H). The deficient controls created system vulnerabilities that potentially jeopardize the integrity, confidentiality, and availability of data reported by the Financial Management System. The Commander, Military Sealift Command must address these vulnerabilities as required by Federal and DoD criteria outlined in the report. See the finding sections of the report for detailed recommendations.

We also reviewed the managers' internal control program as it related to the Financial Management System. The Military Sealift Command managers' internal control program did not identify the control weaknesses.

Management Comments and Audit Response. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) comments were partially responsive and generally concurred with the audit findings and the intent of all except one recommendation.

The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred in principle with the recommendation requiring vacations or job rotations for those employees with “privileged” access to the Financial Management System. They are currently reexamining the entire process as it relates to strong internal controls over system access. They are also working toward eliminating “privileged” access to the extent possible. The Director concurred in part with the recommendation to incorporate the New Employee Form used in assigning and documenting responsibilities in the Financial Management System. They are currently revising the New Employee Form for Financial Management System access to advise the Financial Systems Office of the specific system duties to be performed by the requestor. We revised this recommendation to include a brief description of the employee’s specific duties within the New Employee Form for use in assigning and documenting responsibilities within the Financial Management System. The Director concurred in part to the recommendation requiring accuracy checks and periodic testing of validation and edit checks of calculated data. He disagreed with the periodic testing portion of the recommendation because the Financial Management System is an Oracle commercial-off-the-shelf software package certified by the Joint Financial Management Improvement Program that they have not customized. We revised this recommendation to clarify our intent and believe actions should be taken because modifications to software increase project risk exponentially, therefore, the additional control of periodically testing critical computations would provide a control to mitigate the risk of the system being altered without detection.

We request that the Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) comment on this report by February 1, 2007. See the Finding sections of the report for a discussion of management comments and the Management Comments sections for the complete text of the comments.

Table of Contents

Findings

Appendixes

Management Comments

Background

To support the Department's goal of achieving auditability, the Department of Defense Office of Inspector General launched a long-range strategy to conduct audits of DoD financial statements. The Chief Financial Officers Act of 1990 (Public Law 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements. The reliability of information in Military Sealift Command (MSC) Financial Management System (FMS) directly impacts the MSC and Department of the Navy's ability to produce reliable, and ultimately auditable, financial statements; which is key to achieving the goals of the Chief Financial Officers Act of 1990 (Public Law 101-576). The audit provided an evaluation of the general and application controls over FMS.

The Financial Management System. MSC FMS was implemented from Oracle E-Business Suite 11i, a commercial-off-the-shelf core accounting product, in July 2000. The applications in Oracle E-Business Suite 11i use a unified data model that allows storage of transactions, business intelligence, and financial assets in one place. Oracle E-Business Suite 11i was tested and certified as Joint Financial Management Improvement Program compliant. The Sun Solaris v5.8 operating system houses the FMS production application. FMS accumulates and reports financial data for MSC in addition to providing support for fund and obligation control, budget execution and expenditure accounting, reimbursable accounting, miscellaneous accounting (disbursements and collections), general ledger control, and financial reporting.

Mission and Functions at MSC Headquarters Washington Navy Yard, D.C. MSC is composed of approximately 10,800 civilian and military personnel with various locations worldwide and provides transportation services to the Armed Forces. The mission of MSC is to provide ocean transportation of equipment, fuel, supplies, and ammunition to sustain U.S. forces worldwide during peacetime and in war for as long as operational requirements dictate. MSC provides the sea transportation component for the United States Transportation Command. MSC is financed through two working capital funds, the Navy Working Capital Fund and the Transportation Working Capital Fund. This means MSC is a fee-for-service organization and earns money through products and services provided to their customers. MSC receives funding from the Armed Services for providing these logistics and shipping services. The cost of MSC operations in FY 2005 exceeded $3.1 billion.

Command, Control, Communications, and Computer Systems Directorate. The Command, Control, Communications, and Computer Systems Directorate (Computer Systems Directorate) department is tasked with oversight of the application of technical solutions for FMS. The Computer Systems Directorate mission is to direct and manage the development of capital planning and investment strategy; the implementation of the requirements of the Government Performance and Results Act with respect to Information Technology; the development and application of electronic commerce tools and electronic data interchange policies, practices, standards, and procedures; and the execution of Computer Systems Directorate programs. The Computer Systems Directorate is also required to validate the implementation of appropriate physical access controls, technical security measures, classification, and safeguarding of controlled information rules. The Computer Systems Directorate Director of Operations is responsible for managing information technology (IT) infrastructure for MSC organizations, including MSC connectivity for the Internet, client-server mainframe systems, and Headquarters site classified and unclassified operations, including the MSC Corporate Data Center (MCDC). The Computer Systems Directorate Director of Engineering is responsible for controlling the integration and engineering of IT solutions by issuing policy, overseeing the IT program, performing Database and Systems Administration functions, and maintaining and operating databases and applications systems including FMS.

Financial Management Analysis Division, Comptroller Directorate. The Financial Management Analysis Division, Comptroller Directorate (Comptroller Directorate) is tasked with oversight and creating functional solutions for the financial system. The Comptroller Directorate mission is to study, develop, and implement financial data systems, research and implement changes in financial systems; ensure conformance with prescribed policies and procedures relating to financial management and internal controls; act as liaison for internal and external audit groups; follow up on the status of actions to be taken on recommendations contained in audit reports; and coordinate training in the financial management area. The Comptroller Directorate employs the functional administrators for FMS.

MSC Corporate Data Center. The MCDC is located in Building 196 on the Washington Navy Yard. Space and Naval Warfare Systems Center provides MSC with space in Building 196 for the MCDC. The MCDC is the workspace of MSC contractors tasked with the administration of FMS, which resides on a server in the MCDC lab room. The MCDC provides problem resolution, research and development, expert advice, and trouble call tracking services to MSC. The primary objectives of the MCDC are to:

- establish and maintain a support center that provides global information and infrastructure services;
- provide services to various developers, data warehouse, and consulting staff members;
- enforce the MSC configuration management standards;
- plan effectively for the introduction of new products and upgrades; and
- establish and maintain a high standard of support.

The Computer Systems Directorate provides Government oversight for the contractors in the MCDC.

Objectives

The overall objective was to determine whether the general and application controls over the FMS at the MSC were adequately designed and operating effectively. We also evaluated the managers' internal control program at the MSC as applicable to the audit objectives. See Appendix A for a discussion of the scope and methodology and prior coverage related to the objectives.

Review of Internal Controls

DoD Directive 5010.38, "Management Control Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control Program Procedures," August 28, 1996,[1] require DoD managers to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Managers' Internal Control Program. We reviewed the adequacy of the general and application controls, and management's self-evaluations of those controls, over the FMS at the MSC.

Adequacy of Internal Controls. We identified material control weaknesses as defined by DoD Instruction 5010.40. MSC internal controls did not ensure that an entity-wide security program plan and management was properly documented and enforced. In addition, MSC did not ensure that access controls were adequately designed or operating effectively, software change controls were adequately implemented, system software controls were adequately designed and operating effectively, segregation of duties principles were properly enforced, service continuity plans were designed and tested for effectiveness, and the application controls in place were working effectively and efficiently.

- **Entity-Wide Security Program Plan and Management**. MSC internal controls did not ensure that the entity-wide security program plan was compliant with OMB Circular A-130, Appendix III, "Security of Federal Automated Resources," and DoD 8510.1-M, "DoD Information Technology Systems Certification and Accreditation Program (DITSCAP)," July 31, 2000. In addition, MSC did not ensure that the security management structure was adequately documented, the checkout process for separating employees was properly enforced, and the effectiveness of the security program was adequately being monitored. Recommendation A.1., if implemented, will bring the Enterprise and FMS System Security Authorization Agreements (SSAA) into compliance with OMB and DoD guidance. Recommendation A.2. and A.3., if implemented, will strengthen controls over the security management structure. Recommendation A.4., if implemented, will strengthen controls over the employee check-out process. Recommendation A.5., if implemented, will provide a means for tracking and correcting previously identified vulnerabilities.

[1] Our review of internal controls was done under the auspices of DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996. DoD Directive 5010.38 was canceled on April 3, 2006. DoD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," was reissued on January 4, 2006.

- **Access Controls**. MSC internal controls did not ensure that the list of authorized users was current, physical controls over the MCDC were adequate, fire suppression system was routinely inspected and properly maintained, FMS password parameters enforced DoD strong passwords, privileged user accounts were adequately controlled, and system logon functions locked users out of FMS after three unsuccessful logon attempts. Recommendation B.1., a. through b., if implemented, will strengthen controls for maintaining an active user account list for FMS. Recommendation B.2., a. through b., if implemented, will increase the effectiveness of the physical access controls over the MCDC. Recommendation B.3., if implemented, will provide assurance that the fire suppression system over FMS system servers is properly maintained and working correctly. Recommendation B.4., if implemented, will improve controls for user accountability in FMS. Recommendation B.5., if implemented, will initiate a system change to comply with DoD minimum password requirements in DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003. Recommendation B.6., if implemented, will mitigate the risk of unauthorized individuals accessing the system.

- **Software Development and Change Control.** MSC internal controls did not ensure that processing features and program modifications were adequately documented; revised software was adequately documented, tested, and approved; and software libraries were adequately controlled. Recommendation C.1., if implemented, will provide a process for documenting, authorizing, and approving each phase of all software changes. Recommendation C.2., and C.3., a. through d., if implemented, will document and develop an audit trail for all configuration change. Recommendation C.4., a. through c., if implemented, will strengthen controls for software libraries and software migration.

- **System Software.** MSC internal controls did not ensure that system administrator access was properly authorized, the administrator account was controlled, and system software utilities were appropriately used and monitored. Recommendation D.1., if implemented, will strengthen the controls over the authorization of access to system software by system personnel. Recommendation D.2., if implemented, will increase the evidence of an audit trail for the 'root' administrator account. Recommendation D.3., if implemented, will satisfy the requirement set forth in OMB Circular A-123, "Management's Responsibility for Internal Control," July 2005. Recommendation D.4., if implemented, will strengthen controls over MCDC personnel activities.

- **Segregation of Duties.** MSC internal controls did not ensure that segregation of incompatible duties was taking place, job descriptions were adequately documented, operating procedures for both system configuration and operational use were clearly documented, and proper supervision of MCDC personnel activity within FMS was conducted. Recommendation E.1., if implemented, will increase assurance that users are not assigned incompatible responsibilities in FMS. Recommendation E.2., if implemented, will decrease the risk of fraud and raise awareness of segregation of duties principles and practices. Recommendation E.3., if implemented, will strengthen controls over authorization of a user's responsibilities in FMS. Recommendation E.4., a. through c., if implemented, will increase assurance that operating procedures for system configuration and operational use are clearly documented. Recommendation E.5., if implemented, will satisfy the requirement set forth in Commander, Military Sealift Command Instruction 5239.3A, "Military Sealift Command Information Assurance Policy," October 14, 2003.

- **Service Continuity.** MSC internal controls did not ensure that emergency processing priorities were properly established; a proper data and program backup process was implemented; adequate environmental controls were implemented; staff were trained for emergency situations; steps were taken to ensure the prevention and minimization of potential damage and interruption of the system in the event of a contingency; and fully develop, document, and test a comprehensive contingency plan. Recommendation F.1., if implemented, will increase assurance that the MSC Mission Continuity Plan (MCP) is consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002. Recommendation F.2., a. through c., if implemented, will strengthen controls over backups of FMS data. Recommendation F.3., if implemented, will increase assurance that the environmental control devices over MSC resources are maintained and working properly. Recommendation F.4., if implemented, will strengthen controls over emergency processing procedures and increase personnel awareness of their responsibilities in the event of an emergency. Recommendation F.5., if implemented, will increase assurance that information systems are performing adequately and an alternate data processing site is available in the event of an emergency. Recommendation F.6., if implemented, will satisfy requirements set forth in DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, requiring a Mission Assurance Category II system to be operational within 24 hours of an emergency. Recommendation F.7., if implemented, will increase controls over manual processing procedures in the event of an emergency. Recommendation F.8., if implemented, will increase the effectiveness of teleworking capabilities in the event of an emergency.

- **Authorization.** MSC internal controls did not ensure that all fuel transactions were supported by source documents and were reviewed by a third party. Recommendation G.1., if implemented, will strengthen controls and provide an audit trail over recording fuel purchasing transactions.

- **Accuracy.** MSC internal controls did not ensure that data entry design features contributed to the accuracy of financial data, transaction errors were reviewed after corrections had been made, and sensitive financial reports were protected from unauthorized access. Recommendation H.1., a. through b., if implemented, will strengthen controls over data accuracy in FMS.

A copy of the report will be provided to the Commander of the Military Sealift Command.

Adequacy of Management's Self-Evaluation. Management performs self-evaluations to identify the processes used for conducting day-to-day operations. Management self-evaluations did not identify all of the material control weaknesses found during this audit. This occurred because the self-evaluations did not review those specific areas as part of their processes used for conducting business. Therefore, MSC did not identify or report all the material internal control weaknesses found by the audit.

A. Entity-Wide Security Program Planning and Management

MSC did not adequately design entity-wide security program planning and management general controls to operate effectively. Specifically, MSC did not document a complete entity-wide security program; establish the security management structure; comply with security related personnel procedures; and monitor the effectiveness of the information system security program. MSC did not adequately:

- document the security plan because management did not follow OMB and DoD policies,
- establish the security management structure because management did not follow policies and procedures that require documentation of an organization chart and appointment letters,
- comply with security-related personnel procedures because the checkout procedure was not enforced, and
- monitor the effectiveness of the information system security program because management did not plan and approve corrective actions for recommendations.

As a result, the security planning and internal control weaknesses increase the risk to information systems security.

Entity-Wide Security Program Planning and Management Controls

A program for security planning and management is the foundation of an entity's security control structure. The program should establish a framework and continuing cycle of activity for assessing risk, developing, implementing, and monitoring effective security procedures. MSC did not adequately design and document controls over information systems security planning and management.

Entity-Wide Security Program Plan

MSC did not document a complete information systems security program plan. The Enterprise SSAA documents the unclassified and classified local area networks, Afloat Network Operations Center, MCDC, and selected MSC applications; and was provided as the general support system security program plan. The FMS SSAA documents the financial application, and was provided as the major application security program plan. OMB Circular A-130, Appendix III, "Security of Federal Automated Resources," and DoD 8510.1-M, "DoD Information Technology Systems Certification and Accreditation Program

(DITSCAP)," July 31, 2000, require organizations to review and document the security controls of general support systems and major applications. MSC did not properly document an information systems security review because management did not adhere to OMB and DoD policy.

MSC Enterprise SSAA Comparison to OMB Guidance. OMB Circular A-130, Appendix III requires agencies to implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems. The MSC Enterprise SSAA did not meet the documentation requirements, including:

- **System Security Plan.** Training, personnel controls, continuity of support, and system interconnection were not included or not adequately documented.

- **Review of Security Controls.** The Enterprise SSAA, Appendix H, does not include test procedures or system test and evaluation plan results.

- **Authorized Processing.** MSC approving officials did not sign or date the Enterprise SSAA.

FMS SSAA Comparison to OMB Guidance. OMB Circular A-130, Appendix III requires agencies to implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated by major applications. The MSC FMS SSAA did not meet the documentation requirements, including:

- **System Program Plan.** The FMS SSAA did not provide adequate documentation of application controls and technical controls.

- **Authorized Processing.** MSC approving officials did not sign or date the FMS SSAA.

FMS SSAA Comparison to DoD Guidance. DITSCAP provides a standard certification and accreditation process for DoD Information Technology systems. Management did not sign the FMS SSAA, follow the required document structure, and include the following sections as required by the DITSCAP:

- Training,
- DITSCAP Plan,
- System Concept of Operations,
- Information System Security Policy,
- Incident Response Plan,
- Contingency plans,
- Personnel controls and Technical controls,
- System Interface Agreements (Memorandums of Agreement), and
- Security Education, Training, and Awareness Plan.

MSC did not prepare the security program plans in compliance with OMB and DoD guidance. As a result, management may not identify risks to the general support system and major application. With a well-designed program following

OMB and DoD guidance, MSC could ensure that responsibilities are clear, understandable, and properly implemented; and security controls are adequate and consistently applied.

Security Management Structure

MSC did not adequately establish the information systems security management structure. Specifically, MSC did not have an organization chart that identified personnel and their titles for the Computer Systems Directorate. The Implementation Guide for OMB Circular A-123, “Management’s Responsibility for Internal Control,” July 2005 directs management to become more proactive in overseeing internal controls related to financial reporting. It further explains that management should document key processes and controls, which include organization charts. In addition, MSC did not document, as required by DoD Instruction 8500.2, appointment letters for two of the five Information Assurance personnel. MSC did not adequately establish the information systems security management structure because management did not follow policies and procedures that require documenting an organization chart and appointment letters. As a result, it could not be determined who was responsible for systems security duties; and whether security personnel had the appropriate authority, training, and security clearance to perform their duties.

Security-Related Personnel Procedures

MSC did not adequately checkout employees who had separated from the activity. Commander, Military Sealift Command Instruction (COMSCINST) 5510.8F, “COMSC Information and Personnel Security Regulation,” October 4, 2001, Exhibit F is a checkout form for personnel to complete prior to leaving the activity. From June 1, to August 31, 2005 five employees with FMS access separated from MSC. MSC could only provide a checkout form for one of the five employees who separated. In addition, management in the Accounting Office could not identify the authorizing initials on the provided checkout form. All five of the employees’ FMS user accounts remained active subsequent to there separation. MSC did not properly process separated employees because management did not follow the established procedures. As a result, there is an increased risk of unauthorized access by former employees, who could alter or delete financial data. MSC should comply with the checkout procedures to mitigate this risk.

Information Systems Security Program

MSC did not adequately monitor the effectiveness of the security program. A contractor performed a risk assessment in conjunction with the last DITSCAP review for MSC FMS in 2003. The contractor made 24 recommendations to mitigate risks identified. MSC did not adequately monitor the effectiveness of the security program because IT security management did not document and approve a remediation plan and corrective actions. As a result, 11 of the 24 recommendations remained outstanding that increase risks to system integrity, confidentiality, and availability. A plan of action and milestones for all recommendations would provide a means and identify responsibilities for correcting weaknesses.

Recommendations, Management Comments, and Audit Response

A. We recommend that the Commander, Military Sealift Command:

1. Follow Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Information Resources," and DoD 8510.1-M, "DoD Information Technology Systems Certification and Accreditation Program (DITSCAP)," July 31, 2000, when completing the next Military Sealift Command Enterprise and Financial Management System, System Security Authorization Agreements to identify and document security planning and internal controls.

2. Document an organization chart for the Computer System Directorate that includes a description of all positions, responsibilities, and the names of personnel holding those positions to ensure that employees have the necessary authority to carry out their duties.

3. Create and maintain appointment letters for systems security personnel, including the Military Sealift Command Certification Authority and the Military Sealift Command Enterprise Information Systems Security Manager.

4. Follow the Commander, Military Sealift Command Instruction 5510.8F, "COMSC Information and Personnel Security," October 4, 2001 by using the checkout procedure for each employee leaving the activity.

5. Document a remediation plan of action and milestones for all recommendations for the vulnerabilities identified in the 2003 Financial Management System risk assessment and future systems security recommendations.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to strengthening entity-wide security program planning and management general controls. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for documenting the remediation plan.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 1.

Table 1. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
A.1.	Department of the Navy	—	X	X
A.2.	Department of the Navy	—	X	X
A.3.	Department of the Navy	—	X	X
A.4.	Department of the Navy	—	X	X
A.5.	Department of the Navy	—	X	X

B. Access Controls

MSC did not adequately design access controls to operate effectively. Specifically, MSC did not maintain a current list of authorized users and establish physical and logical controls to prevent or detect unauthorized access or modifications, and protect system information from physical and environmental damage. MSC did not maintain a current list of authorized users because management did not establish a policy for periodic review. MSC did not establish physical and logical controls to prevent or detect unauthorized access or modifications, and protect system information from physical and environmental damage because management did not develop or enforce policies and procedures requiring adequate access controls. As a result, these weaknesses increase the risk of unauthorized access, software modification or deletion, and physical or environmental damage to MSC resources.

Physical and Logical Access Controls

Physical and logical access controls should provide reasonable assurance that organizations protect computer resources (data files, application programs, and computer-related facilities and equipment) against unauthorized modification, disclosure, loss, or impairment. Physical controls include activities such as keeping computers in locked rooms to limit physical access. Logical controls include preventative measures such as security software programs designed to prevent or detect unauthorized access to sensitive files. MSC had access control weaknesses in both physical and logical access controls.

Maintain a Current List of Authorized Users

MSC did not maintain a current list of authorized users. Specifically, management did not disable active user accounts in a timely manner upon personnel terminating their employment. During a 90-day period from June 1 to August 31, 2005, five individuals with access to FMS left the activity. As of November 1, 2005, all five of the individuals still had active accounts in FMS. Additionally, one out of the five user accounts accessed the system multiple times after the user's separation date. The NIST SP 800-12, "An Introduction to Computer Security," chapter 10, October 1995, recommends that management terminate access to the system in a timely manner (during out-processing procedures) and, in case of an unfriendly termination, access should be removed at the same time (or just before) the employee is notified of dismissal. MSC did not maintain a current list of authorized users because management did not establish a policy for periodic review to ensure the disabling of separated employee accounts. As a result, there is an increased risk for separated employees to access FMS, damage system operations, and alter data within the system, which could lead to misstatements of financial data. Management could mitigate risks by strengthening controls, such as reviewing access lists, and following policies and procedures when employees leave the organization.

Establish Physical and Logical Controls

MSC did not establish adequate physical and logical controls to prevent or detect unauthorized access or modifications, and protect system information. Specifically the following controls were inadequate: physical security, fire suppression, user accounts, and application logon parameters. MSC did not establish physical and logical controls to prevent or detect unauthorized access or modifications, and protect system information because management did not develop or enforce policies and procedures requiring these controls.

Physical Security. The physical security controls over the MCDC were inadequate. The NIST SP 800-12 states "…Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation." Unauthorized personnel, without visible identification, gained access to the MCDC four out of five attempts without question. Security personnel did not monitor security cameras, respond to door alarms, or question unauthorized individuals. In addition, unauthorized personnel gained access to a mission-critical server lab within the MCDC on three out of three attempts. An individual who obtains unauthorized entry into the MCDC could damage or destroy system servers, which could impede or shut down MSC financial operations. Increased monitoring of security cameras, personnel awareness, training, and improved alerts of breaches can significantly reduce these risks.

Fire Suppression System. MSC did not ensure that routine inspections of the fire suppression system occurred at the MCDC. NIST SP 800-12 states, "when properly installed, maintained, and provided with an adequate supply of water, automatic sprinkler systems are highly effective in protecting buildings and their contents." Personnel provided one confirmation of a sprinkler system inspection completed on December 5, 2005. MSC did not provide past fire inspection documentation for the MCDC to confirm routine inspections of the fire suppression system. As a result, there is increased risk of hardware damage without the assurance of a fully functional fire suppression system. MSC needs to ensure the inspection of the sprinkler system on a routine basis to ensure the protection of the system servers in the event of a fire.

Shared User Accounts. MSC did not adequately control privileged user accounts. Four individuals at MSC shared the "sysadmin" user account for FMS. The account was shared because management did not enforce COMSCINST 5239.3A, "Military Sealift Command Information Assurance Policy," October 14, 2003, which does not allow sharing of accounts. When multiple personnel use the "sysadmin" account, changes made are no longer traceable to a specific user making it impossible to recreate a complete audit trail. Users with this responsibility could create, review, and approve fictitious transactions without accountability in the system. As a result, the potential exists for unauthorized modification of financial data in FMS. A mitigating control such as a division of responsibilities to specific user accounts and review of "sysadmin" activity would decrease the risk of unauthorized modifications to data.

Application Logon Parameters. FMS password parameters did not comply with DoD minimum password requirements. DoD Instruction 8500.2 states "passwords are, at a minimum, a case sensitive, 8 character mix of upper case letters, lower-case letters, numbers, and special characters, including at least one of each." MSC policy required an 8-character password using at least one number but did not require a special character or case sensitivity. In addition, FMS only required a five-character password. Passwords that are not sufficiently strong are vulnerable to password cracking[2] and other attacks intended to discover user passwords.

Furthermore, the FMS logon parameters did not automatically lock out users after three unsuccessful logon attempts. COMSCINST 5239.3A states that access (to the system) shall be denied after three unsuccessful logon attempts, and System Administrator interaction shall be required for reactivation of the account. Users were able to logon to FMS after multiple failed attempts. A user attempted to access the system 15 consecutive times with an invalid password. On the sixteenth attempt, the user entered the correct password associated with the user name and was granted access to FMS. Management stated that the three unsuccessful lock out security feature was available for FMS. Management was aware of this setting, however did not enable the parameter to lock a user account after three unsuccessful attempts. By not restricting the number of logon attempts, there is an even greater risk that intruders would be able to crack passwords. The weaknesses in application logon parameters leave FMS vulnerable to password cracking, which could result in unauthorized access to FMS. An individual who gains unauthorized access could delete or modify system data or compromise critical system programming. To mitigate this risk, MSC management should enable the function that automatically locks users out of FMS after three unsuccessful logon attempts.

Recommendations, Management Comments, and Audit Response

B. We recommend the Commander, Military Sealift Command:

1. Develop and enforce an access control policy that:

a. Includes quarterly reviews of the Financial Management System list of active user accounts to ensure that only individuals employed at the activity possess active Financial Management System accounts.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred. The Military Sealift Command is currently assessing the optimum way to obtain up-to-date active worldwide employee files, including civilian,

[2] Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system, typically, by repeatedly verifying guesses for the password. One purpose of password cracking is to gain unauthorized access to a system.

military, and contractors to facilitate the recommended comparison on a quarterly basis.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed completion date(s) related to quarterly reviews of the Financial Management System list of active user accounts. We request that the Department of the Navy provide milestones in its comments on the final report for quarterly reviews of the Financial Management System list of active user accounts.

b. Requires a monthly review of the separated employees list to ensure that all separated employees' Financial Management System user accounts are end dated in the system.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred. The Military Sealift Command is currently using the Headquarters biweekly "Accessions and Separation Report" to end date users leaving Military Sealift Command Headquarters on a real-time basis. They are also assessing the optimum way to obtain similar information on all other Headquarters and field personnel.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed completion date(s) related to a required monthly review of separated employees to ensure that user accounts are end dated. We request that the Department of the Navy provide milestones in its comments on the final report for a required monthly review of separated employees to ensure that user accounts are end dated.

2. Develop and enforce a physical security policy that:

a. Increases monitoring of security cameras inside Building 196 and incorporate this policy into the Service-Level Agreement, and

b. Requires security and awareness training to individuals working in the Military Sealift Command Corporate Data Center to raise the awareness of security-related threats to Military Sealift Command resources.

3. Develop and implement a policy requiring a quarterly inspection of the fire suppression system inside Building 196 and incorporate this policy into the Service-Level Agreement.

4. Enforce the shared user account requirement in Commander, Military Sealift Command Instruction 5239.3A "Military Sealift Command Information Assurance Policy," October 14, 2003, and divide the "sysadmin" functions to individual user accounts to ensure accountability. Establish a

policy requiring a periodic independent review of all privileged account activity.

5. Submit a change request to make the Financial Management System password parameters enforce the password requirements set forth by DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

6. Enable the system logon parameter that will lock a user out after three unsuccessful logon attempts.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to strengthening access controls. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for limiting a user to three logon attempts.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 2.

Table 2. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
B.1.a.	Department of the Navy	—	—	X
B.1.b.	Department of the Navy	—	—	X
B.2.a., B.2.b.	Department of the Navy	—	X	X
B.3.	Department of the Navy	—	X	X
B.4.	Department of the Navy	—	X	X
B.5.	Department of the Navy	—	X	X
B.6.	Department of the Navy	—	X	X

C. Software Development and Change Control

MSC did not adequately design software development and change controls to operate effectively. Specifically, MSC did not properly document or authorize processing features and program modifications; adequately document, test, and approve all new and revised software; and document and control software libraries. The general controls over software changes were inadequate because MSC did not establish configuration management authorization, testing, approval, and library policies and procedures. As a result, there is an increased risk that personnel could install unauthorized software, make software changes prior to evaluating test results, and migrate unapproved software into production.

Application and System Software Development and Change Control

Application software supports a specific operation such as purchasing or accounts payable. Establishing controls over the modification of application software programs helps to ensure that implementation of only authorized programs and modifications occurs. Organizations can accomplish this by instituting policies, procedures, and techniques that help ensure the proper authorizing, testing, and approval of all programs, modifications, and that access to and distribution of programs is carefully controlled. System software is a set of programs that operates and controls processing activities for computer equipment. Organizations must control the modification of system software to provide reasonable assurance that personnel have not compromised the system's security and the system will not be impaired. MSC did not adequately implement software change control.

Authorization of Processing Features and Program Modifications

MSC did not properly document or authorize processing features and program modifications for application and system software changes. DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 2002, states DoD Components must use a disciplined life-cycle approach to manage information resources from acquisition through retirement. In addition, Department of the Navy Information Assurance (IA) Publication 5239-13, "Information Assurance Certification and Accreditation," volume II, December 2000, set forth requirements that management review and approve the product development plan for new services and products. Lack of proper documentation and authorization occurred because MSC did not develop and implement policies and procedures for application and system software changes.

Application Software Changes. Three Configuration Management (CM) processes used by MSC to implement a change to application and systems software were:

- Configuration Change Request (CCR) to process changes that required change control board authorization to expend additional funds,

- Internal Configuration Change Request (ICCR) to process changes that do not require change control board authorization, and

- help desk tickets to process changes that did not require fund expenditure.

The CCRs reviewed had little documentation in the CM library. The CCR authorization process was not consistent. There were no policies and procedures in place for authorization of software modifications. Software modification CCR forms were not accurately and completely documented, maintained, authorized, and implemented. MSC could not provide documentation of ICCRs and did not keep documentation of ICCRs and helpdesk tickets in the CM library. MSC had a help desk ticket tracking system; however, MSC could not provide documentation for a software change due to a change of the help desk tracking system.

System Software Changes. There was no documentation to support the authorization of FMS systems software changes in the CM library for the reviewed changes. MSC personnel considered all of the reviewed system software patches[3] to be routine maintenance and did not submit the changes as CCRs. Management communicated authorization through e-mails, but personnel could not identify them with a specific patch because the e-mails did not include the patch number.

As a result of the lack of documentation of application and system software changes, verification of the authorization and implementation of changes to the MSC FMS could not occur. MSC prepared a draft CM Plan that would provide structure to the software change process. MSC could establish consistency of change control processes and documentation by ensuring that the CM plan meets the requirement of a disciplined life-cycle approach and implementing the CM plan upon completion.

Test and Approve All New and Revised Software

MSC did not adequately test and approve all new and revised software. The lack of test plan standards and management approval occurred because MSC did not develop and implement policies and procedures for controlling system changes.

Test. MSC had not developed test plan standards or maintained documentation of testing performed. Joint Financial Management Improvement Program System Requirements 02-01, “Core Financial System Requirements,” November 2001,

[3] A patch is a temporary addition to a piece of code, usually as a quick-and-dirty remedy to an existing bug or misfeature.

states that a financial management system may require maintenance or modification; therefore, agencies should develop standards and procedures for testing, implementing, and installing modifications to the system.

NIST SP 800-26, "Computer Security," November 2001, states that the supporting documentation makes it easier to review the program by describing all the test scenarios that have taken place throughout the life of the program. There were no test plan standards that define responsibilities for management, users, system analysts, programmers, auditors, quality assurance, and library control. In addition, there was no documentation of test plans, test results, changes made based on test results, or user acceptance of the new or revised software in the CM library. A draft test plan, results of the testing performed, documentation of user acceptance, and a feasibility study were included for 1 of the 15 reviewed changes. However, management did not finalize these documents. MSC did not provide documentation to support testing for 14 of 15 reviewed changes including the following:

- test specifications,
- test plans,
- test failures,
- test transactions and data,
- test results,
- management or security administrator reviews,
- user acceptance testing,
- management approval, and
- updates to system and operational documentation.

Approval. MSC management did not adequately approve configuration change requests. NIST SP 800-53 recommends that an approving official within an organization must document and control changes to their information systems while monitoring the changes and conducting security impact analyses. MSC could not provide supporting documentation for adequate approval of software changes requested.

In addition, MSC did not develop procedures for testing and approval of emergency changes. The NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," February 2005, "Configuration Management," Section 3, recommends organizations to include emergency changes in the configuration change control process. The Military Sealift Command Business Impact Analysis (BIA) states that there is a 3- to -14 day system recovery requirement. MSC did not develop emergency change procedures and concluded that personnel could follow the three CM processes in place under any circumstance.

As a result of the lack of testing and approval, an audit trail does not exist to track the system changes for FMS. Not establishing controls over the modification of application software programs increases the risk of implementing unauthorized programs and modifications. Also, not developing emergency change procedures will increase the risk of suspending or abbreviating normal controls. MSC could reduce these risks by completing and implementing a CM plan.

Controls over Software Libraries

MSC did not adequately document or control software libraries. COMSCINST 5239.3A states that MSC should manage and maintain system libraries appropriately. MSC should update libraries when they make changes, and all users should abide by all system library internal controls. Furthermore, the Department of the Navy Staff Officer Publication 5239-07, “Information System Security Officer Guidebook,” February 1996 states that the Information System Security Officer should maintain a library of the documentation detailing the IS hardware, software, and firmware configuration and security features. MSC has implemented control measures to limit access to its software library; however, documentation does not exist for the software library or software migration procedures. MSC did not keep an inventory or a log for the software library. In addition, the same administrator who maintained the software library also tested and migrated system software for production. MSC lacked software library controls because management did not develop policies and procedures for the software library and independent migration process. As a result, MSC could not trace software installations through the development, testing, and production instances, and there is an increased risk that unapproved software would be migrated. The CM plan should include policies and procedures for library management and independent migration to reduce this risk.

Recommendations, Management Comments, and Audit Response

C. We recommend that the Commander, Military Sealift Command complete and implement the Configuration Management Plan in accordance with DoD Directive 8000.1, “Management of DoD Information Resources and Information Technology,” February 2002, which requires a disciplined life-cycle approach. The Configuration Management Plan should include the following:

1. Proper authorization documentation for each phase of a Configuration Change Request and Internal Configuration Change Request used for application and system software changes.

2. Submit all documentation for Internal Configuration Change Requests, configuration change help desk tickets, and system software changes to the Configuration Management library.

3. For the testing and approving of new and revised software, include the following:

a. Document test plan standards for all levels of testing that define responsibilities for each party,

b. Report test failures and modifications,

c. Document test transactions and data, and

d. Develop and implement emergency change procedures.

4. Develop and approve policies and procedures to control the software libraries and independent software migration that:

a. Includes a log for the software library,

b. Requires an inventory for the software library, and

c. Enforces personnel independent of the software testing group to migrate approved changes to production.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to the completion and implementation of the Configuration Management Plan. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for the completion and implementation of the Configuration Management Plan.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 3.

Table 3. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
C.1.	Department of the Navy	—	X	X
C.2.	Department of the Navy	—	X	X
C.3.a., 3.b., 3.c., 3.d.	Department of the Navy	—	X	X
C.4.a., 4.b., 4c.	Department of the Navy	—	X	X

D. System Software

MSC did not adequately design system software general controls to operate effectively. MSC did not properly limit and monitor access to and use of system software. Access was inadequately limited because MSC did not follow established procedures for approval of system administrator access and accounts. The lack of effective monitoring occurred because MSC did not develop or enforce policies and procedures for the use and monitoring of system software utilities. As a result, these weaknesses could create vulnerabilities and the opportunity for unauthorized actions to occur.

System Software Controls

System software is a set of programs designed to operate and control the processing activities of computer equipment. System software helps control and coordinate the input, processing, output, and data storage. MSC used the Sun Solaris 5.8 system software for FMS. MSC did not adequately design general controls over system software to operate effectively.

Access to System Software

MSC did not adequately limit access to system software. Specifically, management did not approve system administrator access and control the administrator account. Access was not adequately limited because MSC did not follow established procedures for approval of system administrator access and a shared account.

Administrator Access. MSC did not properly authorize user access to system software. To gain system administrator access to system software, the COMSCINST 5239.3A requires a valid request to gain a user account and password. The MCDC standard operating procedures require database administrators and end users who need network accounts to fill out a “User Account Request Template” and provide additional required information. From this information, MSC would grant or deny access to the computer system. During a recent contract change, management did not follow this policy. Users at the MCDC were given access to the MSC computer system without providing a valid request and obtaining approval from MSC management. Without proper authorization, individuals may have access to areas of the system that their job duties did not require. This provides the opportunity for unauthorized actions to occur.

Administrator Accounts. Multiple users shared the administrator account “root”[4] for access to the computer system. The use of one username and password is not permitted under COMSCINST 5239.3A as it states that accounts must not be shared. The root account is necessary to perform certain system

[4] The “root” user account is the UNIX system administration account with the highest privilege levels.

functions. The root user had the ability to logon either from a remote logon or directly from the master console. Management could only trace activity on the root account if the user logged on through a remote connection. As a result, management cannot maintain proper auditing logs, which increases the risk of unauthorized activities occurring. To mitigate this risk, personnel should always logon remotely. If it is necessary to logon through the master console, the user should record the activity to provide an audit trail.

Use and Monitoring of System Software

MSC did not effectively use and monitor the system software. The lack of effective use and monitoring occurred because MSC did not enforce policies and procedures for system software utilities.[5]

Use of System Software Utilities. MSC did not properly document the use of system software utilities. OMB Circular A-123 states documentation of the significant computer applications should include the nature of software utilities used at computer processing locations that provide the ability to add, alter, or delete information stored in data files, the database, and program libraries. As a result, there is an increased risk of vulnerabilities and errors in the use of software. MSC could mitigate this risk by establishing policies to prevent errors in the software usage that could cause vulnerabilities.

Monitoring of Software Utilities. MSC did not adequately monitor the use of system software utilities. COMSCINST 5239.3A states:

> Auditing shall be in place to ensure that each person who accesses a system is accountable for their actions. Audit records shall be sufficiently detailed to reconstruct events that lead to a security violation, malfunction, or other adverse event, and determine its cause and scope. These records must be protected and reviewed as appropriate for the level of concern for the system.

MCDC personnel did not document daily reviews performed of software utilities that would create proper audit records. Additionally, MSC management did not perform any review of system software utilities. As a result, MSC cannot effectively manage access to system software utilities. To alleviate this risk, MSC should perform reviews of system software utilities.

[5] MSC had the following system software utilities in place: HP Jet Direct, Secure Shell 3.2.2, Legato, TCP Wrapper 7.6, Big Brother 1.9c, Cops 1.04, and Enterprise Security Manager 55.

Recommendations, Management Comments, and Audit Response

D. We recommend that the Commander, Military Sealift Command:

1. Follow Commander, Military Sealift Command Instruction 5239.3A, "Military Sealift Command Information Assurance Policy," October 14, 2003, to properly authorize the access granted to the Military Sealift Command Corporate Data Center personnel.

2. Require Military Sealift Command Corporate Data Center personnel to logon remotely from their workstation when using the root user account. If access to the root user account is necessary through the master console, a manual log is to be used to record the activity of the root user account to provide a proper audit trail.

3. Establish policies and procedures documenting the use of system software utilities as required by the Office of Management Budget Circular A-123, "Management's Responsibility for Internal Control," July 2005.

4. Require Military Sealift Command to perform reviews of system software utility usage.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to strengthening system software general controls. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for reviewing system software utility usage.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 4.

Table 4. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
D.1.	Department of the Navy	—	X	X
D.2.	Department of the Navy	—	X	X
D.3.	Department of the Navy	—	X	X
D.4.	Department of the Navy	—	X	X

E. Segregation of Duties

MSC did not properly segregate incompatible duties and control and monitor MCDC personnel activities. The general controls over segregation of duties were inadequate because MSC did not develop or enforce policies and procedures to support segregation of duties and control and monitor personnel activity. As a result, there was an increased risk of processing erroneous transactions, assigning improper responsibilities to an FMS user, improper use of computer resources, and unauthorized modifications of financial data in FMS.

Segregation of Duties Controls

Segregation of duties refers to the separation of work responsibilities to prevent one employee from controlling all critical stages of a process. Segregation of duties is a critical control that assures the separation of the functions of authorizing, processing, recording, and reviewing transactions. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other.

Segregate Incompatible Duties

MSC did not properly segregate incompatible duties. Specifically, management did not identify incompatible duties and properly document job descriptions. Segregation of incompatible duties was inadequate because MSC did not develop or enforce policies and procedures to assist in segregating duties.

Incompatible Duties. MSC assigned several users privileged accounts or conflicting responsibilities. DoD Instruction 8500.2 requires the Information Assurance Manager to develop and implement a role-based access scheme that accounts for all privileged access and implements the principles of least privilege and separation of functions. MSC assigned the System Administrator responsibility to 12 application users and the purchasing super user responsibility to 41 users. These privileged responsibilities allow the user to perform a number of incompatible duties. Additionally, MSC assigned nine application users conflicting responsibilities in FMS that included a combination of four responsibilities. The four responsibilities identified were MSC Requisitioner, MSC Purchase Card Holder, MSC Fund Certifier, and MSC Procurement Processor. Table 5. shows the incompatible responsibilities and number of users identified in FMS for each combination of incompatible responsibilities.

Table 5. Number of FMS Users Assigned Incompatible Responsibilities

MSC Requisitioner[a]	MSC Purchase Card Holder[b]	MSC Fund Certifier[c]	MSC Procurement Processor[d]	No. of Users
		X	X	4
	X	X		2
X		X		1
X	X	X	X	1
X	X	X		1
			Total	**9**

[a] Allowed the creation of purchase requisitions and purchase orders from an approved commitment.
[b] Allowed the purchase cardholder to enter their monthly purchase card requisitions.
[c] Allowed the viewing of requisition header information and project status information. It also allowed the approval of commitments and the posting of receipts.
[d] Combined the functions of purchasing requisitioner, purchasing technician, and receiver. The combination of these functions was to improve efficiency.

In addition, MSC did not have policies in place that required regularly scheduled vacations or job rotations to reduce the risk of fraud, and personnel had not received training on the principles of segregation of duties. MSC must provide adequate resources and training to personnel to ensure the understanding of segregation of duties principles, establishment, enforcement, and institutionalization within the organization. As a result of not having policies in place, there was an increased risk of processing erroneous transactions through FMS. Performing a review of user's responsibilities in FMS on a regular basis would mitigate this risk. Providing personnel training on the principles of segregation of duties would also help to mitigate this risk.

Job Descriptions. The MSC job descriptions did not specifically address the user's responsibilities within FMS. According to NIST SP 800-12, employee job descriptions should assist the system administrator in assigning responsibilities to FMS users. The roles and responsibilities found in the job descriptions at MSC were broad categories of functions. To assist the system administrator in assigning responsibilities in FMS, the individual's supervisor would fill out a New Employee Form. However, out of eight employees selected:

- seven did not have a form on file and
- one had a completed form on file that did not include specific duties to be performed in FMS.

As a result, an increased risk existed in assigning improper responsibilities to an FMS user. To mitigate this risk, MSC should revise and require completion of the New Employee Form to include a brief description of the individual's FMS duties to assign and document user responsibilities.

Operations Personnel Activity

MSC did not properly control and monitor personnel activity. Specifically, formal procedures did not guide MCDC personnel in performing their duties, and management did not actively supervise and review personnel activity. MSC did not properly control and monitor MCDC personnel activities because the policies and procedures in place to control and monitor personnel were inadequate.

MCDC Formal Procedures. Management did not document detailed instructions that guide personnel in performance of their duties. Department of the Navy IA Publication 5239-01, "Introduction to Information Assurance Publication," May 2000 states consistent, clearly documented operating procedures for both system configuration and operational use are key to ensuring information assurance. Procedures should define system deployment, configuration, and day-to-day operations for both the system administrator and user, as well as how to respond to real or perceived attempts to violate system security. All Department of the Navy information systems and networks should include written standard operating procedures, which are routinely updated and tailored to reflect changes in the operational environment. Management provided the MCDC Standard Operating Procedures manual as the policy and procedures used to guide personnel activities. Although the MCDC Standard Operating Procedures manual provided a framework to guide personnel activity, examples of omissions were:

- system startup and shutdown procedures or emergency procedures; and

- instructions such as the use of scripts to change passwords of privileged database accounts.

As a result, there is an increased risk of improper use of computer resources. Updating the MCDC Standard Operating Procedures manual would mitigate this risk.

Supervision and Review. MSC did not properly supervise and review MCDC personnel activity within FMS. COMSCINST 5239.3A requires administrators to configure systems to limit sessions and provide accountability for all sessions. It further details session accountability by requiring:

- audit features to be in place to ensure that people who access a system are accountable for their actions,

- audit records to be sufficiently detailed to reconstruct events that lead to a security violation, malfunction or other adverse event, and determine its cause and scope,

- management to protect and review these records as appropriate for the level of concern for the system, and

- MSC to review logs and audit trails at least weekly, but preferably once a day, for indications of inappropriate or unusual activity.

Management did not adequately supervise and review privileged user accounts. As a result, the potential exists for unauthorized modification of financial data in FMS. A mitigating control such as an automated history log of all computer operator activities on the system that supervisors routinely review could serve as part of the audit trail.

Recommendations, Management Comments, and Audit Response

Revised Recommendation. As a result of management comments, we revised draft recommendation E.3. to clarify the nature of the actions needed to improve existing management controls.

E. We recommend that the Commander, Military Sealift Command:

1. Enforce DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, by performing an annual review of the responsibilities assigned to application users of the Financial Management System to strictly limit the number of users who can create, review and approve transactions, create user accounts, create supplier records, or perform other incompatible functions.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to an annual review of the responsibilities assigned to Financial Management System users. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for an annual review of the responsibilities assigned to Financial Management System users.

2. Require vacations or job rotations for personnel who have privileged access to the system, and provide training to personnel on the principles of segregation of duties.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred in principle. The Military Sealift Command is currently reexamining the entire process as it relates to strong internal controls over system access. They are working toward eliminating "privileged" access to the extent possible.

Audit Response. The Department of the Navy comments were partially responsive. The proposed actions that the Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) identified will not adequately ensure that MSC will take measures to require vacations or job rotations for personnel with privileged access to the system. We request that the Department of the Navy provide a specific plan of action with milestones in its comments on the final report for requiring vacations or job rotations for personnel who have privileged access to the system.

3. Require the completion of the New Employee Form to include a brief description of the employee's duties within the Financial Management System, for use in assigning and documenting responsibilities.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred in part. The Military Sealift Command is currently in the process of revising the New Employee Form to advise the Financial Office of the specific Financial Management System duties to be performed by the requestor.

Audit Response. The Department of the Navy comments were partially responsive. We revised the recommendation to mirror the action of the Military Sealift Command. However, the Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed completion date(s) related to revising the New Employee Form to require the specific Financial Management System duties performed by the requestor. We request that the Department of the Navy provide milestones in its comments on the final report for revision of the New Employee Form to require the specific Financial Management System duties performed by the requestor.

4. Update the Military Sealift Command Corporate Data Center Standard Operating Procedure manual to:

a. Include system startup and shut-down procedures;

b. Document emergency procedures; and

c. Incorporate new procedures.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to updating the Military Sealift Command Corporate Data Center Standard Operating Procedures manual. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for updating the Military Sealift Command Corporate Data Center Standard Operating Procedures manual.

5. Follow Commander, Military Sealift Command Instruction 5239.3A, "Military Sealift Command Information Assurance Policy," October 14, 2003, by configuring the Financial Management System to create an automated history log of all computer operator activities on the computer system to serve as an audit trail. In addition, require supervisors to routinely review the history log for privileged accounts and investigate any abnormalities.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to configuring the system to create an automated history log and requiring supervisors to routinely review it to serve as an audit trail. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for configuring the system to create an automated history log and requiring supervisors to routinely review it to serve as an audit trail.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 6.

Table 6. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
E.1.	Department of the Navy	—	X	X
E.2.	Department of the Navy	—	X	X
E.3.	Department of the Navy	—	—	X
E.4.a., 4.b., 4.c.	Department of the Navy	—	X	X
E.5	Department of the Navy	—	X	X

F. Service Continuity

MSC did not adequately design service continuity general controls to operate effectively. Specifically, MSC did not properly assess the criticality and sensitivity of computerized operations and identify supporting resources critical to operations; take steps to prevent and minimize potential damage and interruption to the system; and develop and document a comprehensive contingency plan. Service continuity general controls were not adequately designed or operating effectively because MSC did not establish or follow service continuity policies and procedures. As a result, these weaknesses could cause a delay in the restoration of critical operations, loss of data, equipment failure, unsafe conditions in an emergency, and delays in returning to normal operations.

Service Continuity Controls

Service continuity is synonymous with a disaster recovery plan. A loss of the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. Because of this risk, organizations should implement service continuity controls to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. Controls to ensure service continuity should address the entire range of potential disruptions, which may include relatively minor interruptions, such as temporary power failures, as well as major disasters. MSC developed their MCP as a guide in the event of a contingency. Service continuity controls over FMS at MSC were not adequately designed or operating effectively.

Assess Computerized Operations and Supporting Resources

The MSC MCP did not adequately assess the criticality and sensitivity of computerized operations and identify supporting resources. Management had not included emergency processing priorities in the MSC MCP. MSC assessed emergency processing priorities in the MSC BIA, which identified the maximum tolerable downtime for each mission-critical and mission-essential MSC function and defined four phases of recovery. However, MSC did not incorporate this information into the MSC MCP. MSC did not properly assess computerized operations and supporting resources. NIST SP 800-34 recommends that the results from the BIA be incorporated into the development of the MCP. As a result, there is an increased risk of delaying the resumption of operations in the event of a contingency. Incorporating the BIA into the MSC MCP would mitigate this risk.

Prevent and Minimize Damage and Interruption

MSC did not adequately take steps to prevent and minimize damage and interruption to the system. Specifically, management did not effectively:

- implement data and program backup procedures;
- implement adequate environmental controls;
- train staff for emergencies; and
- maintain hardware, problem management, and alternate data processing capabilities.

MSC did not adequately take steps to prevent and minimize damage and interruption to the system because management did not fully develop or follow service continuity policies and procedures.

Data and Program Backup Procedures. MSC did not properly implement data and program backup procedures. NIST SP 800-34 states that data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. The "MCDC Backup Policy," June 5, 2003, was a simple, generic explanation of the backup and data retention policy. The MCDC Backup Policy did not address the file-naming conventions, exact location of offsite storage, and method for transporting data offsite. MSC was in the process of developing a more complete backup policy; however, management did not provide the updated policy.

MSC used the MCDC Backup Policy as guidance to perform system backups. However, MSC did not adhere to the following portions of the MCDC Backup Policy.

- **Daily Backups.** MSC created a daily incremental backup to a hard drive, which could only be stored for 2 days due to backup tape failure.
- **Weekly Backups.** MSC does not perform a weekly full system backup.
- **Backup Storage.** Tapes were not stored and securely protected for retention periods commensurate with the type of information on the backup.
- **Tests of Backups.** MSC was not performing a test of the backups created.

As a result, there is an increased risk to the availability of data. To mitigate this risk, MSC should finalize and implement the updated MCDC Backup Policy to include: file naming conventions, exact location of storage, a method for transporting data offsite, and hardware maintenance.

Environmental Controls. MSC did not implement adequate environmental controls. NIST SP 800-53 states the organization schedules, performs, and documents routine preventative and regular maintenance in accordance with manufacturer or vendor specifications. MSC was unable to provide sufficient evidence that the environmental controls were functioning properly. As a result, there is an increased risk that in the event of an emergency, equipment will not function properly. MSC installed environmental controls including humidity, temperature, and lighting to protect personnel and equipment based on the operational needs of the site. However, documenting these controls, including preventive and regular maintenance, is vital to ensure the functionality of equipment in the event of an emergency.

Emergency Training. MSC did not train the MCDC staff on procedures to follow in case of an emergency. NIST SP 800-12 provides guidance regarding training personnel on emergency procedures. It states that organizations should provide training to personnel for their contingency-related duties upon joining the organization, as a refresher, and to practice skills. Procedures were not in place to require the necessary training or define the employee training. As a result, staff, without guidance or training in the case of an emergency, can cause unsafe conditions resulting in a loss of life or equipment. Developing these policies and procedures would mitigate this risk.

Hardware Maintenance, Problem Management, and Alternate Data Processing Capabilities. MSC did not perform routine preventative maintenance and establish an adequate alternative processing site. NIST SP 800-53 recommends that the organization schedules, performs, and documents routine preventative and regular maintenance of the information system in accordance with manufacturer or vendor specifications. MSC only performed maintenance after a failure occurred. In addition, MSC did not have an adequate alternative data processing site established for FMS. DoD Instruction 8500.2 and COMSCINST 5239.3A state that a disaster recovery plan, shall provide for the resumption of full operations within 24 hours of an event resulting in the cessation or degradation of full operations. MSC did not meet this requirement with the established processing site. As a result, there is an increased risk of a delay in providing important support services that may seriously affect operational readiness. MSC could mitigate this risk by performing routine maintenance and establishing an alternate data processing site.

Develop and Document a Comprehensive Contingency Plan

MSC did not fully develop and document a comprehensive contingency plan. Specifically, the contingency plan was not up-to-date, did not include the procedures for alternate data processing, and was not fully tested. MSC did not fully develop and document a comprehensive contingency plan because management did not comply with service continuity guidance.

Updated Contingency Plan. MSC had not updated the MSC MCP to include a timeframe for FMS to be operational in the event of a contingency. DoD

Instruction 8500.2 establishes the restoration requirement, which states that a Mission Assurance Category II system must be operational within 24 hours. MSC has developed the BIA to include a timeframe by requiring FMS to be operational in 3-14 days; however, MSC has not incorporated the BIA results into the MCP as is recommended by NIST SP 800-34. In addition, the BIA did not comply with DoD Instruction 8500.2. As a result, there is an increased risk that in the event of a system failure there will be a delay in the return to normal operations. MSC could mitigate this risk by correcting the BIA and incorporating it into the MCP.

Alternate Data Processing Procedures. MSC did not develop and document the procedures necessary to sustain operations in the event of a system disruption. NIST SP 800-34 defines contingency planning as interim measures to recover IT services following an emergency or system disruption. Interim measures may include the performance of IT functions using manual methods. In addition, NIST SP 800-12 states that documentation of all aspects of computer support and operations is important to ensure continuity and consistency. MSC did not develop interim manual procedures for personnel to follow in the event of system disruption. As a result, there is an increased risk of delays in returning to normal operations. MSC could mitigate this risk by documenting interim manual procedures to be used in the event of an emergency.

Contingency Plan Testing. MSC did not test all areas of the contingency plan. NIST SP 800-34 states plan testing is a critical element of a viable contingency capability. Testing enables organizations to identify and address plan deficiencies. Organizations should test each IT contingency plan element to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. MSC did not test the capability of personnel to telework in the event of a contingency. According to the MSC MCP, personnel were to telework in all phases of a contingency. In addition, MSC did not test the restoration of data from backup media and system performance using alternate data processing equipment. As a result, there is an increased risk that MSC personnel would not continue normal operations and financial data would be lost in the event of a contingency. The completion and testing of teleworking capabilities and an alternative data processing site will reduce this risk.

Recommendations, Management Comments, and Audit Response

F. We recommend that the Commander, Military Sealift Command:

1. Incorporate the Business Impact Analysis into the Military Sealift Command Mission Continuity Handbook.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to incorporating the Business Impact Analysis into the Military Sealift Command Mission Continuity Handbook. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for incorporating the Business Impact Analysis into the Military Sealift Command Mission Continuity Handbook.

2. Finalize and implement the updated Military Sealift Command Corporate Data Center Backup Policy to include:

a. File naming conventions,

b. Exact location of storage,

c. A method for transporting data offsite, and

d. Hardware maintenance.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to finalizing and implementing the updated data backup policy. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for finalizing and implementing the updated data backup policy.

3. Obtain and retain maintenance documentation for environmental control devices.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to maintenance documentation for environmental control devices. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for maintenance documentation for environmental control devices.

4. Develop emergency procedures and train the Military Sealift Command Corporate Data Center staff on these procedures.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to emergency procedures for the Military Sealift Command Corporate Data Center personnel. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for emergency procedures for the Military Sealift Command Corporate Data Center personnel.

5. Develop and follow maintenance procedures for information technology equipment and establish an alternative processing site.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to maintenance procedures of information technology equipment and an alternative processing site. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for maintenance procedures of information technology equipment and an alternative processing site.

6. Correct the Business Impact Analysis to be in accordance with DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, requiring a Mission Assurance Category II system to be operational within 24 hours of a contingency.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to correcting the Business Impact Analysis to include the system to be operational within 24 hours of a contingency. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for correcting the Business Impact Analysis to include the system to be operational within 24 hours of a contingency.

7. Develop and document interim manual procedures to be used in the event of an emergency.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred. The Military Sealift Command continues to work diligently on an overall Mission Continuity Plan. In addition, they are developing manual financial procedures for mission critical requirements that they will incorporated into the plan.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the completion date(s) related to manual financial procedures for mission critical requirements. We request that the Department of the Navy provide milestones in its comments on the final report for developing manual financial procedures for Mission Critical requirements.

8. Test telework capabilities and make corrections if appropriate in order to have the ability to telework in the event of an emergency.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to teleworking in the event of an emergency. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for teleworking in the event of an emergency.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 7.

Table 7. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
F.1.	Department of the Navy	—	X	X
F.2.a., 2.b., 2.c.	Department of the Navy	—	X	X
F.3.	Department of the Navy	—	X	X
F.4.	Department of the Navy	—	X	X
F.5.	Department of the Navy	—	X	X
F.6.	Department of the Navy	—	X	X
F.7.	Department of the Navy	—	—	X
F.4.	Department of the Navy	—	X	X

G. Authorization

MSC did not adequately design authorization application controls to operate effectively. Specifically, MSC did not authorize all fuel transactions before entry into FMS. Authorization application controls were not adequate because management did not finalize and enforce draft fuel processing procedures. As a result, the authorization weakness increases the risk of inaccurate data entry into FMS.

Authorization Controls

Authorization application controls ensure the validity of transactions and ensure that they represent economic events that took place during a given time period. Organizations should authorize data before its entry into the application system. Source documents play a significant role in originating data and should fall under control measures to ensure that organizations process only authorized transactions. Additionally, data should undergo an independent or supervisory review prior to entering the application. MSC did not adequately design authorization application controls to operate effectively.

Authorization of Fuel Purchases

MSC did not establish controls that authorized all fuel purchases before entry into FMS. Specifically, MSC did not control source documents or independently review all transactions. MSC did not establish controls that authorized all fuel purchases before entry into FMS because management did not finalize and enforce draft procedures for recording fuel purchases

Control Over Source Documents. MSC did not adequately use authorized source documents to support ship fuel purchases. DoD Financial Management Regulation (FMR) volume 1, chapter 3, “Accounting Systems Conformance, Evaluation, and Reporting,” May 1993, Key Accounting Requirement 8 states that financial transactions must be adequately supported with pertinent documents and source records. It further explains that all transactions, including computer-generated and computer-processed, must be traceable to individual source records. Fuel purchases were a significant portion of the MSC annual operating budget. MSC had draft procedures outlining the procedures for properly supporting fuel transactions, but management did not enforce the procedures to allow proper audit trails. MSC personnel were to record fuel purchases using a DD-1149, “Requisition and Invoice/Shipping Document,” or a DD-1155, “Order for Supplies or Services,” which was generated at the time of delivery, recorded the actual amount of fuel received, and signed by the supplier and MSC ship fuel officers.

However, the official DD-1149 or DD-1155 source document was not always available at the time of data entry. When MSC personnel did not receive the official source document, personnel used unauthorized summary documentation from the Navy Energy Usage Reporting System reports or the supplier bill to record the amount of fuel purchased for MSC ships. As a result, there is an increased risk of inaccurate data entry into FMS. To mitigate this risk, management should finalize and enforce the draft procedures for the recording of ship fuel purchases.

Independent Review. Management did not perform an independent review of all fuel transactions prior to entry into the system. DoD FMR volume 1, chapter 3, Key Accounting Requirement 7 states that organizations must maintain a separation of duties for reviewing transactions. MSC had draft procedures requiring MSC personnel to provide DD-1149 or DD-1155 forms to headquarters to establish proper separation of duties; however, MSC personnel did not always follow the procedures. In the event MSC headquarters did not receive an official source document, an individual was entering, approving, and receipting the fuel purchase transactions from the unauthorized summary documentation from the Navy Energy Usage Reporting System and supplier bills without an independent review. As a result, there is an increased risk that the financial statements contain unauthorized information regarding fuel expenditures. To mitigate this risk, management should finalize and enforce the draft procedures for fuel purchasing that includes a requirement for an independent review of fuel transactions.

Recommendations, Management Comments, and Audit Response

G.1. We recommend that the Commander, Military Sealift Command finalize and enforce the draft fuel processing procedures that will require submission of all DD-1149 and DD-1155 forms and fuel delivery documentation to Military Sealift Command Headquarters for supporting documentation of the financial transactions, independent review, and verification that fuel was received.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to supporting documentation of the financial transactions, independent review, and verification that fuel was received. We request that the Department of the Navy provide a plan of action with milestones in its comments on the final report for supporting documentation of the financial transactions, independent review, and verification that fuel was received.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 8.

Table 8. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
G.1.	Department of the Navy	—	X	X

H. Accuracy

MSC did not adequately design accuracy application controls to operate effectively. Specifically, MSC did not properly ensure that FMS data were valid and accurate. Accuracy application controls were not adequately designed or operating effectively because management did not establish or enforce data accuracy policies and procedures. As a result, financial data reported by FMS may be inaccurate.

Accuracy Controls

Data accuracy indicates that organizations record transactions in the correct amounts. The recording of valid and accurate data into an application system is essential to provide for an effective system that produces reliable results. The controls in this area address financial information as well as other data elements. In addition to the input of accurate transactions, organizations must ensure changes made to master files and other critical system components are valid and accurate. Organizations should perform data validation and editing to identify erroneous data. Many of the programmed checks in this process also concern the validity and accuracy of data fields in a transaction record, including whether a data field has a valid code, such as a vendor code, used in a purchasing system. MSC accuracy application controls were not adequately designed or operating effectively.

Validity and Accuracy of Data

MSC did not ensure that FMS data were valid and accurate. Specifically, management did not adequately design data entry features to contribute to validity and periodically test critical computations to contribute to data accuracy. MSC did not ensure that FMS data were valid and accurate because management did not establish or enforce data accuracy policies and procedures.

Data Entry Design. MSC did not adequately design data entry features to contribute to data validity. NIST SP 800-12 describes techniques to determine the accuracy of data fields that include consistency and reasonableness checks and validation during data entry and processing. These techniques can check data elements against expected values or ranges of values; analyze transactions for proper flow, sequencing, and authorization; or examine data elements for expected relationships. MSC did not have any restriction on the quantity, price, or total fields on the FMS data entry forms. As a result of not having these design features, MSC is at risk of entering invalid data into the application. To mitigate this risk, MSC should develop and implement a policy that requires using the accuracy checks available in FMS to identify unreasonable transactions.

Critical Computation Testing. MSC did not periodically test critical computations to contribute to data accuracy. The Joint Financial Management Improvement Program, "Forum Highlights: System Implementation Success Factors using COTS [commercial-off-the-shelf] Financial Systems," June 12, 2003, states to ensure a successful commercial-off-the-shelf system implementation, Joint Financial Management Improvement Program qualification testing should be viewed as "entry criteria." Agencies should conduct supplemental testing to ensure that the financial management system meets their specific requirements, and to ensure adequate system performance. MSC only performed testing of critical computations when they installed a new version of FMS. As a result of not testing critical computations, MSC is at risk of intentional or unintentional changes to the system that could lead to reporting inaccurate financial data. To mitigate this risk, MSC should perform periodic testing of critical computations.

Recommendations, Management Comments, and Audit Response

Revised Recommendation. As a result of management comments, we revised draft recommendation H.1.b. to clarify the nature of the actions needed to improve existing management controls.

H. We recommend that the Commander, Military Sealift Command:

1. Develop and implement policies and procedures that require:

a. Accuracy checks available in FMS to be used to flag for review unreasonable entries posted in the quantity, price, or total fields; and

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) concurred. The Military Sealift Command has already taken action to develop "System Alerts" to alert the Accounting Officer when quantity, price, or total fields on Requisitions and Purchase Orders exceed reasonable limits.

Audit Response. The Department of the Navy comments were partially responsive. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the completion date(s) related to having the "System Alerts" in place. We request that the Department of the Navy provide milestones in its comments on the final report for having the "System Alerts" in place.

b. Periodic testing of critical computations.

Management Comments. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) nonconcurred. The Military Sealift Command took exception to this recommendation because they use Oracle commercial-off-the-shelf software that is Joint Financial Management Improvement Program certified and untouched by Military Sealift Command personnel. They stated that the action taken in response to Recommendation H.1.a. will substantially strengthen controls.

Audit Response. The Department of the Navy comments were partially responsive. We revised the recommendation to clarify the intent of the recommendation. Modifications to software increase project risk exponentially, therefore, the additional control of periodically testing the critical computations would provide a control to mitigate the risk that a threat, either intentional or unintentional, could alter the system without being detected. The Director, Office of Financial Operations, Assistant Secretary of the Navy (Financial Management and Comptroller) did not identify the proposed action(s) and completion date(s) related to the periodic testing of critical computations. We request that the Department of the Navy reconsider its position by providing additional comments and a plan of action with milestones in its comments on the final report for the periodic testing of critical computations.

Management Comments Required

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements marked with an X in Table 9.

Table 9. Management Comments Required

Recommendation	Organization	Concur/ Nonconcur	Proposed Action	Completion Date
H.1.a.	Department of the Navy	—	—	X
H.1.b.	Department of the Navy	X	X	X

Appendix A. Scope and Methodology

We performed a review of the design and operating effectiveness of the general and application controls over the MSC FMS at two MSC sites, Washington Navy Yard, Washington D.C., and Defense Finance and Accounting Service, Omaha from July 2005 through July 2006 in accordance with generally accepted government auditing standards. Specifically, we performed the following.

- We interviewed personnel at the MSC Program Management Office in Washington Navy Yard, Washington, D.C., and Defense Finance and Accounting Service Technical Services Organization in Omaha, Nebraska.
- We inspected documentation and observed activities supporting the effectiveness of the general and application controls at the MSC Program Management Office in Washington Navy Yard, Washington D.C., and Defense Finance and Accounting Service, Omaha.
- We reviewed and tested specific control activities in place or performed by personnel at the MSC Program Management Office in Washington Navy Yard, Washington D.C.
- We re-performed, using a test environment, selected automated control activities within the MSC FMS application.
- We obtained and inspected system settings, access, and the results of security readiness review assessments performed at the MSC Program Management Office in Washington Navy Yard, Washington D.C.

We used the Government Accountability Office Federal Information System Controls Audit Manual, including Draft Chapter 4, “Evaluating and Testing Application Controls” to develop the procedures performed during this audit. Based on the Federal Information System Controls Audit Manual, the audit was divided into seven areas.

The entity-wide security program planning and management area is the foundation on which all other general controls rely. Security program controls are divided into five critical elements that covered the assessing risk, documenting the security program plan, establishing a security management structure, implementing effective security related personnel policies, and monitoring the security program’s effectiveness.

Physical and logical access controls reasonably protect the system and data from unauthorized modification, loss, and disclosure. Access controls are divided into four critical elements, which cover classification of information resources based on their criticality and sensitivity, access authorization, establishment of physical and technical controls, and monitoring of access.

Change controls are defined as the establishment of controls over the modification of application software programs to ensure that only authorized system programs and modifications were implemented. This is accomplished by instituting policies, procedures, and techniques that helped make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs was carefully controlled.

System software includes programs that are designed to operate and control the processing activities of computer equipment on which an application resides. Generally, one set of system software is used to support and control a variety of applications that run on the same computer hardware. System software helps to control and coordinate input, processing, output, and data storage associated with an application.

Segregation of duties refers to the separation of work responsibilities whereby one employee supporting the application does not control all critical stages of a process. The critical elements assess segregation of incompatible duties and establishment of related policies, establishment of access controls to enforce segregation of duties, and the control of personnel activities through formal operating procedures and supervision and review.

Service continuity includes the protection of an activity's resources, minimization of opportunities for service interruption, and planning for service recovery. The critical elements cover the assessment of the criticality and sensitivity of the system, the steps needed to prevent and minimize possible interruptions, development of a contingency plan, and test of the plan.

Application controls encompass both the automated processing contained within the computer program code and the policies and procedures associated with user activities. Application controls consist of four critical control areas covering authorization controls, completeness controls, accuracy controls, and controls over integrity of processing and data files.

The control objectives included within the scope of the audit were derived from applicable laws and regulations.

The scope of this audit focused on controls at the MSC Washington Navy Yard, Washington D.C., and the Defense Finance and Accounting Service, Omaha sites for the processing of financial transactions within MSC FMS. The controls assessed in this audit included controls associated with the input, processing, and output of MSC FMS information, as well as the manual procedures used to prepare and correct MSC FMS transactions. The controls contained within systems other than MSC FMS were not included in the scope of this audit. We did not assess general and application controls at the other MSC installations. Throughout the audit, if policies and procedures did not exist or were not provided we were unable to determine if MSC concurred with them. Due to these scope limitations, we were unable to test several controls, including:

- updating and maintaining system documentation after a configuration change,
- access paths to the system,

- the alternate data processing facility, and

- FMS edit checks and critical calculations.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit. Rather, we assessed the general and application controls that involved computer-processed data.

Government Accountability Office High-Risk Area. The Government Accountability Office has identified several high-risk areas in DoD. This report provides coverage of the Protecting Federal Government's Information-Sharing Mechanisms, DoD Business System Modernization, and DoD Financial Management high-risk areas.

Prior Coverage

During the last 5 years, the Naval Audit Service issued one report discussing the Military Sealift Command Financial Management System. Unrestricted Naval Audit Service reports can be accessed over the Internet at http://www.hq.navy.mil/.

Naval Audit Service

Naval Audit Service Report No. N2002-0018, “Military Sealift Command Financial Management System,” December 18, 2001

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Director, Program Analysis and Evaluation (PA&E)

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Naval Inspector General
Auditor General, Department of the Navy
Commander, Military Sealift Command

Combatant Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

National Security Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency

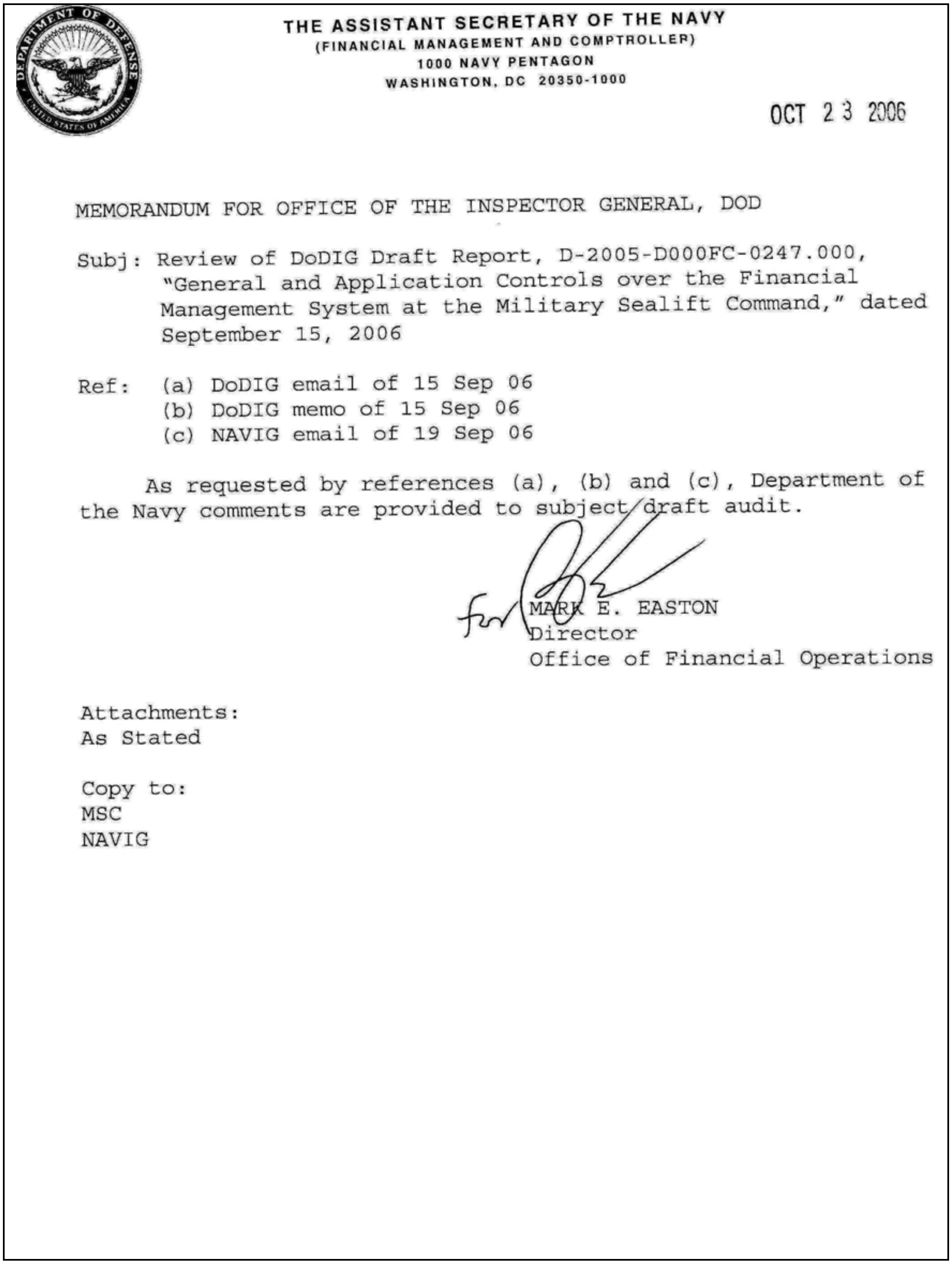
Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management
House Subcommittee on Technology, Information policy, Intergovernmental Relations, and the Census

Department of the Navy Comments



THE ASSISTANT SECRETARY OF THE NAVY
(FINANCIAL MANAGEMENT AND COMPTROLLER)
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

OCT 23 2006

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL, DOD

Subj: Review of DoDIG Draft Report, D-2005-D000FC-0247.000, "General and Application Controls over the Financial Management System at the Military Sealift Command," dated September 15, 2006

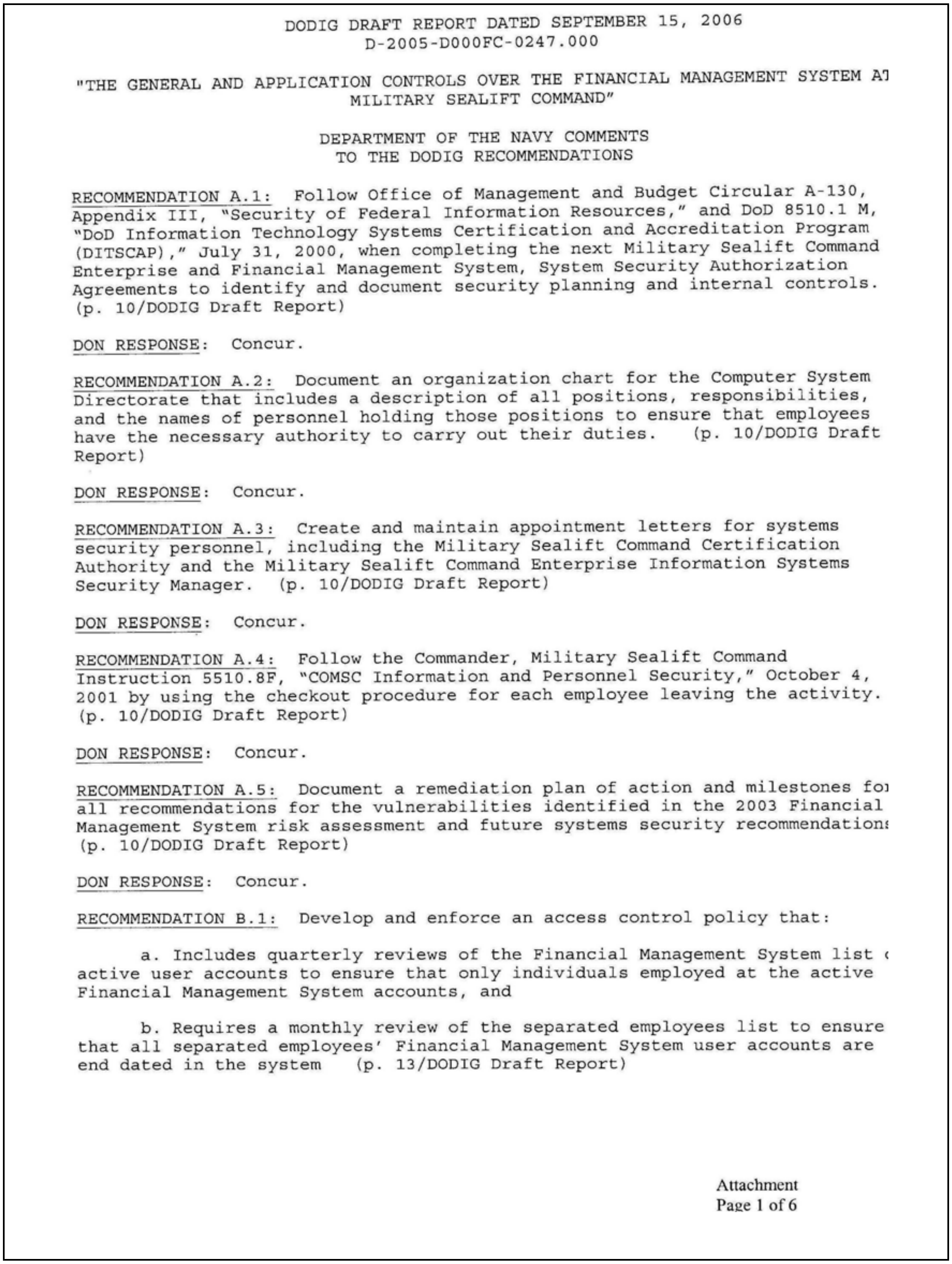
Ref: (a) DoDIG email of 15 Sep 06
(b) DoDIG memo of 15 Sep 06
(c) NAVIG email of 19 Sep 06

As requested by references (a), (b) and (c), Department of the Navy comments are provided to subject draft audit.

for MARK E. EASTON
Director
Office of Financial Operations

Attachments:
As Stated

Copy to:
MSC
NAVIG



DODIG DRAFT REPORT DATED SEPTEMBER 15, 2006
D-2005-D000FC-0247.000

"THE GENERAL AND APPLICATION CONTROLS OVER THE FINANCIAL MANAGEMENT SYSTEM A
MILITARY SEALIFT COMMAND"

DEPARTMENT OF THE NAVY COMMENTS
TO THE DODIG RECOMMENDATIONS

RECOMMENDATION A.1: Follow Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Information Resources," and DoD 8510.1 M, "DoD Information Technology Systems Certification and Accreditation Program (DITSCAP)," July 31, 2000, when completing the next Military Sealift Command Enterprise and Financial Management System, System Security Authorization Agreements to identify and document security planning and internal controls. (p. 10/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION A.2: Document an organization chart for the Computer System Directorate that includes a description of all positions, responsibilities, and the names of personnel holding those positions to ensure that employees have the necessary authority to carry out their duties. (p. 10/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION A.3: Create and maintain appointment letters for systems security personnel, including the Military Sealift Command Certification Authority and the Military Sealift Command Enterprise Information Systems Security Manager. (p. 10/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION A.4: Follow the Commander, Military Sealift Command Instruction 5510.8F, "COMSC Information and Personnel Security," October 4, 2001 by using the checkout procedure for each employee leaving the activity. (p. 10/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION A.5: Document a remediation plan of action and milestones fo all recommendations for the vulnerabilities identified in the 2003 Financial Management System risk assessment and future systems security recommendation (p. 10/DODIG Draft Report)

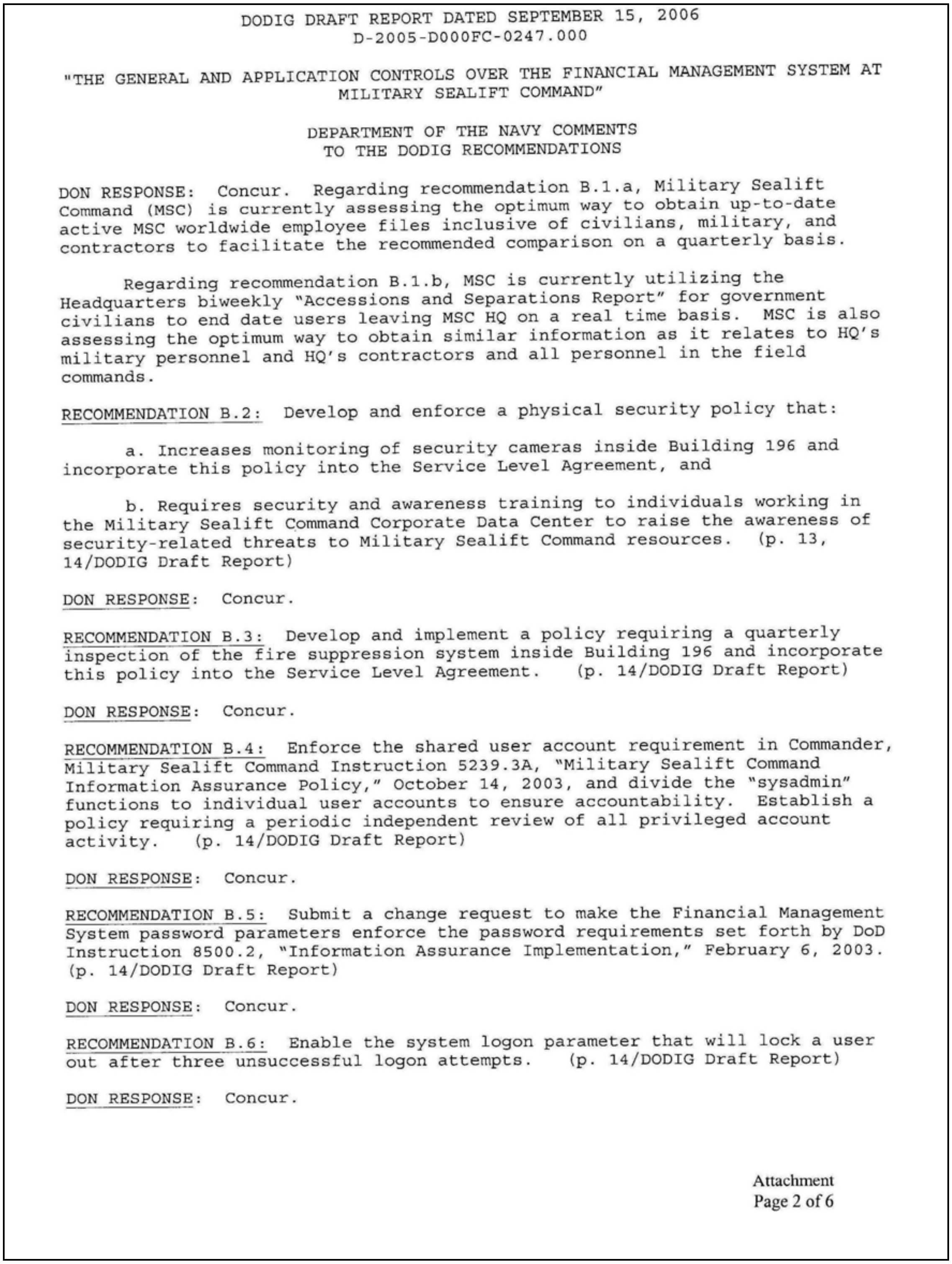
DON RESPONSE: Concur.

RECOMMENDATION B.1: Develop and enforce an access control policy that:

a. Includes quarterly reviews of the Financial Management System list active user accounts to ensure that only individuals employed at the active Financial Management System accounts, and

b. Requires a monthly review of the separated employees list to ensure that all separated employees' Financial Management System user accounts are end dated in the system (p. 13/DODIG Draft Report)

Attachment
Page 1 of 6



DODIG DRAFT REPORT DATED SEPTEMBER 15, 2006
D-2005-D000FC-0247.000

"THE GENERAL AND APPLICATION CONTROLS OVER THE FINANCIAL MANAGEMENT SYSTEM AT MILITARY SEALIFT COMMAND"

DEPARTMENT OF THE NAVY COMMENTS
TO THE DODIG RECOMMENDATIONS

DON RESPONSE: Concur. Regarding recommendation B.1.a, Military Sealift Command (MSC) is currently assessing the optimum way to obtain up-to-date active MSC worldwide employee files inclusive of civilians, military, and contractors to facilitate the recommended comparison on a quarterly basis.

Regarding recommendation B.1.b, MSC is currently utilizing the Headquarters biweekly "Accessions and Separations Report" for government civilians to end date users leaving MSC HQ on a real time basis. MSC is also assessing the optimum way to obtain similar information as it relates to HQ's military personnel and HQ's contractors and all personnel in the field commands.

RECOMMENDATION B.2: Develop and enforce a physical security policy that:

a. Increases monitoring of security cameras inside Building 196 and incorporate this policy into the Service Level Agreement, and

b. Requires security and awareness training to individuals working in the Military Sealift Command Corporate Data Center to raise the awareness of security-related threats to Military Sealift Command resources. (p. 13, 14/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION B.3: Develop and implement a policy requiring a quarterly inspection of the fire suppression system inside Building 196 and incorporate this policy into the Service Level Agreement. (p. 14/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION B.4: Enforce the shared user account requirement in Commander, Military Sealift Command Instruction 5239.3A, "Military Sealift Command Information Assurance Policy," October 14, 2003, and divide the "sysadmin" functions to individual user accounts to ensure accountability. Establish a policy requiring a periodic independent review of all privileged account activity. (p. 14/DODIG Draft Report)

DON RESPONSE: Concur.

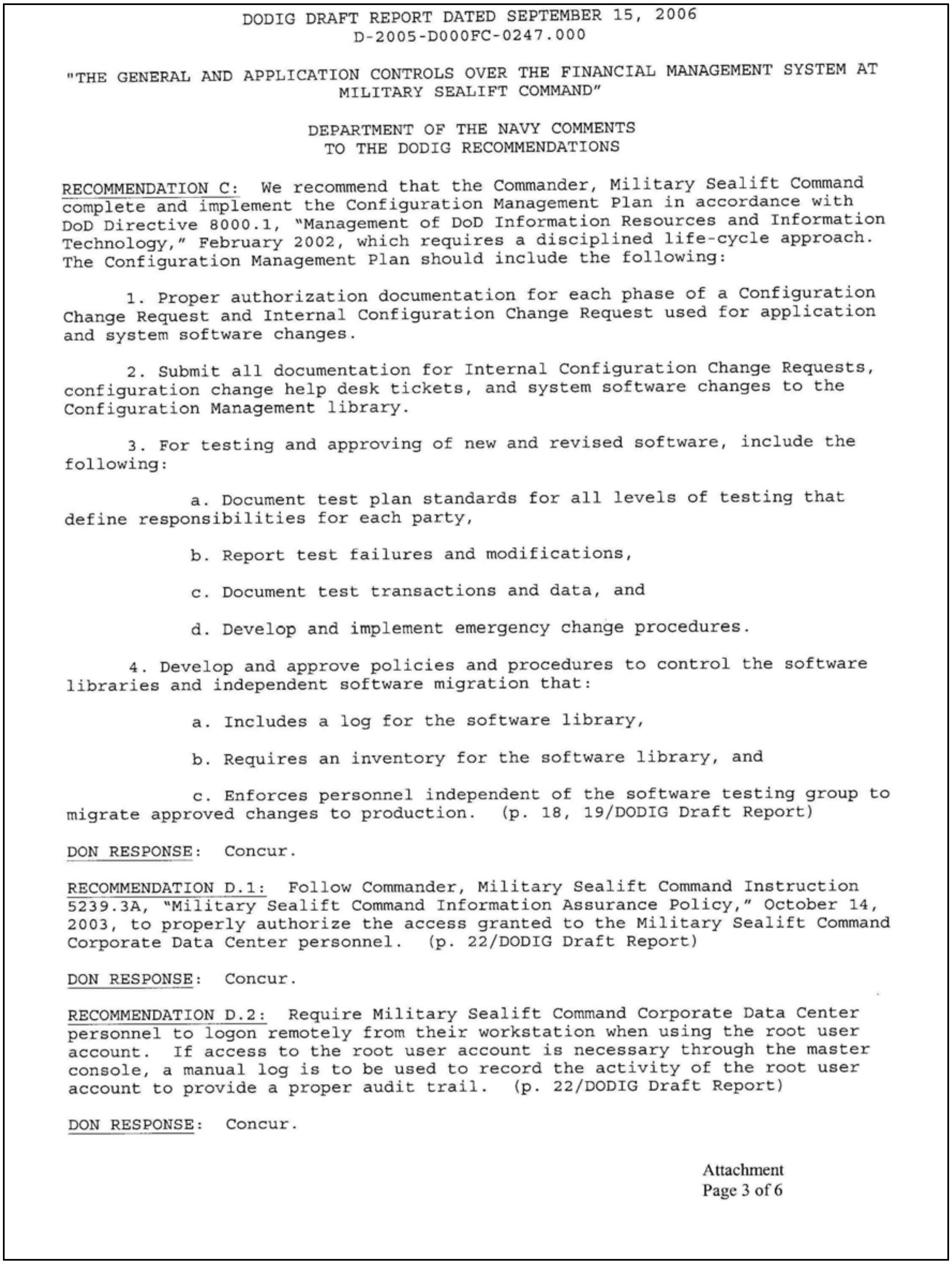
RECOMMENDATION B.5: Submit a change request to make the Financial Management System password parameters enforce the password requirements set forth by DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003. (p. 14/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION B.6: Enable the system logon parameter that will lock a user out after three unsuccessful logon attempts. (p. 14/DODIG Draft Report)

DON RESPONSE: Concur.

Attachment
Page 2 of 6



DODIG DRAFT REPORT DATED SEPTEMBER 15, 2006
D-2005-D000FC-0247.000

"THE GENERAL AND APPLICATION CONTROLS OVER THE FINANCIAL MANAGEMENT SYSTEM AT MILITARY SEALIFT COMMAND"

DEPARTMENT OF THE NAVY COMMENTS
TO THE DODIG RECOMMENDATIONS

RECOMMENDATION C: We recommend that the Commander, Military Sealift Command complete and implement the Configuration Management Plan in accordance with DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 2002, which requires a disciplined life-cycle approach. The Configuration Management Plan should include the following:

1. Proper authorization documentation for each phase of a Configuration Change Request and Internal Configuration Change Request used for application and system software changes.

2. Submit all documentation for Internal Configuration Change Requests, configuration change help desk tickets, and system software changes to the Configuration Management library.

3. For testing and approving of new and revised software, include the following:

a. Document test plan standards for all levels of testing that define responsibilities for each party,

b. Report test failures and modifications,

c. Document test transactions and data, and

d. Develop and implement emergency change procedures.

4. Develop and approve policies and procedures to control the software libraries and independent software migration that:

a. Includes a log for the software library,

b. Requires an inventory for the software library, and

c. Enforces personnel independent of the software testing group to migrate approved changes to production. (p. 18, 19/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION D.1: Follow Commander, Military Sealift Command Instruction 5239.3A, "Military Sealift Command Information Assurance Policy," October 14, 2003, to properly authorize the access granted to the Military Sealift Command Corporate Data Center personnel. (p. 22/DODIG Draft Report)

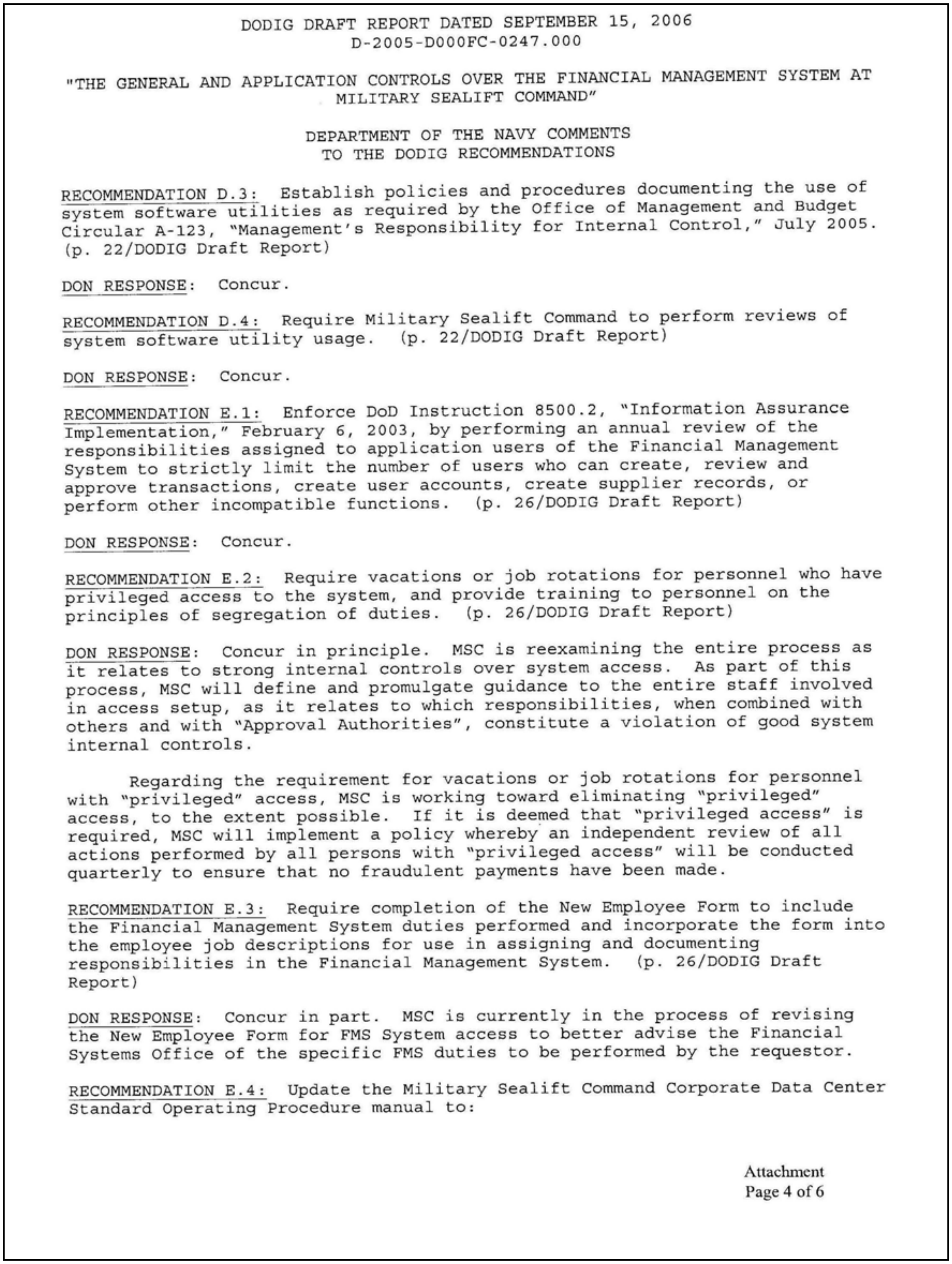
DON RESPONSE: Concur.

RECOMMENDATION D.2: Require Military Sealift Command Corporate Data Center personnel to logon remotely from their workstation when using the root user account. If access to the root user account is necessary through the master console, a manual log is to be used to record the activity of the root user account to provide a proper audit trail. (p. 22/DODIG Draft Report)

DON RESPONSE: Concur.

Attachment
Page 3 of 6

Final Report
Reference



DODIG DRAFT REPORT DATED SEPTEMBER 15, 2006
D-2005-D000FC-0247.000

"THE GENERAL AND APPLICATION CONTROLS OVER THE FINANCIAL MANAGEMENT SYSTEM AT MILITARY SEALIFT COMMAND"

DEPARTMENT OF THE NAVY COMMENTS
TO THE DODIG RECOMMENDATIONS

RECOMMENDATION D.3: Establish policies and procedures documenting the use of system software utilities as required by the Office of Management and Budget Circular A-123, "Management's Responsibility for Internal Control," July 2005. (p. 22/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION D.4: Require Military Sealift Command to perform reviews of system software utility usage. (p. 22/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION E.1: Enforce DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, by performing an annual review of the responsibilities assigned to application users of the Financial Management System to strictly limit the number of users who can create, review and approve transactions, create user accounts, create supplier records, or perform other incompatible functions. (p. 26/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION E.2: Require vacations or job rotations for personnel who have privileged access to the system, and provide training to personnel on the principles of segregation of duties. (p. 26/DODIG Draft Report)

DON RESPONSE: Concur in principle. MSC is reexamining the entire process as it relates to strong internal controls over system access. As part of this process, MSC will define and promulgate guidance to the entire staff involved in access setup, as it relates to which responsibilities, when combined with others and with "Approval Authorities", constitute a violation of good system internal controls.

Regarding the requirement for vacations or job rotations for personnel with "privileged" access, MSC is working toward eliminating "privileged" access, to the extent possible. If it is deemed that "privileged access" is required, MSC will implement a policy whereby an independent review of all actions performed by all persons with "privileged access" will be conducted quarterly to ensure that no fraudulent payments have been made.

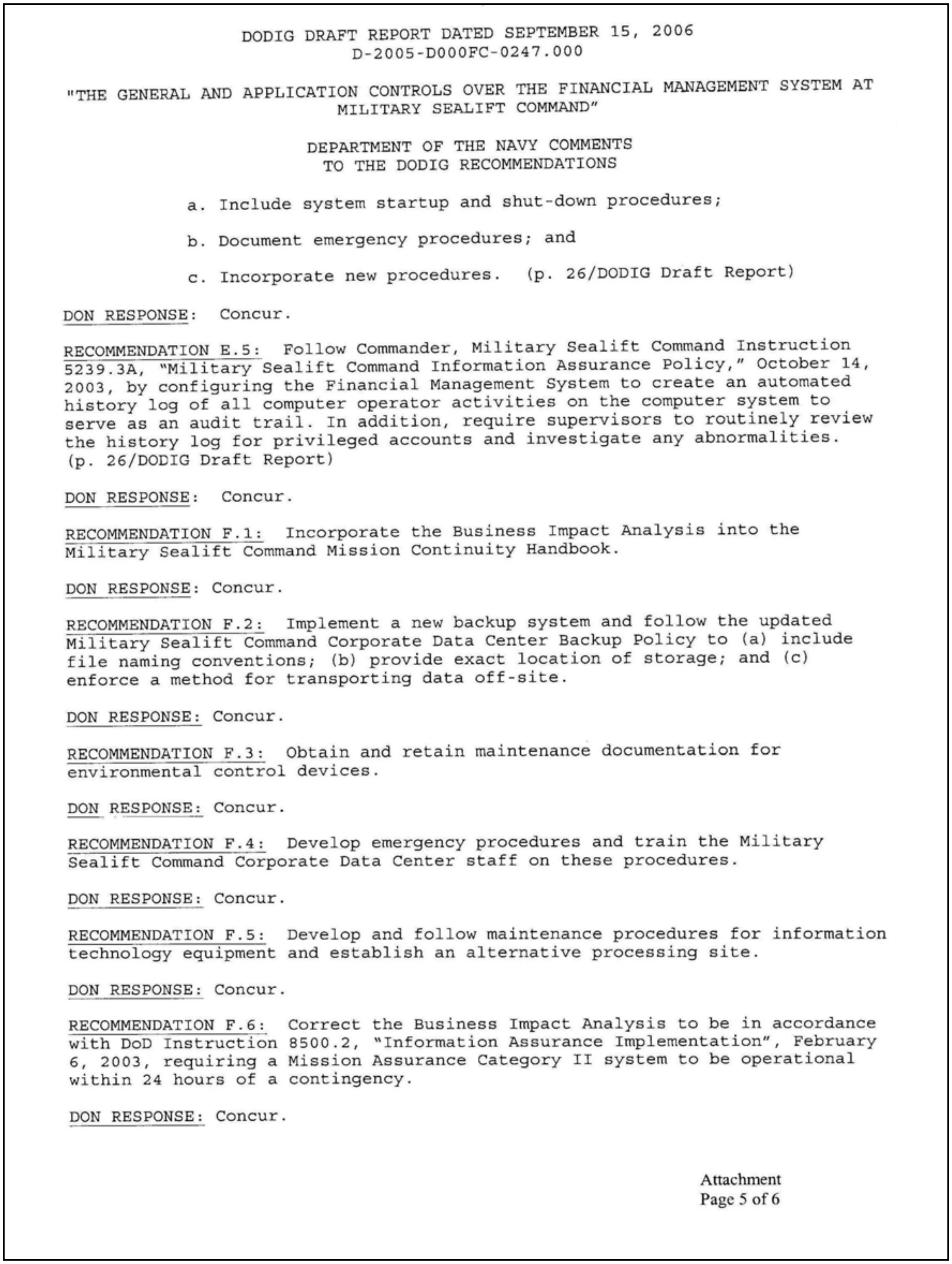
RECOMMENDATION E.3: Require completion of the New Employee Form to include the Financial Management System duties performed and incorporate the form into the employee job descriptions for use in assigning and documenting responsibilities in the Financial Management System. (p. 26/DODIG Draft Report)

Revised
Page 32

DON RESPONSE: Concur in part. MSC is currently in the process of revising the New Employee Form for FMS System access to better advise the Financial Systems Office of the specific FMS duties to be performed by the requestor.

RECOMMENDATION E.4: Update the Military Sealift Command Corporate Data Center Standard Operating Procedure manual to:

Attachment
Page 4 of 6



DODIG DRAFT REPORT DATED SEPTEMBER 15, 2006
D-2005-D000FC-0247.000

"THE GENERAL AND APPLICATION CONTROLS OVER THE FINANCIAL MANAGEMENT SYSTEM AT MILITARY SEALIFT COMMAND"

DEPARTMENT OF THE NAVY COMMENTS
TO THE DODIG RECOMMENDATIONS

a. Include system startup and shut-down procedures;

b. Document emergency procedures; and

c. Incorporate new procedures. (p. 26/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION E.5: Follow Commander, Military Sealift Command Instruction 5239.3A, "Military Sealift Command Information Assurance Policy," October 14, 2003, by configuring the Financial Management System to create an automated history log of all computer operator activities on the computer system to serve as an audit trail. In addition, require supervisors to routinely review the history log for privileged accounts and investigate any abnormalities. (p. 26/DODIG Draft Report)

DON RESPONSE: Concur.

RECOMMENDATION F.1: Incorporate the Business Impact Analysis into the Military Sealift Command Mission Continuity Handbook.

DON RESPONSE: Concur.

RECOMMENDATION F.2: Implement a new backup system and follow the updated Military Sealift Command Corporate Data Center Backup Policy to (a) include file naming conventions; (b) provide exact location of storage; and (c) enforce a method for transporting data off-site.

DON RESPONSE: Concur.

RECOMMENDATION F.3: Obtain and retain maintenance documentation for environmental control devices.

DON RESPONSE: Concur.

RECOMMENDATION F.4: Develop emergency procedures and train the Military Sealift Command Corporate Data Center staff on these procedures.

DON RESPONSE: Concur.

RECOMMENDATION F.5: Develop and follow maintenance procedures for information technology equipment and establish an alternative processing site.

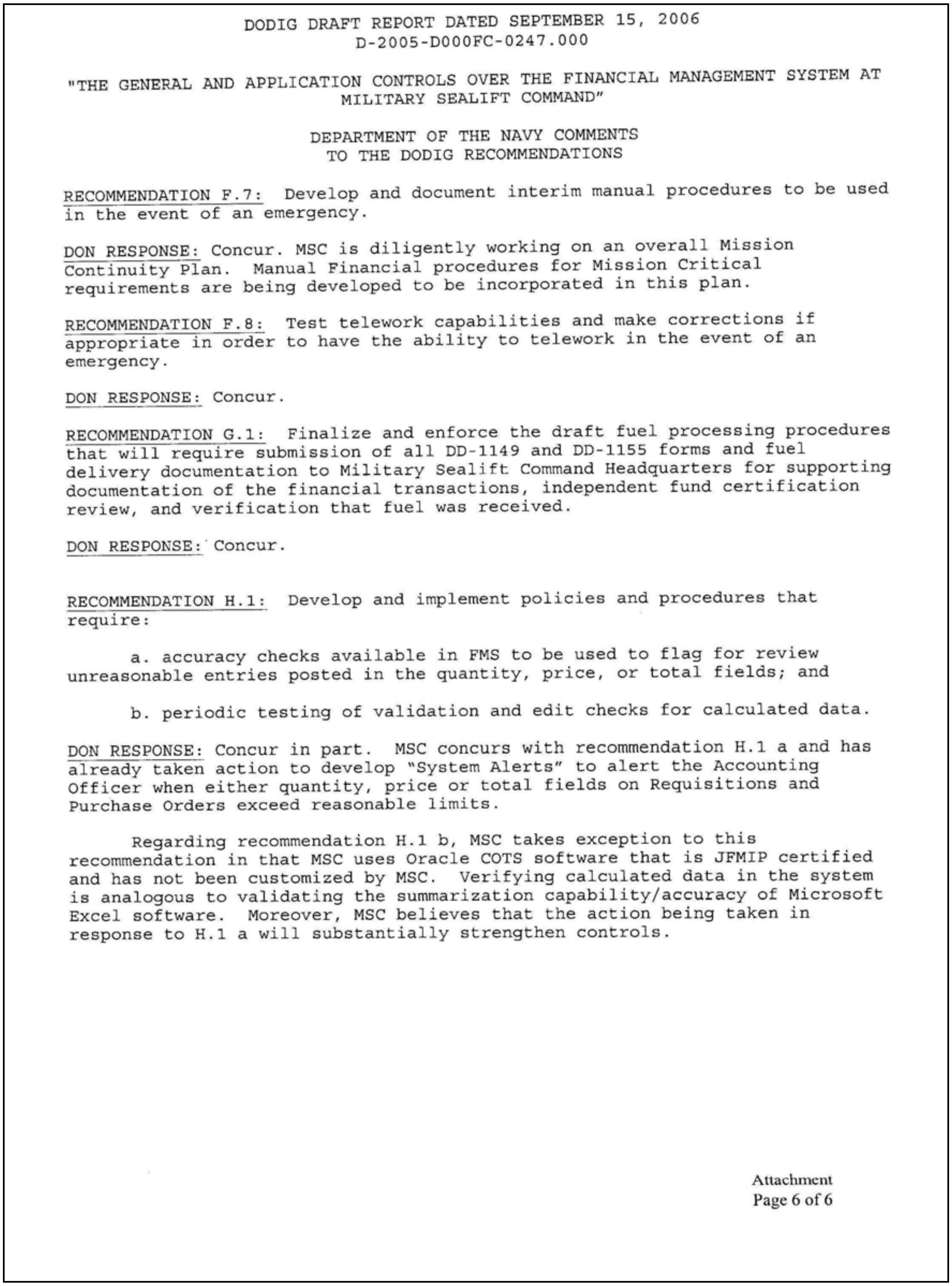
DON RESPONSE: Concur.

RECOMMENDATION F.6: Correct the Business Impact Analysis to be in accordance with DoD Instruction 8500.2, "Information Assurance Implementation", February 6, 2003, requiring a Mission Assurance Category II system to be operational within 24 hours of a contingency.

DON RESPONSE: Concur.

Attachment
Page 5 of 6

Final Report
Reference



DODIG DRAFT REPORT DATED SEPTEMBER 15, 2006
D-2005-D000FC-0247.000

"THE GENERAL AND APPLICATION CONTROLS OVER THE FINANCIAL MANAGEMENT SYSTEM AT MILITARY SEALIFT COMMAND"

DEPARTMENT OF THE NAVY COMMENTS
TO THE DODIG RECOMMENDATIONS

RECOMMENDATION F.7: Develop and document interim manual procedures to be used in the event of an emergency.

DON RESPONSE: Concur. MSC is diligently working on an overall Mission Continuity Plan. Manual Financial procedures for Mission Critical requirements are being developed to be incorporated in this plan.

RECOMMENDATION F.8: Test telework capabilities and make corrections if appropriate in order to have the ability to telework in the event of an emergency.

DON RESPONSE: Concur.

RECOMMENDATION G.1: Finalize and enforce the draft fuel processing procedures that will require submission of all DD-1149 and DD-1155 forms and fuel delivery documentation to Military Sealift Command Headquarters for supporting documentation of the financial transactions, independent fund certification review, and verification that fuel was received.

DON RESPONSE: Concur.

RECOMMENDATION H.1: Develop and implement policies and procedures that require:

a. accuracy checks available in FMS to be used to flag for review unreasonable entries posted in the quantity, price, or total fields; and

b. periodic testing of validation and edit checks for calculated data.

DON RESPONSE: Concur in part. MSC concurs with recommendation H.1 a and has already taken action to develop "System Alerts" to alert the Accounting Officer when either quantity, price or total fields on Requisitions and Purchase Orders exceed reasonable limits.

Regarding recommendation H.1 b, MSC takes exception to this recommendation in that MSC uses Oracle COTS software that is JFMIP certified and has not been customized by MSC. Verifying calculated data in the system is analogous to validating the summarization capability/accuracy of Microsoft Excel software. Moreover, MSC believes that the action being taken in response to H.1 a will substantially strengthen controls.

Revised
Page 46

Attachment
Page 6 of 6

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Defense Financial Auditing Service prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Paul J. Granetto
Patricia A. Marsh
Raymond D. Kidd
Edward A. Blair
Gregory M. Mennetti
Dwayne A. Coulson
Michael B. Dell
Devon R. Houston
Dea M. Algeo
Troy A. Robertson
April D. Taylor
Ann L. Thompson

Text Here

Inspector General
Department of Defense

Text Here