Report No. D-2008-091 May 13, 2008

Inspector General
United States Department of Defense

General Controls of the Capital Asset Management System-Military Equipment

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

CAMS-ME	Capital Asset Management System–Military Equipment
COOP	Continuity of Operations Plan
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
OATS	Ogden Asset Tracking System
IG	Inspector General
P&E	Property and Equipment
SAP	Systems, Applications, and Products in Data Processing
SSAA	System Software Authorization Agreement
SSC San Diego	Space and Naval Warfare Systems Center San Diego, California

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

May 13, 2008

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS/ACQUISITION RESOURCES AND ANALYSIS
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: General Controls of the Capital Asset Management System-Military Equipment (Report No. D-2008-091)

We are providing this report for review and comment. We considered comments from the Director, Acquisition Resources and Analysis and Director, Defense Information Systems Agency when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Director, Acquisition Resources and Analysis comments were partially responsive. We request additional comments on Recommendations B.1. and F.1.c. As a result of new DoD certification and accreditation guidance and management comments, we deleted Recommendation A.2. Therefore, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis provide a corrective action and completion date for Recommendation B.1. and a completion date for Recommendation F.1.c. by June 13, 2008. See findings B and F for the specific management comments required.

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

Patricia A. Marsh

Patricia A. Marsh, CPA
Assistant Inspector General
Defense Financial Auditing Service

Department of Defense Office of Inspector General

Report No. D 2008-091 **May 13, 2008**
(Project No. D2007-D000FN-0124.000)

The General Controls of the Capital Asset Management System-Military Equipment

Executive Summary

Who Should Read This Report and Why? DoD personnel who manage and use the Capital Asset Management System-Military Equipment will be interested in this report. DoD information system program managers and personnel involved in information assurance may also find the report useful. It discusses whether the Capital Asset Management System-Military Equipment's general controls were adequately designed and operating effectively.

Background. The Capital Asset Management System-Military Equipment is the mid-term information technology solution[*] implemented by the DoD to process and report military equipment financial data. Military equipment accounts for three-fourths of DoD General Property, Plant, and Equipment, the line item with the greatest dollar amounts on the balance sheet.

This audit focused on the general controls, which includes:

- security program planning and management,
- access controls,
- application development and change controls,
- system software,
- segregation of duties, and
- service continuity controls.

The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis is the program sponsor for the Capital Asset Management System-Military Equipment; Space and Naval Warfare Systems Center, San Diego, California, is the program management office and is responsible for development including the technical configuration of the application. The Defense Information Systems Agency, Ogden, Utah, maintains the hardware and operating system; the Defense Finance and Accounting Service, Columbus, Ohio, performs the help desk, security, and database administration for the application.

[*] The information technology solution is an automated approach to capitalize military equipment using asset transactional data from the receipt, acceptance, and payment systems.

Results. Our audit determined that management had implemented some controls over entity-wide security program planning and management (finding A), access controls (finding B), application software development and change controls (finding C), system software (finding D), and segregation of duties (finding E). However, we identified internal control weaknesses that affect processing and reporting military equipment financial data. The weaknesses found were related to entity-wide security program planning and management (finding A), access controls (finding B), application software development and change controls (finding C), system software (finding D), segregation of duties (finding E), and service continuity (finding F). The deficient controls created system vulnerabilities that potentially jeopardize the integrity, confidentiality, and availability of data reported by the Capital Asset Management System-Military Equipment. The Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis and the Director, Defense Information Systems Agency 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.

Management Comments and Audit Response. The Director, Acquisition Resources and Analysis provided comments for the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis. The Director, Acquisition Resources and Analysis comments were partially responsive, including one nonconcur and one partially concur. The Director, Defense Information Systems Agency provided comments that were fully responsive. Based on new DoD guidance and comments received from the Director, Acquisition Resources and Analysis, we deleted the recommendation on documenting system firmware. We take exception with the Director, Acquisition Resources and Analysis comments that the controls in place over terminating separated users' accounts comply with guidance or have effectively controlled separated users' accounts. We recommend holding the DoD Components responsible for their users' accounts or providing an alternative control for separated users' accounts. The Director, Acquisition Resources and Analysis plans to rely on Defense Information Systems Agency procedures to restore CAMS-ME to normal operations following a contingency. We recommend documenting or referencing those procedures in the CAMS-ME contingency plan. We request that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis provide comments on this report by June 13, 2008. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Management Actions. We have worked closely with the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis and the Director, Defense Information Systems Agency, and they have taken prompt action by implementing some recommendations prior to the issuance of this report.

Table of Contents

Findings

Appendixes

Management Comments

Background

The Chief Financial Officers Act of 1990 (Public Law 101-576), as amended, mandates the preparation and audit of financial statements for certain agencies. In accordance with the Chief Financial Officers Act and generally accepted accounting principles, DoD is required to capitalize and depreciate the full cost of existing and future acquisitions of military equipment, including modifications and improvements, and report this information in the DoD quarterly and annual financial statements. DoD implemented Capital Asset Management System-Military Equipment (CAMS-ME) to record and value military equipment. To support the DoD goal of achieving auditability of financial statements, we conducted an audit of the general controls over CAMS-ME. General controls over systems are necessary to ensure the integrity, availability, and confidentiality of data processed by those systems.

Capital Asset Management System-Military Equipment. CAMS-ME is the information technology system being implemented to maintain and update military equipment valuation data. It is a DoD information system that is built upon the Systems Applications and Products in Data Processing (SAP) software. CAMS-ME is a mid-term information technology solution that supports the DoD enterprise transition plan. Military equipment accounts for approximately three-fourths of General Property, Plant, and Equipment, the line item with the greatest dollar amounts on the DoD balance sheet.

The Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis, Property and Equipment (P&E) Policy Office (Policy Office) deployed CAMS-ME in two increments. The first increment was deployed in June 2006 and the second increment was deployed on January 31, 2008. Increment 1 includes an interface with the Business Enterprise Information Services to collect expenditure data. Component representatives also use the CAMS-ME Web-based interface to update the status of military equipment assets. Therefore, Increment 1 provides the ability to calculate military equipment value using the average cost methodology. The average cost methodology values assets by calculating average costs from program budgetary data.

The P&E Policy Office designed Increment 2 to value military equipment based on the contract cost methodology. The contract cost methodology values assets by acquisition costs, derived from a contract, and the cost of embedded Government furnished material. Both valuation methodologies reside in CAMS-ME. Programs with new contract actions are to be valued using the contract cost methodology with Increment 2 deployment.

CAMS-ME is supported by the P&E Policy Office in Arlington, Virginia; the Space and Naval Warfare System Center (SSC) in San Diego, California; the Defense Information Systems Agency (DISA) in Ogden, Utah; and the Defense Finance and Accounting Service DFAS in Columbus, Ohio. The Army, Navy, Air Force, Marine Corps, and Other Defense Agencies use CAMS-ME to process and report military equipment financial data.

Under Secretary of Defense for Acquisition, Technology and Logistics/Acquisition Resources and Analysis. The Under Secretary of Defense for Acquisition, Technology, and Logistics and the Under Secretary of Defense (Comptroller) established the P&E Policy Office in December 2000 to ensure a consistent military equipment valuation methodology. The P&E Policy Office is the program sponsor for CAMS-ME and is responsible for administrative configuration management. These responsibilities include assigning a representative to Chair and be a Voting Member of the configuration control board, ensuring the implementation of approved changes, and coordinating and scheduling all releases.

Space and Naval Warfare Systems Center-San Diego. SSC San Diego is the program management office responsible for the technical configuration of the SAP application before production. These technical configuration management responsibilities include creating configuration items, customizing development changes, communicating transport requests to P&E Policy Office and DFAS Columbus, and participating in the functional configuration audits. SSC San Diego also provides help desk support for CAMS-ME.

Defense Information Systems Agency-Ogden. DISA Ogden is responsible for coordinating, scheduling, and managing all hardware, operating systems, networks, and non-SAP software environments with input from CAMS-ME project personnel. The information processing services conducted by DISA Ogden include operating and maintaining the processing site, computer hardware, communications hardware, suite of operating system and software, data backup and tape management, and assisting in problem resolution.

Defense Finance and Accounting Service-Columbus. DFAS Columbus is responsible for the configuration management of the SAP application once it has been developed and tested. This includes managing the promotion of software configuration and custom development from initial development to quality assurance to production. In addition, DFAS Columbus manages configuration items for configuration management control and reporting, coordinates with the SSC San Diego Development Team to execute the SAP Transport Management System Instructions, and manages all application and database maintenance and upgrades. The CAMS-ME Help Desk is also located at DFAS Columbus and assists CAMS-ME users with resetting passwords, answering questions, or resolving any technical difficulties they may encounter. Other responsibilities include testing, training, security, and Web-site development.

Objectives

The overall objective was to assess the integrity, availability, and confidentiality of data processed by CAMS-ME. Specifically, we determined whether the computer and computer-related controls over CAMS-ME were adequate. The general control testing included examining the entity-wide security program planning and management, access controls, application software development and change control, system software, segregation of duties, and service continuity. See Appendix A for a discussion of the scope and methodology.

Review of Internal Controls

We identified material internal control weaknesses for the P&E Policy Office and DISA as defined by DoD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006. The P&E Policy Office did not have CAMS-ME general controls in place to:

- ensure that the CAMS-ME system security authorization agreement was properly documented,
- properly handle a separated user's account,
- establish adequate password parameters for CAMS-ME,
- monitor or investigate unauthorized access attempts,
- adequately document testing of emergency configuration changes,
- segregate incompatible duties,
- prioritize computerized operations, and
- develop and document a comprehensive contingency plan.

DISA Ogden did not implement controls over physical software libraries, monitor access to and use of system software, implement system software change controls, and document a comprehensive contingency plan. Implementing Recommendations A., B.1, B.2, C., D.1, D.2, E.1, E.2, F.1, and F.2 will improve the general controls over CAMS-ME. We will provide a copy of the final report to the senior official responsible for internal controls in the P&E Policy Office and DISA Ogden.

A. Entity-Wide Security Program Planning and Management

The P&E Policy Office implemented many security program planning and management controls. Specifically, management adequately:

- performed risk assessments in accordance with DoD policy,
- established an information system security management structure,
- implemented a security-related personnel procedure,
- monitored the effectiveness of the security program, and
- documented and implemented security planning and management controls over CAMS-ME.

However, the P&E Policy Office did not include an incident response plan and a description of system firmware[1] in the CAMS-ME system security authorization agreement (SSAA). The P&E Policy Office did not include these items because they did not follow Federal and DoD policy for preparing security plans. As a result, there is an increased risk of a system outage and access to, changes to, and deletion of data by unauthorized users.

Security 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 and for developing, implementing, and monitoring effective security procedures. The P&E Policy Office, DISA Ogden, and DFAS Columbus were responsible for security planning and management controls.

Periodic Risk Assessments

The P&E Policy Office, DISA Ogden, and DFAS Columbus adequately performed risk assessments for CAMS-ME and the DISA Ogden non-classified internet protocol router network. The P&E Policy Office and DISA Ogden performed and documented required certification and accreditation testing. Management accepted risks and developed plans of action and milestones for the weaknesses identified in the risk assessments. These controls help to ensure that all threats and vulnerabilities are identified and considered according to the level of risk in establishing security controls.

[1] Firmware is programming that is stored permanently in a hardware device allowing reading and executing of the software.

Security Management Structure

The P&E Policy Office, SSC San Diego, DISA Ogden, and DFAS Columbus adequately established an information system security management structure. Management had an organizational chart for CAMS-ME that identified personnel and their titles. In addition, management documented job descriptions and appointment letters for security personnel. The P&E Policy Office, SSC San Diego, DISA Ogden, and DFAS Columbus implemented an ongoing security awareness program and employees were aware of security policies. These controls assist in employee awareness of the system and application rules, personnel's responsibilities, and their expected behavior.

Security-Related Personnel Procedures

The P&E Policy Office, SSC San Diego, DISA Ogden, and DFAS Columbus implemented effective security-related personnel procedures. They performed background investigations for new hires and reinvestigations within the proper time frame for current employees. DISA Computing Services required Single Scope Background Investigations for all privileged users. Management provided appropriate security training and monitored training records. These controls reduce the risk of hiring unqualified or untrustworthy individuals, providing terminated employees opportunities to impair entity operations or assets, failing to detect unauthorized employee actions, lowering employee morale, and allowing staff expertise to decline.

Information Systems Security Program

The P&E Policy Office and DISA Ogden adequately monitored the effectiveness of the security program. Management identified vulnerabilities that occurred within the past 3 years. The Information Assurance Officer adequately notified the designated approving authority when a significant vulnerability affected the acceptable risk level for the system. In addition, management implemented corrective actions. These controls are important to identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.

System Security Program Plan

The P&E Policy Office did not adequately document the CAMS-ME SSAA. Management did not include an incident response plan and a description of system firmware. Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and DoD Directive 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000, require organizations to include an incident response plan and procedures in Appendix K of the SSAA. In addition, DITSCAP requires that the system architecture include a detailed explanation of the system firmware. The P&E Policy Office did not include an incident response plan and description of system firmware because management did not follow Office of Management and Budget Circular A-130 and DITSCAP policy.

Incident Response Plan. The CAMS-ME SSAA included a Vulnerability Assessment Program Charter, March 6, 1998, which established the CAMS-ME management structure, assigned areas of responsibility, and outlined the delegation of authority. However, the Vulnerability Assessment Program Charter was outdated and did not detail an incident response plan for security events. As a result, there is an increased risk that a security event could occur and will not be properly addressed and corrected. Management has taken action by developing their draft "Capital Asset Management for Military Equipment, Incident Response Reporting Plan for CAMS-ME," September 28, 2007. To further mitigate this risk, the P&E Policy Office should finalize the draft incident response plan and include it in the SSAA to ensure that procedures are clear, allowing security controls to be consistently applied.

Description of Firmware. The CAMS-ME SSAA System Architecture Description identified and described the system hardware, software, interfaces, data flows, and accreditation boundary. However, the SSAA System Architecture Description did not include a description of system firmware. As a result, there is an increased risk of compatibility issues.

We deleted the recommendation to include system firmware in the CAMS-ME SSAA based on the issuance of new DoD guidance and comments from the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis. DoD Instruction 8510.01, "Defense Information Assurance Certification and Accreditation Process," November 28, 2007, replaced DITSCAP. However, at the time of our audit, the CAMS-ME authority to operate was granted under DITSCAP. The DoD Information Assurance Certification and Accreditation Process does not specifically require the documentation of system firmware. The National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, suggests documenting all system resources including firmware. The Director, Acquisition Resources and Analysis identified a brief description of the storage area network in the CAMS-ME System Architecture and Requirements Allocation Description. However, she did not include details of the firmware. We do suggest the Under Secretary of Defense Acquisition, Technology, and Logistics/Acquisition Resources and Analysis document all system resources, including firmware, for security and business continuity purposes. See the Management Comments section of the report for the full text of the comments.

Recommendations, Management Comments, and Audit Response

Deleted and Renumbered Recommendations. As a result of new DoD guidance and management comments, we deleted recommendation A.2. Draft Recommendation A.1. has been renumbered as Recommendation A.

A. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis finalize the draft "Capital Asset Management for Military Equipment, Incident Response Reporting Plan for CAMS-ME," September 28, 2007, and include it in the System Security Authorization Agreement to comply with Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and DoD Directive 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," July 31, 2000.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis completed an incident response plan exercise on December 19, 2007, which included a review of the incident response plan. In addition, she included the incident response plan in the CAMS-ME certification and accreditation package, which was provided to the designated approving authority as required by DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process," November 28, 2007.

Audit Response. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed.

B. Access Controls

The P&E Policy Office effectively implemented several system access controls. Specifically, management identified the CAMS-ME resource and system criticality levels and established adequate physical controls to protect system information. In addition, management developed adequate access control procedures to obtain access to the system and handle inactive accounts. However, the P&E Policy Office did not properly manage account access for employees that had left Government service, establish adequate password parameters for CAMS-ME, and monitor or investigate unauthorized access attempts. The P&E Policy Office did not establish adequate access controls because they did not properly create and follow access control policies and procedures. As a result, there is an increased risk of unauthorized access, modification, and deletion of software and data in CAMS-ME.

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. The P&E Policy Office, SSC San Diego, DISA Ogden, and DFAS Columbus were responsible for CAMS-ME access controls.

Classification of Information Resources

The P&E Policy Office appropriately identified the CAMS-ME resource and system criticality levels as required by DITSCAP. Management identified CAMS-ME as a sensitive but unclassified system. The P&E Policy Office also established a mission assurance category III system criticality level. Classification of information resources is important when defining the acceptable risk for the system in meeting the mission responsibilities and defining the type and sensitivity of data processed by the system. Management established access controls based on the classifications identified.

Authorized Users

The P&E Policy Office implemented procedures for requesting access and handling inactive user accounts. Management documented system access request forms, assigned roles based on the system access request forms, and reviewed accounts for inactivity. However, management did not properly manage system account access for employees who had left Government service.

Since the inception of CAMS-ME, management did not properly deactivate account access for both individuals that had left Government service. Specifically, as of May 17, 2007, one of the individuals with CAMS-ME access had retired from a Government position and returned as a contractor. This individual retained all rights and privileges granted from his system access request provided as a Government employee. The second individual retired from the Government on February 3, 2007; however, the individual's account remained active until March 21, 2007. National Institute of Standards and Technology (NIST) Special Publication 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. Controls over account access were not adequate because the P&E Policy Office did not establish procedures requiring the Components to notify the help desk when employees left Government service or no longer required access. As a result, there is an increased risk for separated employees to access CAMS-ME, damage system operations, and alter data within the system, which could lead to misstatements of military equipment information. To mitigate these risks, the P&E Policy Office should establish clear procedures in the memorandums of understanding for handling accounts of separated employees to include transfer, promotion, retirement, and unfriendly termination.

Physical and Logical Controls

Management established adequate physical controls over the CAMS-ME hardware. However, the P&E Policy Office did not establish adequate logical controls. Specifically, management did not enable SAP password parameters to define the period for passwords created for new accounts, established by the user, and reset by the help desk.

DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, requires management to enforce automatic expiration of passwords by implementing system mechanisms. In addition, "CAMS-ME SAP Password Profile Parameters Policy," April 25, 2006, requires 17 SAP parameters, including those identified above, to be set for CAMS-ME. The P&E Policy Office did not set the password parameters because management did not follow the CAMS-ME password policy. As a result, there is an increased risk that an individual could gain unauthorized access to CAMS-ME and delete or modify critical system programming and data. Management has taken action and mitigated this risk by ensuring that all capable functions are enabled for the 17 password parameters.

Monitor Access and Investigate Security Violations

The P&E Policy Office performed a monthly review of the CAMS-ME activity logs. However, management did not monitor or investigate suspicious activity, such as unsuccessful access attempts. DoD Instruction 8500.2 requires the review of audit logs from all available sources for indications of inappropriate or unusual activities, and tools are available for the review of audit records and for report generation. Audit logs are critical for providing information related to unauthorized and suspicious activities. Controls over monitoring and investigating suspicious activity were not adequate because the P&E Policy Office did not establish procedures for reviewing available audit logs. As a result, there is an increased risk that inappropriate access or activity would go undetected. To mitigate this risk, management should develop procedures for monitoring and investigating unsuccessful access attempts.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis:

1. Incorporate into the Memorandums of Agreement the requirement for supervisors to notify the help desk when employees with access to the Capital Asset Management System-Military Equipment separate from the Component or no longer require access to ensure that the user accounts are deactivated, in accordance with National Institute of Standards and Technology Special Publication 800-12, "An Introduction to Computer Security," October 1995.

Management Comments. The Director, Acquisition Resources and Analysis partially concurred. The Director, Acquisition Resources and Analysis identified the system access request form and account termination policy of 100 days as controls in place.

Audit Response. The Director, Acquisition Resources and Analysis comments were partially responsive. Terminations of access of these two separated employees were not controlled as recommended by the National Institute of Standards and Technology. The system access request form only places responsibility on the employee for alerting management of their departure. In the two cases, this control did not ensure the timely termination of the accounts. Separated user accounts pose a considerable risk to the system. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis enter an agreement with the users' employers—the DoD Components—to provide another layer of accountability for users' accounts or to develop another control to effectively manage separated users' accounts. We request that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis provide a corrective action to control separated users' accounts and a completion date in her comments on the final report.

2. Develop and implement a security policy that includes monitoring and investigating suspicious activity, such as unsuccessful logon attempts as required by DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis plans to update the existing security policy to include monitoring suspicious activity at the operating system and network layers by August 2008.

Audit Response. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed. In addition, we suggest the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis include monitoring the application layer when updating this policy.

C. Application Software Development and Change Control

The P&E Policy Office documented a structured configuration management plan, implemented controls over testing and approving new and revised software, and implemented controls over migrating changes from development to production. However, the P&E Policy Office did not adequately document testing of emergency configuration changes, and DISA Ogden did not implement controls over physical software libraries. These application change control weaknesses occurred because the P&E Policy Office did not follow emergency change procedures for documenting testing of emergency configuration changes, and DISA Ogden did not establish procedures for controlling physical software libraries. As a result, there is an increased risk that software changes may be implemented before evaluating test results and CAMS-ME software may not be available for installing on or updating a CAMS-ME server.

Application Change Control

Application software supports a specific operation or business process. Establishing controls over the modification of application software helps to ensure that only authorized programs and modifications are implemented. Organizations can accomplish this by instituting policies, procedures, and techniques that help ensure all programs and program modifications are properly authorized, tested, and approved, and ensure access to and distribution of programs is carefully controlled. The P&E Policy Office, SSC San Diego, DISA Ogden, and DFAS Columbus are responsible for configuration management.

Authorization of Processing Features and Program Modifications

The P&E Policy Office, SSC San Diego, and DFAS Columbus documented and implemented procedures for CAMS-ME configuration management responsibilities. The procedures established requirements to involve the user throughout the process, provided guidance to staff with varying levels of skill and experience, and documented configuration management changes. The P&E Policy Office consistently documented and approved system changes using standard forms. In addition, they enforced policies prohibiting the use of public domain and personal software. These controls reduce the risk of implementing of unauthorized programs and modifications.

Testing and Approval of all New and Revised Software

The P&E Policy Office implemented controls over testing and approving new and revised software. Management provided sufficient documentation to support testing and approval for 12 reviewed changes. However, management did not provide documentation to support testing of emergency changes. The P&E Policy Office "Capital Asset Management System-Military Equipment (CAMS-ME) Configuration Control Board Procedures" states that the systems integrator should work with the help desk to document emergency changes within 24 hours after the change. Management did not properly document testing of emergency changes because they did not follow configuration control board procedures. As a result, there is an increased risk that errors or unauthorized modifications could be implemented and have an impact on the reliability, confidentiality, and availability of CAMS-ME data. To mitigate this risk, the P&E Policy Office should enforce the configuration control board procedure that requires documenting the tests of emergency changes.

Controls over Software Libraries

The P&E Policy Office had adequate controls over migrating changes from development to quality assurance and from quality assurance to production. Management used the SAP Transport Management System to ensure proper migration and tracking for application changes. However, DISA Ogden did not implement controls over the CAMS-ME Windows® physical software library. A physical software library is a storage repository for definitive authorized versions of all software. It provides assurance that the official approved version of all software is available and provides a record of old program versions. Management did not maintain a log to record the check-in and check-out of software. National Institute of Standards and Technology Special Publication 800-53, "Information Security," February 2005, recommends implementing controls over the information system and media libraries, including the authorization of delivery to and removal from the library. Controls over the CAMS-ME Windows® physical software library were not adequate because management did not develop procedures to control the Windows® physical software libraries. As a result, there is an increased risk that CAMS-ME software would not be available for installing on or updating a CAMS-ME server. DISA Ogden has taken action by developing standard operating procedures for Windows® physical software library controls that were effective August 1, 2007. The procedures include maintaining a spreadsheet of all current software on hand and checked out and requires the check-out and check-in process through a librarian.

Recommendations, Management Comments and Audit Response

Renumbered Recommendation. Draft recommendation C.1. has been renumbered to Recommendation C.

C. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis properly document testing of emergency configuration changes to comply with the "Capital Asset Management System-Military Equipment (CAMS-ME) Configuration Control Board Procedures."

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis stated that the exception noted in the finding occurred at the inception of the application and policies and procedures have been in place to control emergency changes since March 2007.

Audit Response. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed.

D. System Software

The P&E Policy Office and DISA Ogden documented and effectively implemented many required controls over access to CAMS-ME system software. However, DISA Ogden did not effectively monitor access to, use of, and control changes to system software. Management did not monitor access to and use of system software and did not implement system software change controls because they did not follow DISA policies for system audit log review and vulnerability management, and they did not have adequate procedures for tracking asset information. As a result, there is an increased risk that unauthorized access to system software could occur without being identified, vulnerabilities could be exploited, and management could make decisions without complete software and version information for CAMS-ME servers.

System Software Controls

System software is a set of programs designed to operate and control the processing activities of computer equipment. System software assists with controlling and coordinating the input, processing, output, and data storage. The CAMS-ME application is installed on Microsoft® Windows® Server 2003, and the database is installed on servers with the UNIX operating system. DISA Ogden is responsible for maintaining CAMS-ME system software and related access controls. The P&E Policy Office is responsible for maintaining the database.

Access to System Software

DISA Ogden implemented controls to protect the integrity of CAMS-ME. These controls included employing automated mechanisms to support managing user accounts, disabling accounts after time requirements expired, and appropriate auditing of user accounts. These controls help ensure that system software is adequately protected and that security features are not bypassed.

Monitor Access to and Use of System Software

DISA Ogden implemented controls, including system audit logs and an automated tool to track changes to critical system files. However, DISA Ogden did not implement controls to fully monitor access to and use of system software. Specifically, management did not implement controls over reviews of system audit logs and vulnerability management.

Audit Log Reviews. Management did not implement an independent review of the system audit logs. The system administrator explained that he reviewed the audit logs for anomalies. However, no one else performed reviews or analyzed the logs. DISA Access Control STIG, "Security Technical Implementation Guide," Version 1, Release 1, June 2006, requires not only a review of system audit logs, but also suggests, as a best practice, an independent review and analysis of system audit logs. It further requires that a security manager, information assurance manager, or other designated person review the audit logs for trends and anomalies, which can serve as a preventive and detective control against down-time and attacks on the system. In addition, DISA Interoffice Memorandum, "Auditing Requirements," May 7, 2007, provides guidance for configuring system audit logs to focus limited resources on the most important audit information while DoD pursues an enterprise solution to fully address system audit requirements. The system audit logs were not independently reviewed because management did not follow DoD guidance. Management also stated there was too much data in the logs to review. As a result, there is an increased risk that unauthorized system changes, including installation of unauthorized software, addition of new users, and profile changes to current users, could be made without being detected.

No recommendation is being made to address CAMS-ME Windows® system audit logs because management was responsive to a recommendation made in DoD Inspector General (IG) Report D-2006-086, "Report on the General and Applications Controls at the Defense Information Systems Agency, Center for Computing Services," May 18, 2006. Recommendation C.2. of that report recommended that the Chief, Field Security Operations develop and implement consistent procedures across the entity to create, monitor and review, protect, and maintain system audit trails to comply with the Security Technical Implementation Guides to provide a standard set of auditing tools. The Chief, Field Security Operations concurred and stated that an Enterprise Wide Solutions Steering Group initiative, called the Tier III Security Incident Manager, was established in 2007 to acquire an audit capability. The solution is a DoD-level initiative, and DISA plans to leverage the Tier III Security Incident Manager solution when it becomes available to DoD.

Vulnerability Management. Management did not address CAMS-ME server vulnerabilities in a timely manner. DISA separates the vulnerabilities into one of the following four categories based on severity.

- **Category I.** Any vulnerability that may provide an attacker immediate access into a machine, allow super-user access, or bypass a firewall.
- **Category II.** Any vulnerability that provides information that has a high potential of giving access to an unauthorized person or provides an unauthorized person the means to circumvent security controls.
- **Category III.** Any vulnerability that provides information that potentially could lead to unauthorized access.
- **Category IV.** Any other vulnerabilities that would potentially contribute to degraded security.

The Windows® servers contained 3 Category I and 68 Category II vulnerabilities[2] that remained open past the allowed time frame. The UNIX servers contained 18 Category II vulnerabilities that remained open past the allowed time

[2] Category III and IV vulnerabilities were not analyzed because the time period in which action must be taken, 180 and 1000 days respectively, was outside of the scope of our audit.

frame. The DISA Information Assurance Vulnerability Alert Handbook, February 2007, states information assurance vulnerability alerts must be mitigated within a specified time frame or, in the case where it cannot be resolved, a plan of action must be documented and approved. It further states that vulnerabilities must be corrected, have a mitigation plan in place, or an updated plan of action and milestones within 25 days for Category I or 60 days for Category II. The vulnerabilities existed because management did not follow vulnerability management policy. As a result, there is an increased risk of successful attacks on the system which could impact the reliability, availability, and confidentiality of CAMS-ME data. To mitigate this risk, management should immediately address the identified Category I and II vulnerabilities and appropriately address other identified vulnerabilities within the specified policy time frames.

Control System Software Changes

DISA Ogden documented and implemented controls for system software changes, including tracking problems with system software and alerting customers of down-time required to perform system maintenance. However, DISA Ogden did not record software and software version information in the Ogden Asset Tracking System (OATS) in a timely manner. Specifically, Windows® system administrators did not maintain current system software information in OATS for all 19 of the CAMS-ME Windows® servers. Before we requested the CAMS-ME system information in March 2007, system administrators had not updated system software information since September 2006. The "DISA Computing Services Operations Operational Change and Configuration Management Plan," March 21, 2006, requires quarterly census audits to compare and reconcile property management and asset accounting records. According to the DISA Systems Management Center Ogden Configuration Management Plan, March 2006, system administrators are responsible for updating the information in OATS. The system administrators did not update the CAMS-ME Windows® software information in a timely manner because the DISA Systems Management Center Ogden Configuration Management Plan did not establish a time frame for updating system information in OATS. As a result, there is an increased risk that management would not have complete and updated software and software version information to make decisions regarding vulnerabilities, licensing, interconnectivity, and recovery. To mitigate this risk, DISA Ogden should update the Configuration Management Plan to include a requirement for updating the OATS data quarterly, at minimum, for new versions of installed system software and for conducting audits of the information for validity.

Recommendations, Management Comments, and Audit Response

D.1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis address Capital Asset Management System-Military Equipment database vulnerabilities within the specified time frames to comply with DISA Information Assurance Vulnerability Alert Handbook, February 2007.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis has documented an ongoing issue with delayed critical patch updates with the Systems, Applications, and Products in Data Processing implementation and will document a plan of action and milestones in the vulnerability management system.

Audit Response. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed.

D.2. We recommend that the Director, Defense Information Systems Agency:

a. Address Capital Asset Management System-Military Equipment Windows® server vulnerabilities within the specified time frames to comply with DISA Information Assurance Vulnerability Alert Handbook, February 2007.

b. Update the DISA Systems Management Center Ogden Configuration Management Plan, March 2006, to include a requirement for updating the Ogden Asset Tracking System data at a minimum on a quarterly basis for new versions of system software installed. The Configuration Management Plan should also require periodic audits of the information to comply with the "DISA Computing Services Operations Operational Change and Configuration Management Plan," March 21, 2006.

Management Comments. The Defense Information Systems Agency concurred. The Director, Defense Information Systems Agency Computing Services plans to develop a plan of action and milestones for all Windows and Unix category I and II vulnerabilities by May 5, 2008. In addition, the Director, Defense Information Systems Agency Computing Services has already taken action and provided the audit team with the updated configuration management plan in November 2007.

Audit Response. We commend the Director, Defense Information Systems Agency for taking prompt corrective action. The Director, Defense Information Systems Agency comments were responsive and conform to requirements; no additional comments are needed.

E. Segregation of Duties

The P&E Policy Office documented procedures for personnel to follow in performing their job functions and established access controls to separate the development, testing, and production environments. However, management did not properly segregate incompatible duties. Segregation of incompatible duties was inadequate because the P&E Policy Office did not follow DoD guidance. As a result, there is an increased risk of unauthorized or erroneous posting of, changes to, or deletion of transactions within CAMS-ME.

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. Segregation of duties reviewed includes duties performed by the project team, development personnel, and the help desk at the P&E Policy Office, SSC San Diego, and DFAS Columbus.

Operating Procedures

The P&E Policy Office effectively controlled personnel activity through the use of operating procedures. In conjunction with SSC San Diego and DFAS Columbus, the P&E Policy Office documented operating procedures for the development, help desk, and security management personnel. Management also reviewed and approved configuration and administration changes that effected the operation of CAMS-ME. These procedures help prevent and detect unauthorized personnel actions such as fraudulent transactions and improper implementation of program changes.

Segregate Incompatible Duties

The P&E Policy Office implemented access controls to segregate duties, such as creating separate development, testing, and production environments. In addition, management developed, assigned, and monitored CAMS-ME profiles to limit user activity and provided project team, development, and help desk personnel with information necessary to understand their job functions. However, they did not develop and implement controls to segregate all functions. Specifically, management created help desk and generic data input user accounts that did not allow for least privilege and separation of duties principles.

Help Desk User Accounts. Management assigned more profiles to help desk user accounts than were necessary to perform their job functions. The profiles provided them the ability to create, edit, and delete transactions within CAMS-ME. According to the DFAS Columbus, "CAMS-ME Operations Support Team Management Plan," the primary responsibilities of the help desk at DFAS Columbus were to perform user administration and record transaction problems. The transaction problems were to be resolved by personnel at the P&E Policy Office, not the help desk. DoD Instruction 8500.2, “Information Assurance Implementation,” February 6, 2003, requires the Information Assurance Manager to develop and implement a role-based access scheme that implements the principles of least privilege and separation of functions. Management assigned the help desk user accounts these profiles because they did not follow DoD policy on segregation of duties and least privilege principles. As a result, there is an increased risk of unauthorized entries, corrections, or deletions of transactions within CAMS-ME. To mitigate this risk, management should review the help desk user accounts to ensure that they have enough, but not excessive, CAMS-ME profiles to perform their job functions.

Generic Data Entry User Accounts. The P&E Policy Office developed generic user accounts that did not provide for segregation of duties. Management developed three data conversion accounts to enter military equipment data into CAMS-ME at inception, and subsequently created four more of these accounts. These seven accounts allowed a user to input or change data for any military equipment program without a review for accuracy. The generic accounts were used at the end of FY 2006, but management did not retain documentation of how and why the accounts were used. DoD Financial Management Regulation, volume 1, chapter 3, Key Accounting Requirement 7 states that organizations must maintain a separation of duties for reviewing transactions. In addition, DoD Instruction 8500.2 states access to DoD information systems processing sensitive information requires presentation of an individual authenticator. The accounts remained in the system because the P&E Policy Office did not follow DoD guidance. As a result, there is an increased risk that one or more of these accounts could be intentionally or unintentionally unlocked and unauthorized or erroneous data could be entered into CAMS-ME. If there is no review of this data, it will go undetected and will subsequently be reported on the DoD balance sheet. To mitigate this risk, management should delete these accounts.

Recommendations, Management Comments, and Audit Response

E. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis:

1. Review help desk user accounts to ensure that they have the appropriate profiles to perform their job functions to comply with DoD Instruction 8500.2, “Information Assurance Implementation,” February 6, 2003.

2. Delete the generic data conversion user accounts to limit the ability of a user to intentionally or unintentionally enter erroneous data without an audit trail or supervisory review in accordance with DoD Financial

Management Regulation, volume 1, chapter 3, Key Accounting Requirement 7 and DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis has completed a review of the help desk user accounts and identified mitigating controls to ensure that assets are protected. In addition, the Director, Acquisition Resources and Analysis deleted the generic data entry accounts in November 2007.

Audit Response. We commend the Director, Acquisition Resources and Analysis for taking prompt action in resolving these recommendations. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed.

F. Service Continuity

DISA Ogden established adequate environmental controls. However, the P&E Policy Office and DISA Ogden did not adequately design service continuity controls to operate effectively. Specifically, management did not prioritize computerized operations and develop and document a comprehensive contingency plan. The P&E Policy Office and DISA Ogden did not design adequate service continuity controls because they did not establish or follow service continuity policies and procedures. As a result, there is an increased risk of delay in the restoration of critical operations and loss of data in an emergency.

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 interruption, such as temporary power failures, as well as major disasters. The P&E Policy Office developed their "CAMS-ME 1.1 COOP [Continuity of Operations Plan] Executive Summary of Planning Activities," June 19, 2006, and DISA Ogden developed their "Business Continuity Plan for Systems Management Center Ogden," May 2005, as guides in the event of a contingency.

Prevent and Minimize Damage and Interruption

DISA Ogden established adequate environmental controls over the CAMS-ME hardware to prevent and minimize damage and interruption. Management implemented controls including inspections of the fire extinguishers; fire, smoke, and water detection systems; and uninterruptible power supply. The DISA Ogden facility was constructed in compliance with earthquake specifications and the server lab was temperature controlled. These controls help prevent minor problems from becoming costly disasters.

Prioritize Computer Operations and Supporting Resources

The P&E Policy Office appropriately established the CAMS-ME resource and system criticality levels. However, they did not establish service continuity controls based on the assessment of the criticality and sensitivity of computerized operations. Specifically, management did not:

- identify resources supporting critical data and operations,
- establish emergency data processing procedures, and
- establish system recovery and reconstitution procedures.

The P&E Policy Office did not establish service continuity controls based on the assessment of the criticality and sensitivity of computerized operations because management did not fully develop or follow service continuity policies and procedures.

Resources Supporting Critical Data and Operations. The P&E Policy Office did not adequately identify resources supporting critical data and operations. The "CAMS-ME 1.1 COOP Executive Summary of Planning Activities" did not identify supporting resources on its list of "decisions and details to be completed." In addition, management did not ensure that the DISA Ogden prioritized restoration list included CAMS-ME. DoD Directive 3020.26, "Defense Continuity Program (DCP)," January 1, 2007, states that contingency plans should identify and prioritize organizational mission essential functions. According to the DISA "Business Continuity Plan for Systems Management Center Ogden," May 2005, the customer is responsible for ensuring that their system is included on the prioritized restoration list.

Emergency Data Processing Procedures. The P&E Policy Office did not document emergency processing procedures. Management planned to provide Components with spreadsheets to collect data. However, they did not document procedures for creating or completing the spreadsheets. Office of Management and Budget Circular No. A-127, Revised, "Financial Management Systems," July 23, 1993, states that agency financial management systems and processing instructions must be clearly documented in hard copy or electronically.

System Recovery and Reconstitution Procedures. The P&E Policy Office did not adequately develop and document procedures for system recovery and reconstitution once a contingency is complete. Management did not adequately document procedures for starting up CAMS-ME at an alternate location. Also, management did not document or develop reconstitution procedures which include restarting the system, reloading manually processed data, and cleaning the alternate site once a contingency is complete. National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, recommends developing a recovery strategy and reconstitution procedures.

The P&E Policy Office did not establish service continuity controls based on the assessment of the criticality and sensitivity of computerized operations. As a result, there is an increased risk of delays in the restoration of data processing leading to inaccurate or incomplete financial information. Management has taken action by developing the "Capital Asset Management for Military Equipment, Contingency Planning Tabletop Test Plan," September 27, 2007, and the draft "Capital Asset Management System for Military Equipment (CAMS-ME), Continuity of Operations Plan (COOP)," September 26, 2007. However, the Test Plan and draft CAMS-ME COOP did not address all findings. To further mitigate this risk, management should finalize the draft CAMS-ME COOP, ensure that CAMS-ME is included on the DISA Ogden prioritized restoration list, and document emergency data processing and develop reconstitution procedures.

Develop and Document a Comprehensive Contingency Plan

The P&E Policy Office and DISA Ogden did not document a comprehensive contingency plan for CAMS-ME. Specifically, the P&E Policy Office did not develop a contingency plan for the CAMS-ME application and business processes. DISA Ogden had a contingency plan for the facility and other applications; however, it was not complete and up-to-date. DITSCAP and DoD Directive 3020.26 provide guidance for documenting and updating a comprehensive contingency plan. The P&E Policy Office and DISA Ogden did not have comprehensive contingency plans because they did not follow service continuity guidance.

CAMS-ME Contingency Plan. The CAMS-ME 1.1 COOP Executive Summary of Planning Activities was not a comprehensive contingency plan. The P&E Policy Office did not include the following, as recommended by National Institute of Standards and Technology Special Publication 800-34:

- a disaster recovery plan,
- procedures for backup tapes,
- results of scheduled exercises and drills, and
- criteria on when the continuity of operations plan should be implemented and who can make that decision.

DISA Ogden Contingency Plan. DISA Ogden developed and tested the Business Continuity Plan. However, the DISA Ogden contingency plan did not incorporate emergency procedures to follow in the event of a natural disaster. In addition, the plan was not up-to-date and did not identify the current off-site storage provider.

The P&E Policy Office and DISA Ogden did not document a comprehensive contingency plan for CAMS-ME. As a result, there is an increased risk that recovery of CAMS-ME processing would be delayed in the event of a contingency. P&E Policy Office management has taken action by developing their CAMS-ME COOP and CAMS-ME Contingency Planning Tabletop Test Plan. To further mitigate this risk, DISA Ogden should update their Business Continuity Plan to include the current off-site storage provider and emergency procedures.

Recommendations, Management Comments, and Audit Response

F.1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis:

a. Provide the Defense Information Systems Agency Ogden the necessary information to ensure that Capital Asset Management System-Military Equipment is included in the prioritized restoration list according to DoD Directive 3020.26, "Defense Continuity Program (DCP)," January 1, 2007.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis stated that the Capital Asset Management System-Military Equipment was added to the prioritized restoration list in September 2007.

Audit Response. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed.

b. Document manual processing procedures.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director Acquisition Resources and Analysis tested the contingency plan on September 27, 2007.

Audit Response. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed.

c. Develop and document procedures to restore the original facility and IT system to normal operating conditions once a contingency is over.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis refer the ability to restore the original facility and IT system to normal operation conditions to the Defense Information Systems Agency business continuity plan.

Audit Response. The Director, Acquisition Resources and Analysis comments were partially responsive. The Director, Acquisition Resources and Analysis identified the Defense Information Systems Agency Business Continuity Plan for procedures on restoring the system to normal operating conditions once a contingency is over. We request that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis document or at least reference the Defense Information Systems Agency procedures within the CAMS-ME Continuity of Operations Plan and provide a completion date in his comments on the final report.

d. Finalize the draft "Capital Asset Management System for Military Equipment (CAMS-ME), Continuity of Operations Plan (COOP)," September 26, 2007.

Management Comments. The Director, Acquisition Resources and Analysis concurred. The Director, Acquisition Resources and Analysis finalized the contingency plan following the table top exercise on September 27, 2007.

Audit Response. We commend the Director, Acquisition Resources and Analysis for taking prompt corrective action. The Director, Acquisition Resources and Analysis comments were responsive and conform to requirements; no additional comments are needed.

F.2. We recommend that the Director, Defense Information Systems Agency update their contingency plan to:

a. Include emergency procedures to follow during a natural disaster.

b. Identify the current off-site storage provider.

Management Comments. The Defense Information Systems Agency concurred. The Director, Defense Information Systems Agency Computing Services plans to include the local emergency procedures for natural disasters including earthquakes and the current off-site storage provider in the contingency plan by May 5, 2008, and April 30, 2008, respectively.

Audit Response. The Director, Defense Information Systems Agency comments were responsive and conform to requirements; no additional comments are needed.

Appendix A. Scope and Methodology

We conducted this performance audit from January 2007 through February 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

- We interviewed personnel at the P&E Policy Office Arlington, Virginia; SSC San Diego California; DISA Ogden, Utah; and DFAS Columbus, Ohio.

- We inspected documentation and observed activities supporting the effectiveness of the general controls at the P&E Policy Office Arlington, Virginia; SSC San Diego, California; DISA Ogden, Utah; and DFAS Columbus, Ohio.

- We reviewed and tested specific control activities in place at the P&E Policy Office Arlington, Virginia; SSC San Diego, California; DISA Ogden, Utah; and DFAS Columbus, Ohio.

- We obtained and inspected system settings, access controls, and the results of security readiness review assessments performed at the SSC San Diego, California; DISA Ogden, Utah; and DFAS Columbus, Ohio.

We used the Government Accountability Office "Federal Information System Controls Audit Manual" to develop the audit guide and procedures performed during this audit. Based on the Federal Information System Controls Audit Manual, the audit was divided into six areas:

- The entity-wide security program planning and management area is the foundation on which all other general controls rely.

- Physical and logical access controls reasonably protect the system and data from unauthorized modification, loss, and disclosure.

- Application 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.

- System software includes programs that are designed to operate and control the processing activities of computer equipment on which an application resides.

- 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.

- Service continuity includes the protection of an activity's resources, minimization of opportunities for service interruption, and planning for service recovery.

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 P&E Policy Office Arlington, Virginia; SSC San Diego, California; DISA Ogden, Utah; and DFAS Columbus, Ohio, sites. The controls assessed in this audit included controls associated with the security planning and management, access, application change, system software, segregation of duties, and service continuity controls of CAMS-ME. Because of the planned CAMS-ME Increment 2 Release, the Statement on Auditing Standards No. 70 Audit of the Defense Information Systems Agency, and availability of audit resources, we did not perform tests of the following:

- Application controls,

- System penetration, and

- Segregation of duties controls over functional users.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit. Rather, we assessed the general controls over 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 Approach to Business Transformation, and DoD Financial Management high-risk areas.

Prior Coverage

During the last 5 years, the Department of Defense Office of Inspector General has issued two reports discussing the Defense Information Systems Agency Controls over the Center for Computing Services. These reports are indirectly related to CAMS-ME because they discuss controls that the Defense Information Systems Agency has implemented. Unrestricted Department of Defense Office of the Inspector General reports can be accessed over the Internet at http://www.dodig.mil/.

DoD IG

DoD IG Report No. D-2007-082, "Defense Information Systems Agency Controls over the Center for Computing Services," April 9, 2007

DoD IG Report D-2006-086, "Report on the General and Applications Controls at the Defense Information Systems Agency, Center for Computing Services," May 18, 2006

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
  Director, Acquisition Resources and Analysis
Under Secretary of Defense (Comptroller)/Chief Financial Officer
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer
Director, Program Analysis and Evaluation (PA&E)

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)

Combatant Commands

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

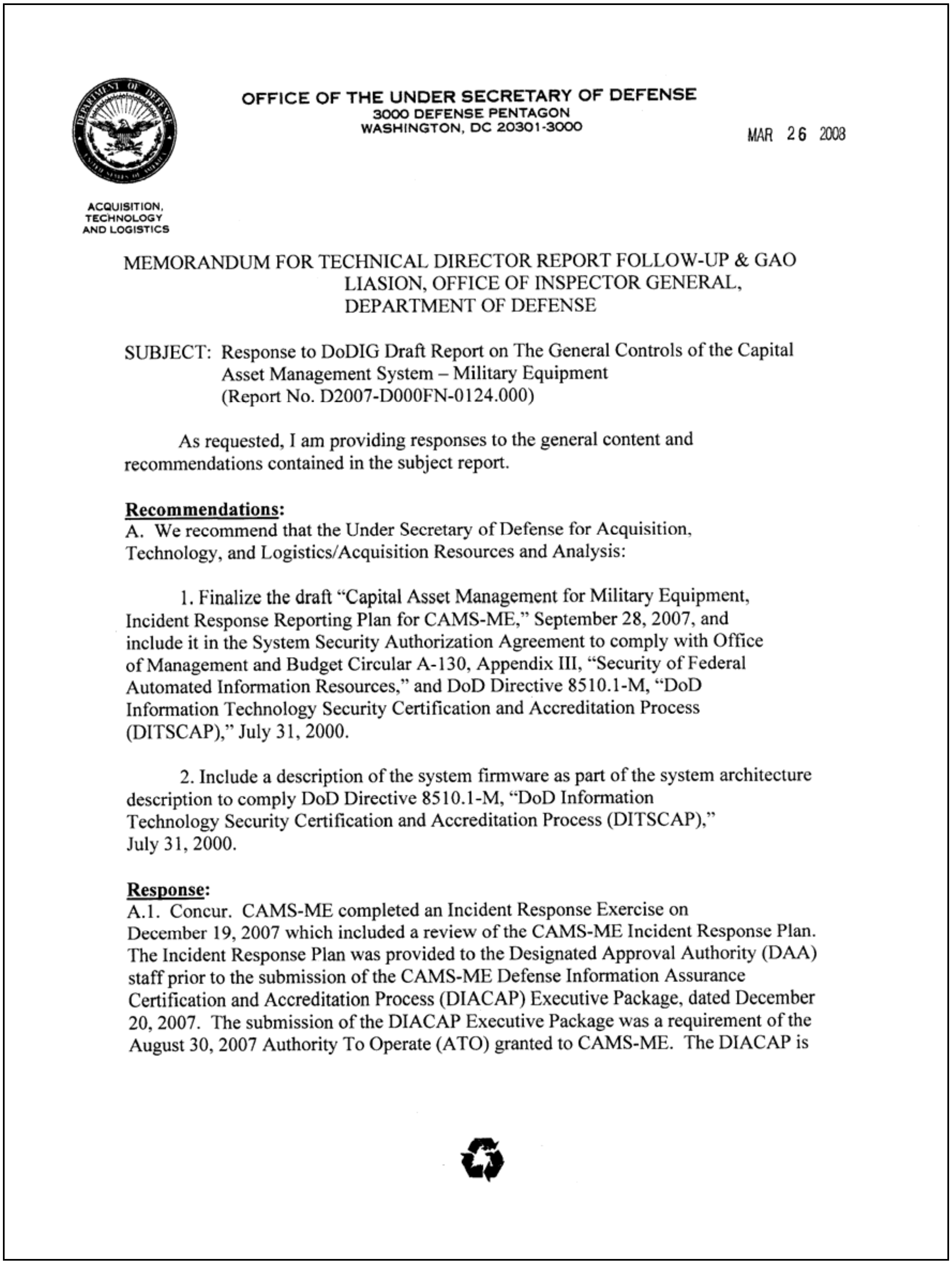
Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services

Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Oversight and Government Reform
House Subcommittee on Government Management, Organization, and Procurement,
Committee on Oversight and Government Reform
House Subcommittee on National Security and Foreign Affairs,
Committee on Oversight and Government Reform

Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis Comments

Final Report Reference



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

MAR 26 2008

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

MEMORANDUM FOR TECHNICAL DIRECTOR REPORT FOLLOW-UP & GAO LIASION, OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Response to DoDIG Draft Report on The General Controls of the Capital Asset Management System – Military Equipment (Report No. D2007-D000FN-0124.000)

As requested, I am providing responses to the general content and recommendations contained in the subject report.

Recommendations:
A. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis:

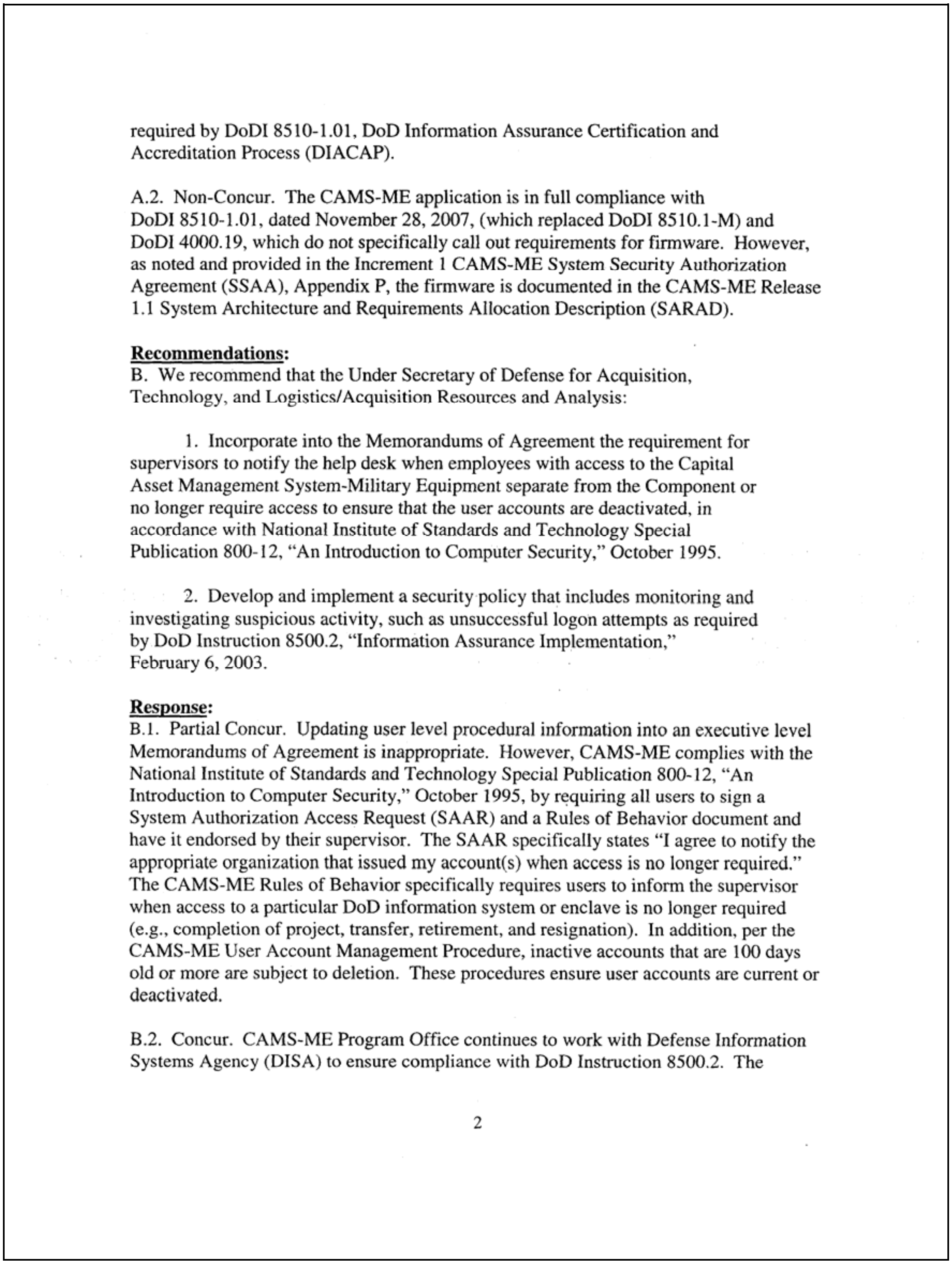
1. Finalize the draft "Capital Asset Management for Military Equipment, Incident Response Reporting Plan for CAMS-ME," September 28, 2007, and include it in the System Security Authorization Agreement to comply with Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and DoD Directive 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," July 31, 2000.

Renumbered as Recommendation A.

2. Include a description of the system firmware as part of the system architecture description to comply DoD Directive 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," July 31, 2000.

Deleted

Response:
A.1. Concur. CAMS-ME completed an Incident Response Exercise on December 19, 2007 which included a review of the CAMS-ME Incident Response Plan. The Incident Response Plan was provided to the Designated Approval Authority (DAA) staff prior to the submission of the CAMS-ME Defense Information Assurance Certification and Accreditation Process (DIACAP) Executive Package, dated December 20, 2007. The submission of the DIACAP Executive Package was a requirement of the August 30, 2007 Authority To Operate (ATO) granted to CAMS-ME. The DIACAP is



required by DoDI 8510-1.01, DoD Information Assurance Certification and Accreditation Process (DIACAP).

A.2. Non-Concur. The CAMS-ME application is in full compliance with DoDI 8510-1.01, dated November 28, 2007, (which replaced DoDI 8510.1-M) and DoDI 4000.19, which do not specifically call out requirements for firmware. However, as noted and provided in the Increment 1 CAMS-ME System Security Authorization Agreement (SSAA), Appendix P, the firmware is documented in the CAMS-ME Release 1.1 System Architecture and Requirements Allocation Description (SARAD).

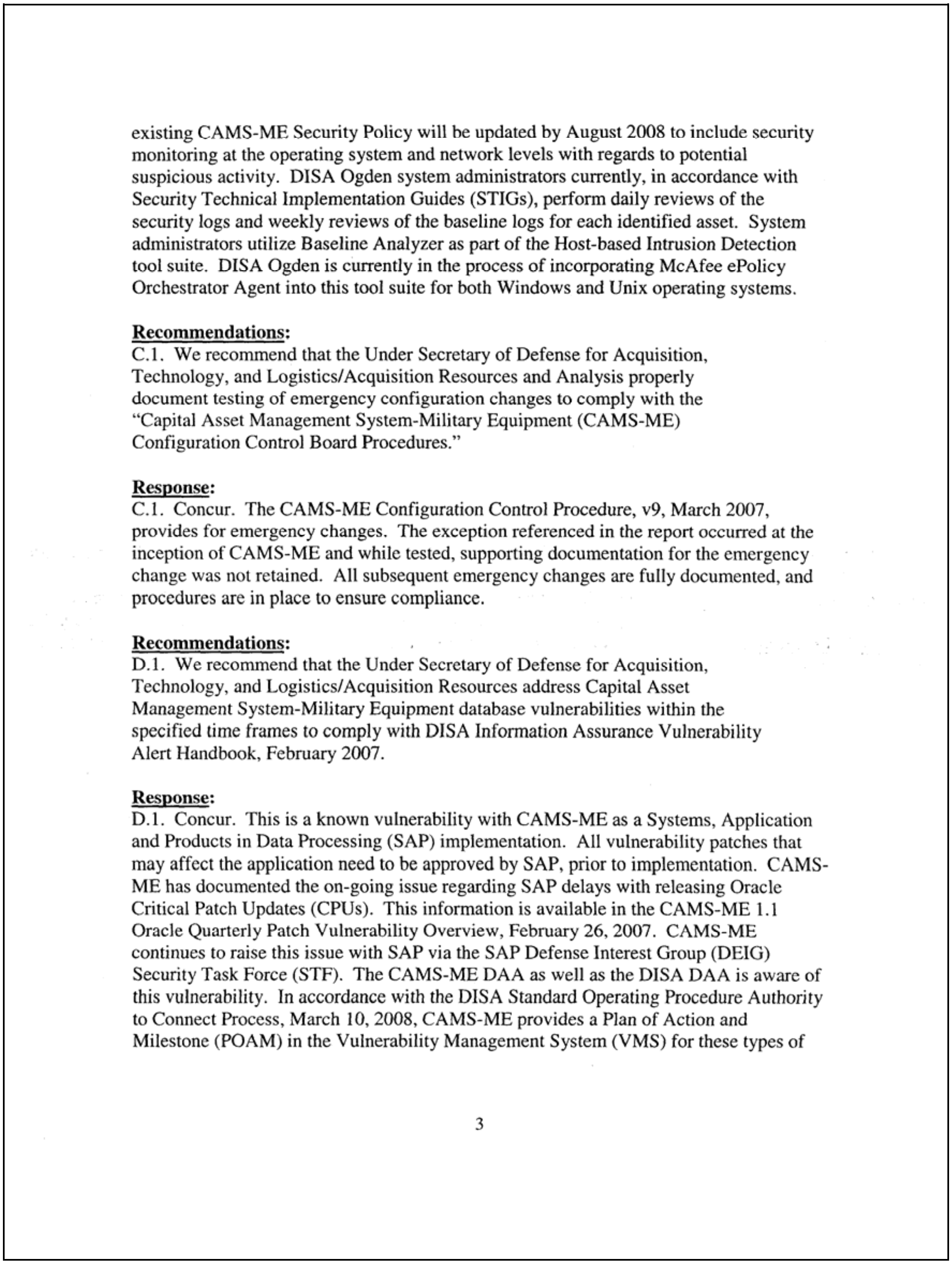
Recommendations:
B. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis:

1. Incorporate into the Memorandums of Agreement the requirement for supervisors to notify the help desk when employees with access to the Capital Asset Management System-Military Equipment separate from the Component or no longer require access to ensure that the user accounts are deactivated, in accordance with National Institute of Standards and Technology Special Publication 800-12, "An Introduction to Computer Security," October 1995.

2. Develop and implement a security policy that includes monitoring and investigating suspicious activity, such as unsuccessful logon attempts as required by DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

Response:
B.1. Partial Concur. Updating user level procedural information into an executive level Memorandums of Agreement is inappropriate. However, CAMS-ME complies with the National Institute of Standards and Technology Special Publication 800-12, "An Introduction to Computer Security," October 1995, by requiring all users to sign a System Authorization Access Request (SAAR) and a Rules of Behavior document and have it endorsed by their supervisor. The SAAR specifically states "I agree to notify the appropriate organization that issued my account(s) when access is no longer required." The CAMS-ME Rules of Behavior specifically requires users to inform the supervisor when access to a particular DoD information system or enclave is no longer required (e.g., completion of project, transfer, retirement, and resignation). In addition, per the CAMS-ME User Account Management Procedure, inactive accounts that are 100 days old or more are subject to deletion. These procedures ensure user accounts are current or deactivated.

B.2. Concur. CAMS-ME Program Office continues to work with Defense Information Systems Agency (DISA) to ensure compliance with DoD Instruction 8500.2. The



existing CAMS-ME Security Policy will be updated by August 2008 to include security monitoring at the operating system and network levels with regards to potential suspicious activity. DISA Ogden system administrators currently, in accordance with Security Technical Implementation Guides (STIGs), perform daily reviews of the security logs and weekly reviews of the baseline logs for each identified asset. System administrators utilize Baseline Analyzer as part of the Host-based Intrusion Detection tool suite. DISA Ogden is currently in the process of incorporating McAfee ePolicy Orchestrator Agent into this tool suite for both Windows and Unix operating systems.

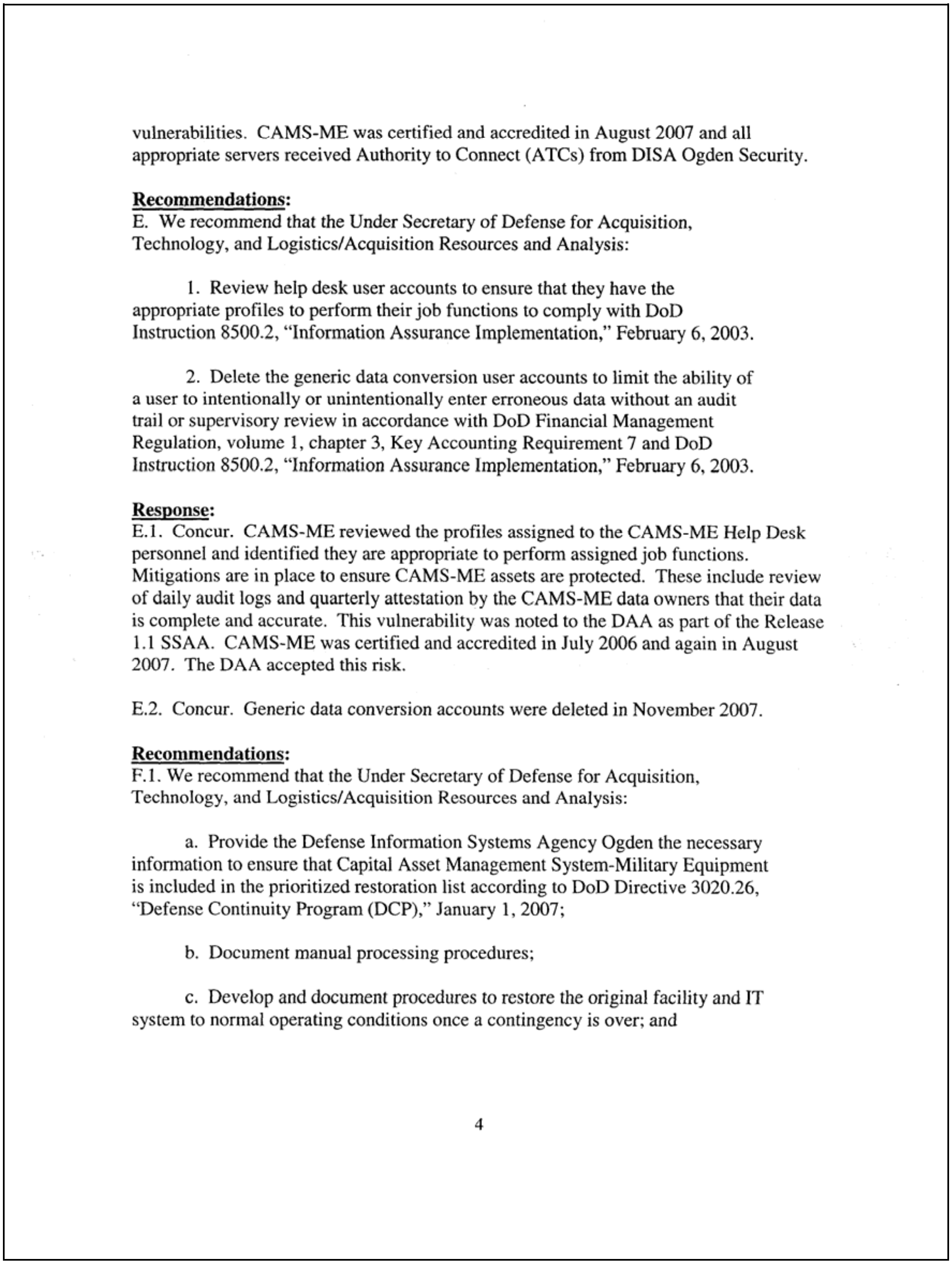
Recommendations:
C.1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis properly document testing of emergency configuration changes to comply with the "Capital Asset Management System-Military Equipment (CAMS-ME) Configuration Control Board Procedures."

Renumbered as Recommendation C.

Response:
C.1. Concur. The CAMS-ME Configuration Control Procedure, v9, March 2007, provides for emergency changes. The exception referenced in the report occurred at the inception of CAMS-ME and while tested, supporting documentation for the emergency change was not retained. All subsequent emergency changes are fully documented, and procedures are in place to ensure compliance.

Recommendations:
D.1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources address Capital Asset Management System-Military Equipment database vulnerabilities within the specified time frames to comply with DISA Information Assurance Vulnerability Alert Handbook, February 2007.

Response:
D.1. Concur. This is a known vulnerability with CAMS-ME as a Systems, Application and Products in Data Processing (SAP) implementation. All vulnerability patches that may affect the application need to be approved by SAP, prior to implementation. CAMS-ME has documented the on-going issue regarding SAP delays with releasing Oracle Critical Patch Updates (CPUs). This information is available in the CAMS-ME 1.1 Oracle Quarterly Patch Vulnerability Overview, February 26, 2007. CAMS-ME continues to raise this issue with SAP via the SAP Defense Interest Group (DEIG) Security Task Force (STF). The CAMS-ME DAA as well as the DISA DAA is aware of this vulnerability. In accordance with the DISA Standard Operating Procedure Authority to Connect Process, March 10, 2008, CAMS-ME provides a Plan of Action and Milestone (POAM) in the Vulnerability Management System (VMS) for these types of



vulnerabilities. CAMS-ME was certified and accredited in August 2007 and all appropriate servers received Authority to Connect (ATCs) from DISA Ogden Security.

Recommendations:
E. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis:

1. Review help desk user accounts to ensure that they have the appropriate profiles to perform their job functions to comply with DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

2. Delete the generic data conversion user accounts to limit the ability of a user to intentionally or unintentionally enter erroneous data without an audit trail or supervisory review in accordance with DoD Financial Management Regulation, volume 1, chapter 3, Key Accounting Requirement 7 and DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

Response:
E.1. Concur. CAMS-ME reviewed the profiles assigned to the CAMS-ME Help Desk personnel and identified they are appropriate to perform assigned job functions. Mitigations are in place to ensure CAMS-ME assets are protected. These include review of daily audit logs and quarterly attestation by the CAMS-ME data owners that their data is complete and accurate. This vulnerability was noted to the DAA as part of the Release 1.1 SSAA. CAMS-ME was certified and accredited in July 2006 and again in August 2007. The DAA accepted this risk.

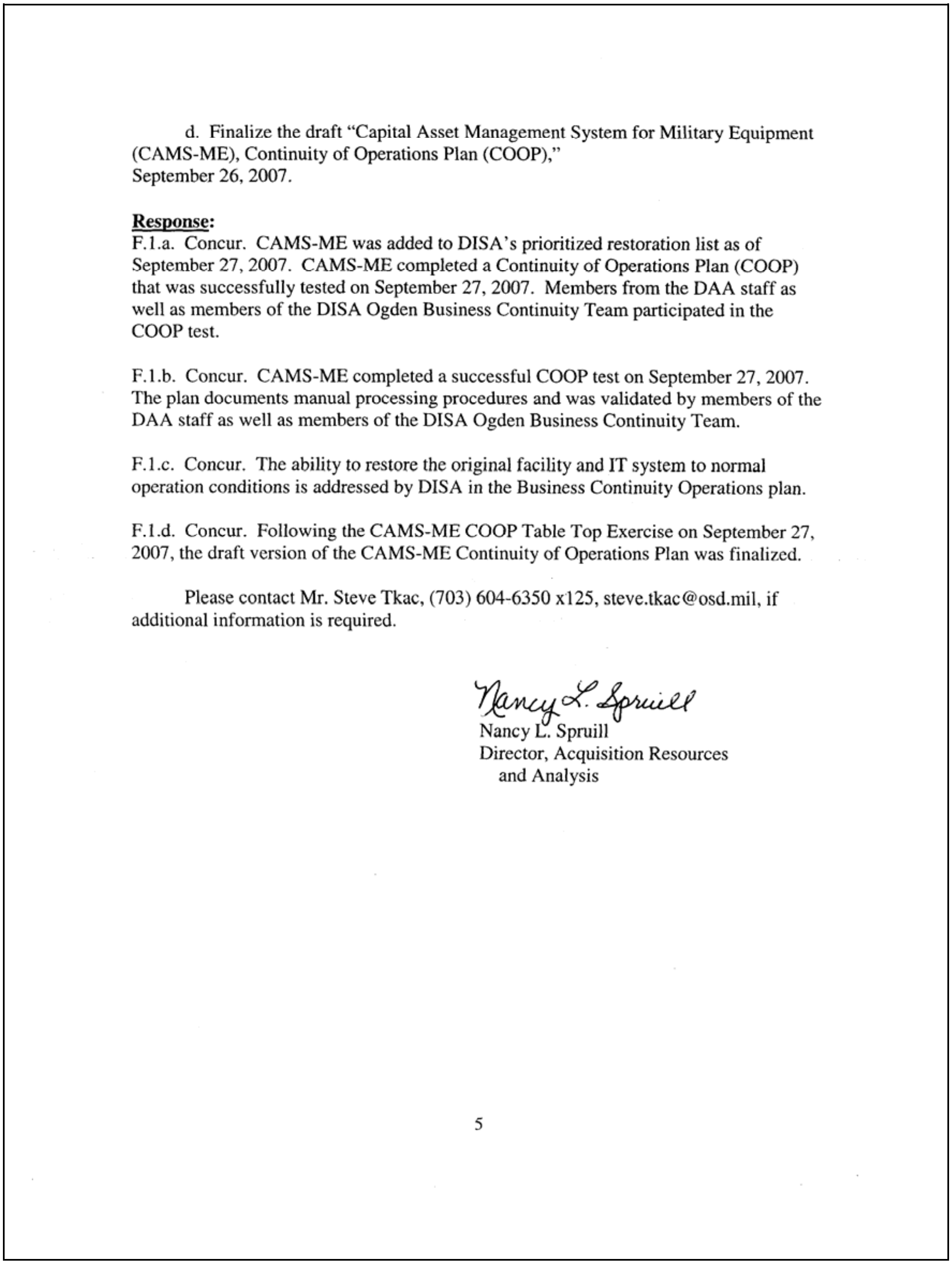
E.2. Concur. Generic data conversion accounts were deleted in November 2007.

Recommendations:
F.1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics/Acquisition Resources and Analysis:

a. Provide the Defense Information Systems Agency Ogden the necessary information to ensure that Capital Asset Management System-Military Equipment is included in the prioritized restoration list according to DoD Directive 3020.26, "Defense Continuity Program (DCP)," January 1, 2007;

b. Document manual processing procedures;

c. Develop and document procedures to restore the original facility and IT system to normal operating conditions once a contingency is over; and



d. Finalize the draft "Capital Asset Management System for Military Equipment (CAMS-ME), Continuity of Operations Plan (COOP),"
September 26, 2007.

Response:
F.1.a. Concur. CAMS-ME was added to DISA's prioritized restoration list as of September 27, 2007. CAMS-ME completed a Continuity of Operations Plan (COOP) that was successfully tested on September 27, 2007. Members from the DAA staff as well as members of the DISA Ogden Business Continuity Team participated in the COOP test.

F.1.b. Concur. CAMS-ME completed a successful COOP test on September 27, 2007. The plan documents manual processing procedures and was validated by members of the DAA staff as well as members of the DISA Ogden Business Continuity Team.

F.1.c. Concur. The ability to restore the original facility and IT system to normal operation conditions is addressed by DISA in the Business Continuity Operations plan.

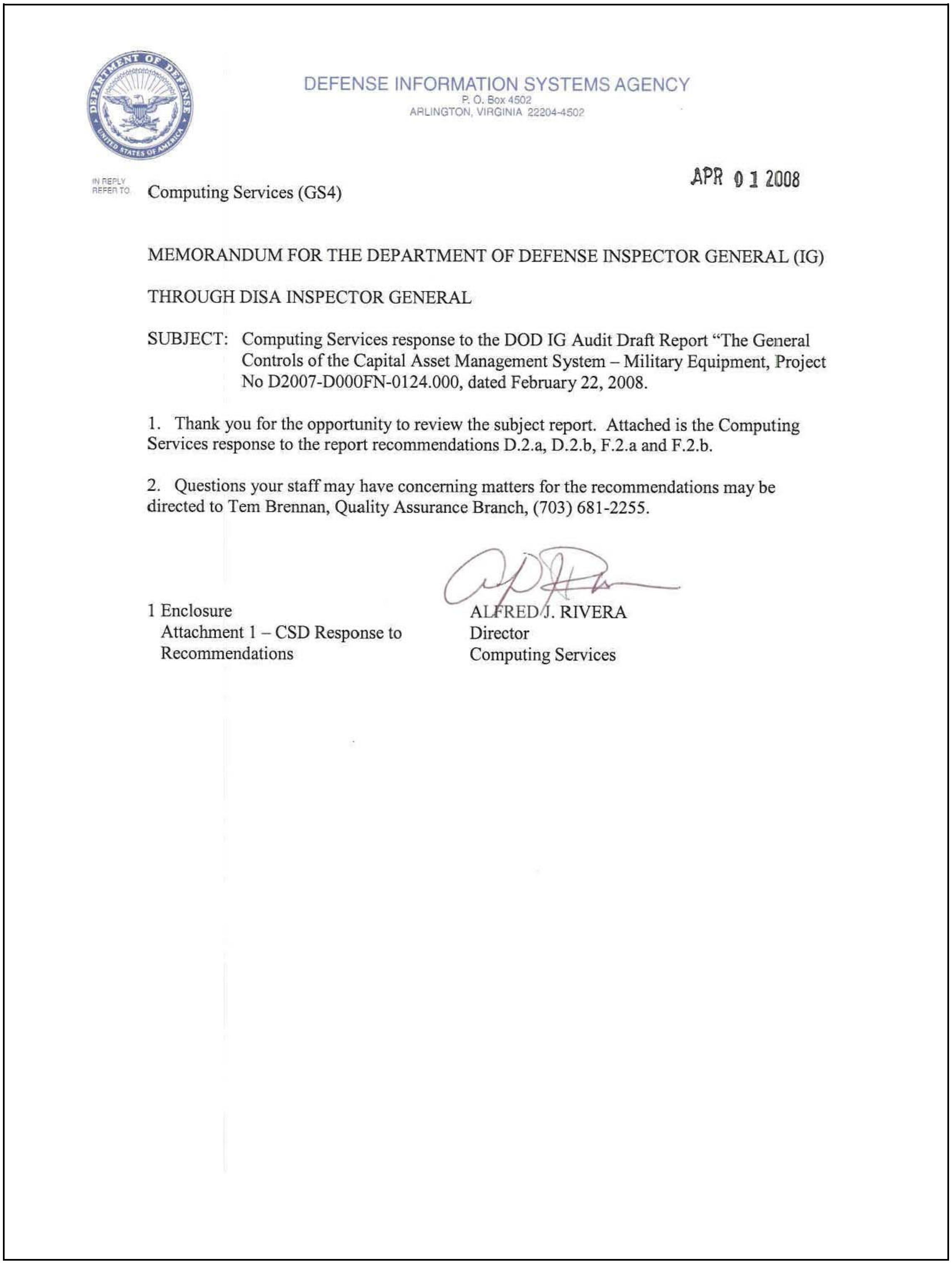
F.1.d. Concur. Following the CAMS-ME COOP Table Top Exercise on September 27, 2007, the draft version of the CAMS-ME Continuity of Operations Plan was finalized.

Please contact Mr. Steve Tkac, (703) 604-6350 x125, steve.tkac@osd.mil, if additional information is required.

Nancy L. Spruill

Nancy L. Spruill
Director, Acquisition Resources
and Analysis

Director, Defense Information Systems Agency



DEFENSE INFORMATION SYSTEMS AGENCY
P. O. Box 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Computing Services (GS4)

APR 0 1 2008

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL (IG)

THROUGH DISA INSPECTOR GENERAL

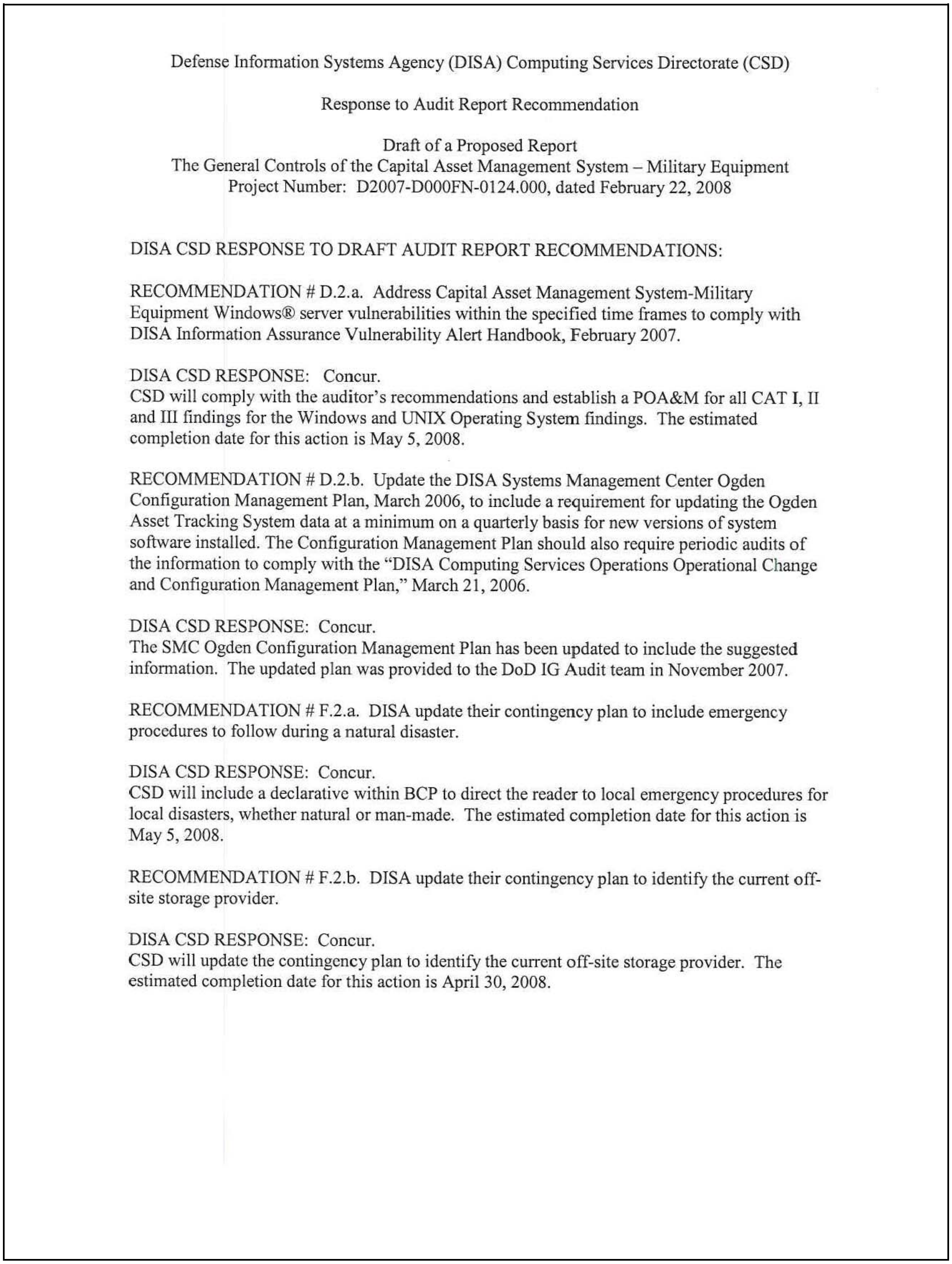
SUBJECT: Computing Services response to the DOD IG Audit Draft Report "The General Controls of the Capital Asset Management System – Military Equipment, Project No D2007-D000FN-0124.000, dated February 22, 2008.

1. Thank you for the opportunity to review the subject report. Attached is the Computing Services response to the report recommendations D.2.a, D.2.b, F.2.a and F.2.b.

2. Questions your staff may have concerning matters for the recommendations may be directed to Tem Brennan, Quality Assurance Branch, (703) 681-2255.

ALFRED J. RIVERA
Director
Computing Services

1 Enclosure
Attachment 1 – CSD Response to Recommendations



Defense Information Systems Agency (DISA) Computing Services Directorate (CSD)

Response to Audit Report Recommendation

Draft of a Proposed Report
The General Controls of the Capital Asset Management System – Military Equipment
Project Number: D2007-D000FN-0124.000, dated February 22, 2008

DISA CSD RESPONSE TO DRAFT AUDIT REPORT RECOMMENDATIONS:

RECOMMENDATION # D.2.a. Address Capital Asset Management System-Military Equipment Windows® server vulnerabilities within the specified time frames to comply with DISA Information Assurance Vulnerability Alert Handbook, February 2007.

DISA CSD RESPONSE: Concur.
CSD will comply with the auditor's recommendations and establish a POA&M for all CAT I, II and III findings for the Windows and UNIX Operating System findings. The estimated completion date for this action is May 5, 2008.

RECOMMENDATION # D.2.b. Update the DISA Systems Management Center Ogden Configuration Management Plan, March 2006, to include a requirement for updating the Ogden Asset Tracking System data at a minimum on a quarterly basis for new versions of system software installed. The Configuration Management Plan should also require periodic audits of the information to comply with the "DISA Computing Services Operations Operational Change and Configuration Management Plan," March 21, 2006.

DISA CSD RESPONSE: Concur.
The SMC Ogden Configuration Management Plan has been updated to include the suggested information. The updated plan was provided to the DoD IG Audit team in November 2007.

RECOMMENDATION # F.2.a. DISA update their contingency plan to include emergency procedures to follow during a natural disaster.

DISA CSD RESPONSE: Concur.
CSD will include a declarative within BCP to direct the reader to local emergency procedures for local disasters, whether natural or man-made. The estimated completion date for this action is May 5, 2008.

RECOMMENDATION # F.2.b. DISA update their contingency plan to identify the current off-site storage provider.

DISA CSD RESPONSE: Concur.
CSD will update the contingency plan to identify the current off-site storage provider. The estimated completion date for this action is April 30, 2008.

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.

Patricia A. Marsh
Edward A. Blair
Gregory M. Mennetti
Dwayne A. Coulson
Michael B. Dell, Jr.
Devon R. Houston
Kendall A. Miller
Dea M. Algeo
Troy A. Robertson
Celita M. Pomales
Ai T. Nguyen
Erin S. Hart

Inspector General
Department of Defense