

# Inspector General

United States  
Department of Defense



## General Controls Over the Standard Accounting, Budgeting, and Reporting System (SABRS)

### **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

DEPARTMENT OF DEFENSE

**hotline**

**To report fraud, waste, mismanagement, and abuse of authority.**

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900  
Phone: 800.424.9098 e-mail: [hotline@dodig.mil](mailto:hotline@dodig.mil) [www.dodig.mil/hotline](http://www.dodig.mil/hotline)

### **Acronyms**

CIO	Chief Information Office
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
FISMA	Federal Information Security Management Act
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PMO	Program Management Office
SABRS	Standard Accounting, Budgeting, and Reporting System
TASO	Terminal Area Security Officer
USMC	United States Marine Corps



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

June 6, 2008

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING  
SERVICE  
NAVAL INSPECTOR GENERAL  
ASSISTANT DEPUTY COMMANDANT FOR PROGRAMS AND  
RESOURCES (FISCAL), UNITED STATES MARINE CORPS

SUBJECT: General Controls Over the Standard Accounting, Budgeting, and Reporting  
System (SABRS) (Report No. D-2008-101)

We are providing this report for review and comment. We considered comments from the Defense Finance and Accounting Service when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Defense Finance and Accounting Service comments were partially responsive. We request additional comments on Recommendations A.1.a, A.1.d, A.2.a, A.2.b, A.2.d, A.2.e, B.1.a, B.1.b, B.2.b, B.2.c, B.2.d, B.2.e., B.2.f, B.3, B.4.b, and C. Therefore, we request that the Chief Information Officer, Defense Finance and Accounting Service provide comments by July 7, 2008.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to [AudDFS@dodig.mil](mailto:AudDFS@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 Ms. Cecelia M. Ball at (816) 926-8501 ext. 222 (DSN 465-8501). The team members are listed inside the back cover. See Appendix C for the report distribution.

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



## Department of Defense Office of Inspector General

Report No. D-2008-101

(Project No. D2006-D000FC-0068.000)

June 6, 2008

### General Controls Over the Standard Accounting, Budgeting, and Reporting System (SABRS)

#### Executive Summary

**Who Should Read This Report and Why?** DoD personnel who manage and use the Standard Accounting, Budgeting, and Reporting System (SABRS) should read this report. This report discusses whether the SABRS general controls were adequately designed and operating effectively.

**Background.** SABRS is the accounting system used by the Defense Finance and Accounting Service Kansas City to standardize accounting, budgeting, and reporting procedures for the United States Marine Corps (USMC) general fund. The USMC reported \$27,155 million in assets and \$2,255 million in liabilities on its FY 2006 Balance Sheet. This audit was conducted to determine whether the Defense Finance and Accounting Service Kansas City ensures general control standards issued by the Office of Management and Budget, the National Institute of Standards and Technology, and DoD were implemented and operating effectively for SABRS.

**Results.** Controls over SABRS security management and operations are ineffective because the Defense Finance and Accounting Service Chief Information Officer did not assign clear security responsibilities to the SABRS Program Management Office (finding A), the SABRS Program Management Office did not provide assurance that SABRS security was effective because it did not coordinate with all responsible parties (finding B), and Defense Finance and Accounting Service Accounting Services-Marine Corps and Defense Information Systems Agency did not have an approved Service Level Agreement because Defense Finance and Accounting Service did not sufficiently coordinate with the Defense Information Systems Agency to complete the approval process (finding C). See the Findings section of the report for the detailed recommendations.

**Management Comments.** The Director, Information and Technology, Defense Finance and Accounting Service concurred with all recommendations except one. We considered some corrective actions responsive to the intent of the recommendations. No further comments are required for those recommendations. We reiterated other recommendations to the Chief Information Office, Defense Finance and Accounting Service and the Program Management Office because comments were nonresponsive and partially responsive.

We request that the Chief Information Office, Defense Finance and Accounting Service and the Program Management Office comment on the final report by July 7, 2008. See the Findings 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.

# Table of Contents

---

<b>Executive Summary</b>	i
<b>Background</b>	1
<b>Objectives</b>	2
<b>Findings</b>	
A. Standard Accounting, Budgeting, and Reporting System Security Management	3
B. Program Management Office Security Coordination	15
C. Defense Finance and Accounting Service and Defense Information Systems Agency Service Level Agreement	22
<b>Appendixes</b>	
A. Scope and Methodology	24
B. Security Plan Comparison	26
C. Report Distribution	32
<b>Management Comments</b>	
Defense Finance and Accounting Service	35



---

## Background

The Chief Financial Officers Act of 1990 (Public Law 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements. Under Secretary of Defense (Comptroller) guidance implementing the Chief Financial Officers Act of 1990, as amended, requires the United States Marine Corps (USMC) complete stand-alone General Fund and Working Capital Fund financial statements.

The Defense Finance and Accounting Service (DFAS) Kansas City is responsible for reporting the USMC financial statement data to the Department of the Navy. These financial statement data are ultimately included in the DoD consolidated financial statements. The USMC relies on DFAS Kansas City's assurances regarding the controls used to prepare the USMC financial reports and its financial statements. The USMC reported \$27,155 million in assets and \$2,255 million in liabilities on its FY 2006 Balance Sheet.

The Standard Accounting, Budgeting, and Reporting System (SABRS) is a computer-based information system designed to standardize accounting, budgeting, and reporting procedures for all general funds accounted for by the USMC. SABRS produces general data to support automated and auditable financial statements. It facilitates the preparation of financial statements and other financial reports in accordance with Federal accounting and reporting standards.

DFAS Kansas City, Accounting Systems Branch owns and manages SABRS. As the owner, it is required to review and maintain the SABRS security policy. The USMC Fiscal Director is the functional sponsor. As a functional sponsor, USMC uses SABRS to record and account for financial data that it owns and processes. DFAS Technology Service Organization developed and maintains the SABRS system. The System Management Center, Mechanicsburg, Pennsylvania, provides SABRS processing support, and the System Management Center, St. Louis, Missouri, provides SABRS hardware support.

Federal agencies, Congress, and the public rely on computer-based information systems to provide data about agency programs, manage Federal resources, and report program costs and benefits. The Federal Information Security Management Act of 2002 (FISMA) assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to strengthen information system security.

FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce Information Technology (IT) security risks to an

---

acceptable level. Additionally, the head of each agency is to appoint a Chief Information Officer (CIO) responsible for developing and maintaining an agency-wide information security program. Agency-wide information security programs should include subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. The DFAS CIO has tasked the SABRS PMO with ensuring adequate information security for SABRS.

FISMA directs NIST to develop IT security standards and guidelines and directs each agency to implement an information security program. FISMA requires that the OMB oversee IT security policies and practices across all Federal agencies. NIST works collaboratively with OMB to develop standards and guidelines to achieve cost-effective security and privacy of sensitive information in Federal computer systems. Agencies, like DFAS, must follow NIST standards and guidance for non-national security programs and systems.

The Office of the Assistant Secretary of Defense directed the Defense-Wide Information Systems Security Program to create standardized requirements and processes for accreditation of computers, systems, and networks. DoD Instruction 5200.40 established the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The DITSCAP Manual (DoD 8510.1-M) presents the detailed requirements for completing the certification and accreditation process.

Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. General controls are the policies and procedures that apply to an entity's information systems and help ensure their proper operation. Primary objectives for general controls include safeguarding data, protecting computer application programs, preventing system software from unauthorized access, and ensuring continued computer operations in case of unexpected interruptions. The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. Without effective general controls, application controls may be rendered ineffective by circumvention or modification. General and application controls become more critical when functions are transferred to other DFAS locations as DFAS Kansas City is scheduled to close under the Base Realignment and Closure.

## **Objectives**

Our overall audit objective was to assess the integrity, confidentiality, and availability of data reported by SABRS. Specifically, we determined whether the general controls over SABRS were adequate. We did not evaluate the application

---

controls over SABRS because of the lack of general controls identified. See Appendix A for a discussion of the scope and methodology.

---

## A. Standard Accounting, Budgeting, and Reporting System Security Management

Controls over SABRS security management and operations were ineffective because the CIO did not assign clear security responsibilities to the Program Management Office (PMO). Specifically:

- the SABRS security management structure did not ensure proper segregation of duties and security responsibilities;
- the CIO did not clearly delegate the authority and duty to responsible parties to develop approved policies and procedures for SABRS IT security operations;
- the CIO did not clearly assign an office the responsibility for the IT security and control requirements; and
- software waivers and license agreements were not maintained to assure personnel that only authorized software was loaded on computers which can be used to access SABRS.

Ineffective controls over SABRS security management and operations increase the vulnerability of SABRS IT resources and are detrimental to an effective information security program.

### Proper Segregation of Duties and Responsibility

The SABRS security management structure lacks proper segregation of duties and security responsibilities. The CIO did not ensure that the Terminal Area Security Officer (TASO) duties were independent from operations. The CIO did not include clear security responsibilities in the PMO personnel job expectations.

**TASO Segregation of Duties.** TASOs create and assign user IDs and set user privileges for SABRS. TASOs report to DFAS operations instead of to a separate DFAS office. The current reporting hierarchy has TASOs reporting to DFAS operations instead of to a separate function outside of operations. DFAS attempted to segregate duties when it moved PMO reporting to the CIO, but the TASOs, who had reported to the PMO, remained in DFAS operations. This structure allows security controls to be circumvented to provide certain services to customers, including to USMC. For example, TASOs can grant access rights

---

to personnel that allow them to bypass or change security controls. NIST advises that computer security embedded in operations lacks independence, has minimal authority, receives little management attention, and has few resources.

**Assigned Security Responsibilities.** We reviewed the performance plans for the PMO personnel to determine each employee's specific security responsibilities. The performance plans for PMO personnel did not have security responsibilities included as part of their job expectations from the CIO. According to NIST, the assignment of security responsibilities should be in writing to ensure that a system's application has adequate security. It would be appropriate to use performance plans to formally communicate the security responsibilities to PMO personnel.

## Security Policies and Procedures

Controls over SABRS security management and operations are ineffective because the CIO did not clearly delegate the authority and duty to responsible parties to develop approved policies and procedures for SABRS IT security operations. Policies and procedures did not exist or were not formally approved for access authorizations, periodic reviews of access authorizations, and data encryption. Management's requirements or actual intent is not known and cannot be enforced if the policies and procedures have not been formally approved.

**Access Authorizations.** The PMO, as a component of the CIO, provided desk procedures, but not formal policies, for granting system access authorizations. The desk procedures were not properly approved by DFAS management. According to NIST, approved policies are needed to provide sufficient information or direction to be used in establishing an access control list. In addition, the Government Accountability Office Federal Information System Controls Audit Manual states management is responsible for developing the detailed policies, procedures, and practices to fit an agency's operations. Management should also ensure these policies are built into and are an integral part of IT security operations. Documented and approved access control policies will make these operations substantially easier to follow and will improve system access control.

**Periodic Reviews of Access Authorizations.** The PMO, as a component of the CIO, provided desk procedures, but not formal policies, for periodic reviews of access authorizations. The desk procedures were not properly approved by DFAS management, and they did not provide for periodic review of access rights for each user. According to NIST, it is necessary to periodically review user accounts on a system to ensure proper authorizations and manage system access. Application managers (and data owners, if different) should review all access

---

levels of all application users every month and sign a formal access approval list, which will provide a written record of the approvals. The PMO is often the only individual in a position to know current access requirements.

Informal policies and procedures lack the weight of authority provided by the written approval of a senior management official, the CIO. Management officials' approval provides clear evidence to employees and contractors that management is in agreement with the stated policies and procedures and that adherence is required.

Effective administration of users' access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. This process should include periodic verification of user accounts and access authorizations. User accounts must also be timely changed for modification or removal of access and associated issues for employees who are reassigned, promoted, terminated, or who retire.

**Data Encryption.** The PMO, as a component of the CIO, could not identify its data encryption procedures. PMO personnel stated encryption is not under their direct control so they do not believe they need to know this information. According to NIST, an organization should use encryption to protect the confidentiality of remote access sessions. During our audit, NIST was updated (December 2006); however, the requirement to use encryption did not change and still applies. The requirements for encryption and remote access policies are critical because they address the security of data transmission. The PMO has primary responsibility for the security of SABRS. It should be aware of the encryption used for their application.

## **SABRS Security and Control Requirements**

Controls over SABRS security management and operations are ineffective because the CIO did not clearly assign responsibility for the IT security and control requirements. Specifically, the SABRS security environment did not include:

- a complete risk assessment;
- an adequate security plan, also called a System Security Authorization Agreement;
- identification of information and resources critical to the operations of SABRS in its contingency plan;

- 
- implementation of intrusion detection and incident response procedures; and
  - assurance that users completed required security awareness training.

**Risk Assessments.** The PMO, as a component of the CIO, did not complete a required risk assessment because the CIO did not clearly assign security responsibilities to the PMO. Although the PMO identified some potential risks, it did not perform a risk assessment of natural threats or rank the probability of identified threats occurring, as required by NIST, OMB, and DoD Instructions.

“Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual,” July 31, 2000, states:

The SSAA<sup>1</sup> should clearly state the nature of the threat that is expected and wherever possible, the expected frequency of occurrence. Generic threat information is available but it must be adapted to clearly state the expected threats to be encountered by the system. DITSCAP also requires the risk analysis to identify appropriate cost-effective countermeasures to mitigate the risk.

The PMO did not adequately complete the risk assessment and, therefore, did not include appropriate countermeasures in its security plan. DoD Instruction 8500.2 requires agencies to ensure that DoD Component-owned or controlled DoD information systems are assessed for information assurance vulnerabilities on a regular basis, and that appropriate information assurance solutions are implemented to eliminate or otherwise mitigate identified vulnerabilities.

Without adequate risk assessments and appropriate countermeasures, the SABRS application could be at risk for a security event (for example, flood, loss of power, or intrusion) to occur that cannot be promptly mitigated. Ultimately, SABRS could be unable to perform its mission of financial accounting and reporting for the USMC.

**Security Plans.** Although the PMO prepared a security plan for SABRS, it did not conform to NIST, OMB, and DITSCAP standards. Of the 65 sections in the 2003 security plan, 26 sections did not comply with standards; of 65 sections for the 2006 security plan, 27 did not comply with standards. Specific areas of noncompliance are listed in Appendix B. In addition, the 2003 security plan was out of date. A major modification to SABRS was completed in October 2005, but the PMO waited until May 2006 to update the security plan. This met the 3-year minimum update, but it did not meet the NIST requirement to update the security plan when a major modification was completed on the system. Management authorizes a system to process information or to operate based on the security

---

<sup>1</sup> The SSAA (System Security Authorization Agreement) is the Security Plan.

---

plan when completing the certification and authorization process. Authorizing a system to process information provides an important quality control, and, by authorizing processing in a system, the manager accepts its associated risks. Because the security plan for SABRS was not up to date, management may be unaware of the risks they are accepting within SABRS when certification and authorization is completed.

**Contingency Planning.** The SABRS contingency plan did not define the information resources criticality in accordance with NIST guidance and DoD Instruction 8500.2. Both standards require the identification of mission and business essential functions for priority restoration planning along with all assets supporting mission or business essential functions.

The PMO provided the contingency plan and results of testing performed. The criticality of data and business essential functions were not identified as part of the plan. Contingency plan testing identified the users' inability to obtain remote access to the contingency site. Remotely accessing the contingency site could be critical during an emergency or system disruption.

**Intrusion Detection and Incident Response Procedures.** The PMO, as a component of the CIO, provided policies and procedures to employees for reporting intrusions; however, the policies and procedures did not address how monitoring within SABRS detects security violations. NIST recommends a baseline level of logging and auditing on all systems. That is, all systems should have a minimum level of recording and reviewing of all system activity. Furthermore, NIST recommends all critical systems have a higher baseline level. The logs frequently provide value during incident analysis, particularly if auditing is enabled. The PMO did not have procedures established for monitoring, through logging and auditing, for SABRS to detect security violations.

SABRS is considered a major application, and according to DoD Instruction 8500.2 major applications require intrusion detection systems. The DoD Instruction requires an incident response plan that identifies the responsible Computer Network Defense Service Provider, defines reportable incidents, outlines a standard operating procedure for incident response, identifies user training, and establishes an incident response team. The plan should be exercised at least annually. The PMO did not have an intrusion detection system as part of an incident response plan.

Application-level audit trails should record user activities, such as opening and closing data files; reading, editing, and deleting records or fields; and printing reports. Without this security control, security violations could occur within SABRS that would not be detected, investigated, or corrected.

---

**Security Awareness Training.** The PMO did not verify that all SABRS users attended the required annual computer security awareness training. FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes security awareness training. This training applies to all personnel, contractors and other users of information systems that support the operations and assets of the agency. Additionally, DoD and OMB require employees receive mandatory periodic training. NIST standards, which are directed by OMB and are considered best practices, require annual training for all users.

An effective IT security program requires significant attention be given to training IT users on security policy, procedures, and techniques. We compared an incomplete list of SABRS users to a list of employees who attended annual IT security training and determined that 2,946 of 3,148 SABRS users were not identified as having completed the required training. Because the PMO did not verify that SABRS users completed the required IT security training, SABRS is vulnerable to greater security risk.

## **Software Waivers or License Agreements**

DFAS Technology Services Organization, as a component of the CIO, did not maintain waivers or license agreements for selected software loaded on their computers. The CIO did not clearly assign those security responsibilities to the Technology Services Organization. Waivers or license agreements authorize the software for use. Unauthorized software could degrade SABRS processing.

DFAS Technology Services Organization was unable to provide waivers or license agreements for 8 of 12 auditor sampled software programs. DFAS Instructions require that only software that is part of the DFAS standard suite of software may be loaded onto a Government computer. All other software must be approved for installation in writing by the DFAS Technology Services Organization. The DFAS CIO should require that the Technology Services Organization maintain software waivers and license agreements. These waivers and license agreements provide assurance that only authorized software is operating on DFAS computers.

---

## Recommendations, Management Comments, and Audit Response

### **A.1 We recommend the Chief Information Officer, Defense Finance and Accounting Service:**

#### **a. Separate the Terminal Area Security Officer functions from Defense Finance and Accounting Service Operations to ensure segregation of duties.**

**Management Comments.** The Director, Information and Technology, DFAS<sup>2</sup> nonconcurred. He stated that TASOs<sup>3</sup> assist in implementing information assurance provisions for local users and systems so they have to be physically located in the same work area or organization as the users. He added that system access procedures involve multiple roles and people, all of which provide an appropriate measure of segregation of duties.

**Audit Response.** The Director, Information and Technology, DFAS nonconcurred and the comments were nonresponsive. We recommended that the TASO functions be separated from operations to ensure segregation of duties. We do not agree that DFAS provides the appropriate measure of segregation of duties between TASOs and operations. TASO functions should not be embedded in DFAS Operation's chain of command regardless of where the TASOs are physically located.

We request that the Director, Information and Technology, DFAS provide the corrective actions taken to segregate TASO functions from operations and the associated implementation dates.

#### **b. Develop performance plans that:**

**(1) Incorporate security duties as performance measurements for personnel with security responsibilities, including but not limited to the Program Management Office, and**

**(2) Management can use to evaluate personnel and hold them accountable for security operations.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He explained that the requirement to develop performance plans that incorporate security duties as performance measurements for personnel with security responsibilities will be added to the DFAS Information Assurance Workforce Improvement Program. The estimated completion date for this action is September 30, 2008.

---

<sup>2</sup> Defense Finance and Accounting Service (DFAS).

<sup>3</sup> Terminal Area Security Officer (TASO).

---

**Audit Response.** Comments from the Director, Information and Technology, DFAS are responsive and no additional comments are required.

**c. Identify and clearly delegate to specific offices the responsibility for establishing and executing policy and procedural authorities over Standard Accounting, Budgeting, and Reporting System information technology security operations.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. The Director, Information and Technology, DFAS stated that he updated DFAS 8500.1-R, Information Assurance, November 2007. This updated policy assigns clear security responsibilities to program managers, system managers, system information assurance managers, site information assurance managers, and other security officials.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are responsive and no additional comments are required.

**d. Direct applicable offices to create, document, implement, and approve policies and procedures in accordance with National Institute of Standards and Technology, DoD, and Government Accountability Office guidance to address:**

- **access authorizations,**
- **periodic reviews of access authorizations,**
- **data encryption, and**
- **detecting and investigating security violations and activities.**

**Management Comments.** The Director, Information and Technology, DFAS concurred.

The Director, Information and Technology, DFAS described the procedures that DFAS uses for access authorizations and periodic review of access authorizations. He explained that an automated process identifies monthly ACIDs<sup>4</sup> that have SABRS<sup>5</sup> access. A systems task documents the validation, showing access identifications and entries that were removed. He added that the SABRS PMO<sup>6</sup> is notified of the monthly validation. He also stated that all ACIDs are reviewed when DFAS receives a request for SABRS access.

For data encryption, the Director, Information and Technology, DFAS stated that all relevant requirements were identified in the System Security Authorization

---

<sup>4</sup> A form of access identification, known as ACessor Identification (ACID).

<sup>5</sup> Standard Accounting, Budgeting, and Reporting System (SABRS).

<sup>6</sup> Program Management Office (PMO).

---

Agreement for SABRS with additional requirements identified in the DITSCAP<sup>7</sup> based System Security Authorization Agreement. He stated that procedures do not need to be developed as other entities implement the inherited controls.

The Director, Information and Technology, DFAS stated that baseline controls for detecting and investigating security violations are in the System Security Authorization Agreement and that the SABRS incident response plan is in Appendix K of the System Security Authorization Agreement. He added that the appropriate DISA<sup>8</sup> and DFAS Computer Emergency Response Teams conduct investigations and each has its own documentation procedures.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive.

Although the Director, Information and Technology, DFAS described the procedures DFAS uses for access authorizations and review of access authorizations, he did not identify the approved policy that the procedures implement

We disagree that the data encryption requirements are identified in the System Security Authorization Agreement for SABRS. The requirements were implied in checklists instead of formally stated in the System Security Authorization Agreement. Although the data encryption requirements were inherited, the PMO, as a component of the CIO,<sup>9</sup> has primary responsibility for the security of SABRS. Therefore, it should be aware of the encryption used for their application. The Director, Information and Technology, DFAS did not provide encryption procedures.

We disagree that the controls for detecting and investigating security violations are stated in the System Security Authorization Agreement. Appendix K of the System Security Authorization Agreement does not include an incident response plan that identifies the responsible Computer Network Defense Service Provider, defines reportable incidents, outlines a standard operating procedure for incident response, identifies user training, and establishes an incident response team as required by regulation. Appendix K states only that users must immediately report all Information Assurance-related events and potential threats and vulnerabilities involving a DoD information system to the appropriate Information Assurance Officer.

We request that the Director, Information and Technology, DFAS create, document, implement, and approve policies and procedures in accordance with NIST,<sup>10</sup> DoD, and Government Accountability Office guidance to address access authorizations, periodic reviews of access authorizations, data encryption, and detecting and investigating security violations and activities.

---

<sup>7</sup> Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

<sup>8</sup> Defense Information Systems Agency (DISA).

<sup>9</sup> Chief Information Officer (CIO).

<sup>10</sup> National Institute of Standards and Technology (NIST).

---

**e. Provide training to Defense Finance and Accounting Service Kansas City personnel regarding DoD and Defense Finance and Accounting Service license agreements and waivers.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that software licensing requirements are part of the mandatory Information Assurance awareness training provided to all DFAS information technology users. DFAS also broadcasted educational information related to software piracy DFAS wide and posted the information on its ePortal.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are responsive and no additional comments are required.

**f. Maintain license agreements and waivers for software to ensure only authorized software is present on the Defense Finance and Accounting Service computer system.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. The requirement to maintain license agreements and waivers is stated in DFAS 8400.1-R, Information Technology. He stated that DFAS will initiate a review of all installed software to confirm that all workstations comply with software licensing agreements. The estimated completion date for this action is September 30, 2008.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are responsive and no additional comments are required.

**A.2. We recommend the Chief Information Officer, Defense Finance and Accounting Service clearly assign security responsibilities to the Program Management Office and direct that office to comply with National Institute of Standards and Technology, Office of Management and Budget, and DoD requirements. Specifically,**

**a. Perform a risk assessment of Standard Accounting, Budgeting, and Reporting System at least every 3 years or when a major change occurs. This risk assessment should include identifying risks, the likelihood of the identified risks, and appropriate cost-effective countermeasures to mitigate the risks.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He explained that when DoD Instruction 8500.2 was issued subsequent to the DITSCAP manual, the required threat analysis, cited in the report as the basis for this recommendation, was substantially altered. DoD Instruction 8500.2 negated the mandatory requirement to conduct a separate threat and risk assessment for each system. DITSCAP has since been replaced with the Defense Information Assurance Certification and Accreditation Process, which does not require a threat analysis as part of the certification and accreditation process.

---

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. We realize DITSCAP has been replaced with the Defense Information Assurance Certification and Accreditation Process. The assessment of natural threats, as a possible risk, is not addressed in the Defense Information Assurance Certification and Accreditation Process. Therefore, we applied guidance identified in NIST. NIST recommends that information on the probability of natural threats impacting the system be readily available and appropriate countermeasures for those threats be identified.

We request that the Director, Information and Technology, DFAS perform a risk assessment that includes identifying risks, the likelihood of the identified risks, and appropriate cost-effective countermeasures to mitigate the risks.

**b. Prepare and document a security plan.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that the last SABRS security plan was completed on June 9, 2006. He added that DFAS will complete a new security plan as part of the DFAS corporate transition to the Defense Information Assurance Certification and Accreditation Process. The required date for completion is June 30, 2008.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. The security plan should incorporate NIST, Office of Management and Budget, and DoD requirements. We request that the Director, Information and Technology, DFAS review and comment how its security plan meets NIST, Office of Management and Budget, and DoD requirements.

**c. Identify the critical data and resources that support Standard Accounting, Budgeting, and Reporting System. The critical data and resources should be used to identify recovery priorities. This information should be documented in the Standard Accounting, Budgeting, and Reporting System contingency plan.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that DFAS annually updates the SABRS contingency plan. DFAS most recently updated and tested the contingency plan on November 7, 2007.

**Audit Response** Comments from the Director, Information and Technology, DFAS are responsive and no additional comments are required.

**d. Prepare an intrusion detection policy for the Standard Accounting, Budgeting, and Reporting System, including who is responsible for monitoring intrusion detection. The policy should address the recording and auditing of users' activities and intrusion incidents.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that intrusion detection and monitoring requirements are included in the System Security Authorization Agreement as part of the DoD

---

Instruction 8500.2 baseline controls. DISA, DFAS, and USMC<sup>11</sup> personnel implement and perform intrusion detection for SABRS operations at their own user sites.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. Application-level audit trails should record user activities, such as opening and closing data files; reading, editing, and deleting records or fields; and printing reports. DFAS, as the system owner, is ultimately responsible for these functions. They are not controlled by DISA. We request that the Director, Information and Technology, DFAS prepare an intrusion detection policy for SABRS that specifically addresses recording and auditing user activities and intrusion incidents.

**e. Ensure that all Standard Accounting, Budgeting, and Reporting System users have attended annual computer security awareness training and implement a method to verify that all users are adequately completing the required training.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that DFAS is managing and tracking the completion of information assurance awareness training for its own users using an automated method. USMC maintains its own documentation of the information assurance awareness training for SABRS users.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. Because DFAS owns SABRS, the PMO should be aware of all users that have completed security awareness training. In addition, DFAS should periodically verify that all users, including non-DFAS users, annually complete the required training. We request that the Director, Information and Technology, DFAS document how it ensures that all SABRS users have attended annual computer security awareness training and implement a method to verify that all users are adequately completing the required training.

---

<sup>11</sup> United States Marine Corps (USMC).

---

## **B. Program Management Office Security Coordination**

The PMO did not provide assurance that SABRS security was effective because it did not coordinate with all parties responsible for security over SABRS. Specifically, the PMO did not:

- provide documentation that proved the SABRS user passwords were in accordance with Joint Task Force Global Networks Communications Tasking Order 06-02 requirements,
- identify general support system security controls implemented by other responsible parties,
- provide an accurate list of all TASO account holders,
- provide documentation that proved SABRS acceptance testing was completed, and
- prevent unauthorized software from being introduced to the SABRS environment.

As a result, the PMO cannot ensure an effective security control environment exists for SABRS.

### **SABRS User Passwords**

The PMO did not provide documentation that proved SABRS user passwords were in accordance with the requirements in the Joint Task Force Global Networks Communications Tasking Order 06-02 because, PMO personnel stated, this was outside of their direct control. They stated Defense Information Systems Agency (DISA) set the password parameters; therefore, they did not need to know this information. The Tasking Order states that passwords have to meet the following requirements.

- Passwords must be set to a minimum of nine characters.
- Passwords must contain a mix of at least two lowercase letters, two uppercase letters, two numbers, and two special characters.
- Passwords must be changed every 60 days.
- Password history must be set to a minimum of five.

- 
- Unsuccessful logon attempt counter must be set to three with a counter reset of no less than 60 minutes. This allows no more than two unsuccessful logon attempts within a 60-minute period.
  - After the third unsuccessful logon attempt, the account lockout duration must be set to “forever,” requiring the account to be unlocked by a system administrator.

Passwords are a technical measure that prevents unauthorized people (or unauthorized processes) from entering a computer system. Passwords are also critical to computer security because they are the basis for most types of access control and for establishing user accountability. Because the PMO is ultimately responsible for SABRS security, it should be aware of the password parameters and ensure that passwords are robust.

## **General Support System Controls**

The PMO did not identify security controls implemented by other responsible parties because personnel did not believe those security controls were also their responsibility. PMO personnel stated that DISA was responsible for security over the general support system used by SABRS. This security includes physical and system software controls and a minimum level of recording or reviewing system activity. PMO personnel stated they did not need to know this information or obtain any assurances regarding the effectiveness of controls used by DISA, the organization that maintains the SABRS general support system. According to NIST, if an agency runs a major application on another organization’s general support system, the agency should request a copy of the other organization’s general support system security plan. In addition, DoD requires that all interconnected DoD information systems be managed to ensure that one system is not undermined by vulnerabilities of interconnected systems. The PMO did not obtain assurances of security controls over the mainframe by obtaining the general support system security plan as recommended by NIST. The PMO also did not obtain the DISA Statement of Auditing Standards No. 70 report. The Statement on Auditing Standards No. 70 report is used to provide an opinion on the adequacy of the internal controls over information processed by a service organization.

The PMO should be aware of types of controls in place or at least obtain the service organization security plan to determine if a security function performed by other responsible parties ensures that the security environment of the SABRS is not undermined.

---

## **TASO Account Identification**

An accurate list of all TASO account holders was not available because the PMO did not periodically reconcile the TASO appointment letters with actual TASO account holders identified within SABRS. SABRS TASOs create and assign user IDs and set user privileges. DFAS requires that TASOs be designated in an appointment letter.

We obtained three separate documents to determine SABRS TASO account holders:

- a SABRS generated user ID list,
- a list of TASO user IDs maintained by the PMO office, and
- TASO appointment letters maintained by the DFAS Kansas City Technology Services Organization.

The SABRS TASO account holders identified on each of these three documents did not agree and the PMO did not reconcile the differences.

The PMO must regularly reconcile TASO users with the applicable rights assigned in SABRS. When an individual is no longer required to perform TASO duties, appointment letters should be formally rescinded, along with the rights provided to TASOs. The individual is no longer accountable for TASO duties after the formal rescission. This practice would institute the principle of least privileges, which states that users should be granted access only to the resources they need to perform their official functions. By applying this principle, the PMO may limit damages resulting from human error or unauthorized use of system resources.

## **Acceptance Testing Documentation for Software Changes**

The PMO did not provide documentation that proved acceptance testing was completed prior to issuing software changes to SABRS. SABRS software change requests are documented in the Configuration Management Information System. We reviewed 17 SABRS software change requests from this system. There was no evidence of software acceptance testing by the PMO for any of the 17 requests. The PMO did provide us with e-mail documentation stating that the SABRS system change was accepted, but it did not provide any documentation that supported the type of testing conducted and the corresponding results.

---

The DFAS Kansas City Technology Services Organization is responsible for making the technical system changes to SABRS. Its own SABRS Software Configuration Management Plan requires the completion of acceptance testing prior to implementing software changes. In addition, its SABRS Software Development Plan states the USMC will participate in acceptance testing.

The PMO stated that it was responsible for performing acceptance testing on behalf of the USMC. USMC confirmed that they rely on the PMO to perform SABRS acceptance testing. Application users should conduct acceptance testing to verify that its requirements were met by the software change. Failure to document the results of acceptance testing creates uncertainty that user requirements have been met.

## **Authorized Software**

Unauthorized software had been installed on DFAS Kansas City network computers. SABRS security could be compromised by introducing unauthorized software to the DFAS Kansas City Enterprise-wide Local Area Network, which allows access to SABRS. The PMO did not coordinate with all parties responsible for security over SABRS to ensure that unauthorized software was restricted from network computers.

DoD Instruction 8500.2 restricts the use of unauthorized software and firmware on its information systems. However, DFAS Kansas City did not adequately prohibit users from installing software on their desktop computers.

DFAS Technology Services Organization personnel stated that because DFAS Kansas City is on the Base Realignment and Closure list, the computers located at DFAS Kansas City are not locked down using the Desktop Management Initiative. The Desktop Management Initiative locks down the computer so the user cannot load software or otherwise change the standard configuration. DFAS Technology Services Organization did not institute this at DFAS Kansas City because, personnel stated, it is not cost effective. However, based upon this information, DFAS does have the ability to lock down the computer so personnel cannot add unauthorized software. Unauthorized software increases the risk that viruses will be introduced, errors can occur, and copyright laws may be violated. The PMO should coordinate with the Technology Services Organization to ensure these vulnerabilities are minimized to provide an effective security control environment for SABRS.

---

## Recommendations, Management Comments, and Audit Response

**B.1. We recommend the Program Management Office coordinate with Defense Information Systems Agency to:**

**a. Determine if the Standard Accounting, Budgeting, and Reporting System password parameters meet the Joint Task Force Global Networks requirements.**

**b. Establish password parameters and maintain relevant documentation.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He explained that DISA provides password support over mainframe applications using Top Secret software and this software meets the Joint Task Force Global Network requirements to the best extent possible.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. Because DFAS owns SABRS, the PMO should be aware of the SABRS password parameters, regardless of who provides password support. We request that the Director, Information and Technology, DFAS determine and document, for DFAS and the PMO, whether the SABRS password parameters meet the Joint Task Force Global Networks requirements.

**B.2. We recommend the Program Management Office:**

**a. Identify security controls performed by responsible organizations.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that DFAS will identify the responsible organizations for implementing required security controls and will make these explicitly clear in the updated System Security Authorization Agreement. This action is required to be completed by June 30, 2008.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are responsive and no additional comments are required.

**b. Assess the security controls to ensure risks are identified and appropriate countermeasures are implemented.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that assessments are embedded activities in the certification and authorization process and the Federal Information Security Management Act reporting process.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. The Director, Information and Technology,

---

DFAS did not identify the proposed actions and completion dates for assessing the security controls to ensure risks are identified and appropriate countermeasures are implemented. We request that the Director, Information and Technology, DFAS provide the corrective actions taken and their associated implementation dates.

**c. Identify all Terminal Area Security Officer account holders maintained within the Standard Accounting, Budgeting, and Reporting System.**

**d. Document Terminal Area Security Officer account holders with formal appointment letters.**

**e. Periodically reconcile the appointment letters with Terminal Area Security Officer account holders identified within the Standard Accounting, Budgeting, and Reporting System to ensure Terminal Area Security Officer access is removed on a timely basis.**

**f. Rescind appointment letters for personnel who have been relieved of Terminal Area Security Officer account holder duties.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that DFAS already complies with these recommendations.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. The Director, Information and Technology, DFAS did not identify the proposed actions and completion dates for:

- identifying all TASO account holders maintained in SABRS,
- documenting TASO account holders with formal appointment letters,
- periodically reconciling the appointment letters with TASO account holders identified within SABRS to ensure TASO access is removed on a timely basis, and
- rescinding appointment letters for personnel who have been relieved of TASO account holder duties.

We request that the Director, Information and Technology, DFAS provide the corrective actions taken for these four recommendations and provide the associated implementation dates.

**B.3. We recommend the Program Management Office in conjunction with the Technology Services Organization and United States Marine Corps create documentation requirements for acceptance testing including what documentation needs to be maintained and for how long. This testing**

---

**documentation should include results of the tests performed in terms of pass or fail.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that the PMO performs the acceptance testing and authorizes it for release. Once all the software change requests for the release have passed acceptance testing, the Program Manager signs a memo indicating that the software can be loaded to the production environment.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. The DFAS did not provide documentation from the PMO that supports the type of testing conducted and the corresponding results. We request that the Director, Information and Technology, DFAS formally document requirements for acceptance testing including what documentation needs to be maintained and for how long.

**B.4. We recommend the Program Management Office in conjunction with the Technology Services Organization:**

**a. Provide training to Defense Finance and Accounting Service Kansas City personnel regarding DoD policies about unauthorized software.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that the DoD-required annual information assurance awareness training provides personnel with the policies regarding unauthorized software.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are responsive and no additional comments are required.

**b. Determine, document, and implement procedures to identify and restrict the load of unauthorized software.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. He stated that the Technology Services Organization maintains all test plans and test results for the system integration testing. The PMO performs the acceptance testing and authorizes it for release.

**Audit Comments.** Comments from the Director, Information and Technology, DFAS are partially responsive. The comments do not explain how users are prevented from installing unauthorized software on their computers. We request that the Director, Information and Technology, DFAS determine, document, and implement procedures to identify and restrict users from loading unauthorized software.

---

## **C. Defense Finance and Accounting Service and Defense Information Systems Agency Service Level Agreement**

DFAS Accounting Services-Marine Corps and DISA did not have an approved Service Level Agreement because DFAS did not sufficiently coordinate with DISA to complete the approval process. The absence of an approved Service Level Agreement could result in unfulfilled responsibilities and unresolved questioned authorities. In addition, neither party can be held accountable for not executing the Service Level Agreement requirements or for expenses incurred.

The PMO representing DFAS Accounting Services-Marine Corps and DISA did not fully execute and approve the Service Level Agreement because the PMO and other designated parties did not sign it. The Execution section of the Service Level Agreement states, “Official signatures indicate approval to the terms and conditions of this agreement by the indicated parties. This Service Level Agreement is effective upon the date of the final signature.” Without official signatures, the PMO cannot ensure DISA performs necessary security controls. Also, the PMO cannot hold DISA accountable if DISA fails to provide the necessary security controls.

NIST 800-35 states that a Service Level Agreement should define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance. To ensure SABRS is adequately protected, the PMO and DISA must have a clear understanding of their respective roles and responsibilities as discussed in the Service Level Agreement. Therefore, the Service Level Agreement must be properly approved.

---

## **Recommendations, Management Comments, and Audit Response**

**C. We recommend the PMO representing the Defense Finance and Accounting Service Accounting Services-Marine Corps coordinate with Defense Information Systems Agency to obtain approval of the Service Level Agreement by all applicable parties which includes authorized signatures of designated individuals.**

**Management Comments.** The Director, Information and Technology, DFAS concurred. The PMO has an annual Service Level Agreement with DISA.

**Audit Response.** Comments from the Director, Information and Technology, DFAS are partially responsive. The comments do not address whether the Service Level Agreement is signed. The Service Level Agreement is not effective until the date of the final signature. We request that the Director, Information and Technology, DFAS obtain approval of the Service Level Agreement by all applicable parties, which includes authorized signatures of designated individuals, and provide us a copy.

---

## Appendix A. Scope and Methodology

We conducted this audit from February 2006 through January 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 reviewed the general controls over SABRS provided by DFAS Kansas City. Specifically, we analyzed the 2003 and 2006 security plans, intrusion detection policies, software change request information, and related documentation. We interviewed DFAS Kansas City personnel to determine what general controls were in place over SABRS. We reviewed the FY 2005 FISMA report prepared by DFAS.

We used the Government Accountability Office Federal Information System Controls Audit Manual, January 1999, to develop the procedures performed during this audit. At the beginning of the audit we provided a list of required audit documentation needed to perform the audit work outlined in the Federal Information Systems Control Audit Manual. We did not receive all the documentation.

Our audit scope for general control testing was limited because not all documentation was made available during the audit. SABRS PMO management stated this information was not under their direct control and they did not provide this information. We were unable to assess the adequacy of the following general controls over SABRS:

- security controls necessary to address the hiring, transferring, termination, work performance requirements, and other personnel issues;
- controls to address the verification of appropriate training for employees designated with specialized duties or advanced system privileges;
- controls necessary to determine whether system administrators can identify all authorized users and their corresponding authorized access;
- controls used for authorizing emergency and temporary access;
- controls necessary to determine whether access to system data is appropriate as determined by the data owner; and,

- 
- policies and controls necessary to segregate incompatible duties.

Without effective general controls, application controls may be circumvented or modified. Based upon the magnitude of general control weaknesses, we did not perform audit work on the application controls within SABRS.

**Use of Computer-Processed Data.** We did not use computer-processed data to perform this audit.

**Government Accountability Office High-Risk Area.** The Government Accountability Office has identified several high-risk areas in DoD. This report covers the protection of the Federal Government's information systems.

No prior coverage has been conducted on general controls over SABRS during the last 5 years.

## Appendix B. Security Plan Comparison

The table below provides the areas of SABRS security plan noncompliance with DITSCAP and NIST. This is further detail of weaknesses identified in finding B.

<b>DITSCAP and NIST Requirements</b>	<b>Met Requirement in 2003?</b>	<b>Security Plan 2003 Explanation</b>	<b>Met Requirement in 2006?</b>	<b>Security Plan 2006 Explanation</b>
<b>MISSION DESCRIPTION AND SYSTEM IDENTIFICATION</b>				
System Description - Describe the system focusing on the information security relevant features of the system.	No	Security relevant features were not addressed in security plan.	No	Security relevant features were not addressed in security plan.
System Criticality	No	The security plan labeled SABRS system criticality as a Mission Assurance Category III system, although the COOP delineated the system as Priority 1.	No	The security plan labeled SABRS system criticality as a Mission Assurance Category III system, although the COOP delineates the system is Priority 1.
<b>ENVIRONMENT DESCRIPTION</b>				
Physical Security	No	The security plan did not list physical security controls for Defense Enterprise Computing Center St. Louis.	No	The security plan did not list physical security controls for DFAS Kansas City.
Administrative Issues	No	The security plan did not list the administrative security. For example, the separation of duties is not stated or explained.	No	The security plan did not list the administrative security. For example, the separation of duties is not stated or explained.

<b>DITSCAP and NIST Requirements</b>	<b>Met Requirement in 2003?</b>	<b>Security Plan 2003 Explanation</b>	<b>Met Requirement in 2006?</b>	<b>Security Plan 2006 Explanation</b>
Personnel	Yes	The security plan stated the number and type of personnel required to operate and maintain SABRS.	No	The security plan did not state the number and type of personnel required to operate and maintain SABRS.
Threat Description	No	The security plan does not describe the likelihood of threats and how those threats are mitigated.	No	The security plan does not describe the likelihood of threats and how those threats are mitigated.
<b>SYSTEM ARCHITECTURAL DESCRIPTION</b>				
National and DoD Security Requirements	Yes	The security plan lists applicable requirements.	No	The security plan did not list all applicable DoD and OMB requirements.
Governing Security Requisites	No	The security plan did not stipulate the SABRS specific or DFAS policies and procedures	No	The security plan did not stipulate the SABRS specific or DFAS policies and procedures
Security Concept of Operations	No	The security plan did not describe how the objectives of the security concept of operations would be accomplished.	No	The security plan did not describe how the objectives of the security concept of operations would be accomplished.
Network Connection Rules	No	The security plan did not identify the network connection rules.	No	The security plan did not identify the network connection rules.
Configuration and Change Management Requirements	No	The security plan did not identify the configuration and change management requirements.	No	The security plan did not identify the configuration and change management requirements.
<b>ORGANIZATIONS AND RESOURCES</b>				

<b>DITSCAP and NIST Requirements</b>	<b>Met Requirement in 2003?</b>	<b>Security Plan 2003 Explanation</b>	<b>Met Requirement in 2006?</b>	<b>Security Plan 2006 Explanation</b>
Organizations	Yes	The security plan identified other organizations and specific individuals for the certification and accreditation process.	No	The security plan did not identify a DISA representative for the certification and accreditation process.
Resources	No	All members of the certification and accreditation team were not independent of the system developer or project manager.	No	The security plan did not identify a DISA representative for the certification and accreditation process.
Other Supporting Organizations	Yes	The security plan identified other organization or working groups that were supporting the certification and accreditation process.	No	The security plan did not identify a DISA representative for the certification and accreditation process.
<b>DITSCAP PLAN</b>				
Information System characteristics	Yes	The security plan identified SABRS characteristics.	No	The security plan provided details of SABRS characteristics, but the security level changed from 2003 to 2006 without an explanation why this certification level was changed.
Tasks and Milestones	No	The security plan did not identify tasks and milestones.	No	The security plan did not identify who has the responsibility for the activity and completion criteria task.
Roles and Responsibilities	No	The security plan did not identify roles and responsibilities.	Yes	The security plan identified roles and responsibilities.

<b>DITSCAP and NIST Requirements</b>	<b>Met Requirement in 2003?</b>	<b>Security Plan 2003 Explanation</b>	<b>Met Requirement in 2006?</b>	<b>Security Plan 2006 Explanation</b>
APPENDIX D: SYSTEM CONCEPT OF OPERATIONS	No	The security plan did not describe how the SABRS operated.	No	The security plan did not describe how the SABRS operated.
APPENDIX E: INFORMATION SYSTEM SECURITY POLICY	No	The security plan did not identify and describe the security policies of SABRS.	No	The security plan did not identify and describe the security policies of SABRS.
APPENDIX F: SECURITY REQUIREMENTS AND/OR REQUIREMENTS TRACEABILITY MATRIX	No	The security plan did not identify how SABRS was compliant with security requirements.	No	The security plan did not identify how SABRS was compliant with security requirements.
APPENDIX H: SECURITY TEST AND EVALUATION PLAN AND PROCEDURES	No	The security plan did not document security test and evaluation plan and procedures or the results of that testing.	Yes	The security plan documented security test and evaluation plan and procedures.
APPENDIX I: APPLICABLE SYSTEM DEVELOPMENT ARTIFACTS OR SYSTEM DOCUMENTS	Yes	The security plan identified where the system development artifacts and system documents were located.	No	The security plan identified a letter that was supposed to identify a risk mitigation currently in progress, but the letter was not there.
APPENDIX J: SYSTEM RULES OF BEHAVIOR	No	The security plan did not identify any SABRS rules of behavior.	Yes	The security plan identified SABRS rules of behavior.
APPENDIX K: INCIDENT RESPONSE PLAN	No	The security plan did not identify monitoring for intrusions within SABRS or investigating intrusions.	No	The security plan did not identify monitoring for intrusions within SABRS or investigating intrusions.

<b>DITSCAP and NIST Requirements</b>	<b>Met Requirement in 2003?</b>	<b>Security Plan 2003 Explanation</b>	<b>Met Requirement in 2006?</b>	<b>Security Plan 2006 Explanation</b>
APPENDIX M: PERSONNEL CONTROLS AND TECHNICAL SECURITY CONTROLS	No	The security plan did not address the personnel and technical security controls for SABRS.	No	The security plan did not address the personnel and technical security controls for SABRS.
APPENDIX N: MOA - SYSTEM INTERCONNECT AGREEMENTS	No	The security plan did not include MOA and interconnection agreements.	Yes	The security plan identified MOA and interconnection agreements.
APPENDIX O: SECURITY EDUCATION, TRAINING, AND AWARENESS PLAN	No	The security plan did not identify security education, training, and awareness plans.	No	The security plan did not identify how the security education, training, and awareness were to be accomplished.
APPENDIX Q: RESIDUAL RISK ASSESSMENT RESULTS	No	The security plan did not identify residual risk assessment results.	No	The security plan did not identify residual risk assessment results.
ADDITIONAL NIST REQUIREMENTS DITSCAP DOES NOT REQUIRE				
Assignment of Security Responsibility	No	The security plan did not assign security responsibilities.	No	The security plan did not assign security responsibilities.
Data Integrity/Validation Controls	No	The security plan did not identify data integrity or data validation controls.	No	The security plan did not identify data integrity or data validation controls.
MAJOR APPLICATIONS-TECHNICAL CONTROLS				

---

<b>DITSCAP and NIST Requirements</b>	<b>Met Requirement in 2003?</b>	<b>Security Plan 2003 Explanation</b>	<b>Met Requirement in 2006?</b>	<b>Security Plan 2006 Explanation</b>
Identification and Authentication	No	The security plan did not identify the identification and authentication controls used by SABRS.	No	The security plan did not identify the identification and authentication controls used by SABRS.
Audit Trails	No	The security plan did not identify the audit trails for SABRS.	Yes	The security plan identified the audit trails for SABRS.

---

## **Appendix C. Report Distribution**

### **Office of the Secretary of Defense**

Under Secretary of Defense (Comptroller)/Chief Financial Officer  
Deputy Chief Financial Officer  
Deputy Comptroller (Program/Budget)

### **Department of the Navy**

Naval Inspector General  
Auditor General, Department of the Navy  
Director, Office of Financial Operations, ASN (FM&C)  
Assistant Deputy Commandant for Programs and Resources (Fiscal), United States  
Marine Corps

### **Other Defense Organizations**

Director, Defense Finance and Accounting Service  
Chief Information Officer, Defense Finance and Accounting Service  
Central Site Director, Defense Finance and Accounting Service Kansas City

### **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

# Defense Finance and Accounting Service Comments



DEFENSE FINANCE AND ACCOUNTING SERVICE  
ARLINGTON  
1851 SOUTH BELL STREET  
ARLINGTON, VA 22240-5291

MAR 10 2008

DFAS-HT

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Management Comments to Draft Report "Standard Accounting,  
Budgeting Reporting Systems (SABRS)", Report Number  
D2006-D000FC-0068.000

The attached is to provide updated Management Comments for the subject audit;  
Recommendations A1a-A1F, A2a-A2f, B2a-B2f, B4a, B4b and C.

My point of Contact Point of Contact for this is Mr. Michael Reiche, 216-204-7021.

A handwritten signature in black ink, appearing to read "Jerry S. Hinton".

Jerry S. Hinton  
Director, Information and Technology

Attachment:  
As stated

[www.dod.mil/dfas](http://www.dod.mil/dfas)  
Your Financial Partner @ Work

---

**Comments on the Draft Report for the General Controls Over the Standard  
Accounting, Budgeting, and Reporting System (SABRS)  
Project No. D2006-D000FC-0068.000**

**Recommendation A1a:** Separate the Terminal Area Security Officer functions from Defense Finance and Accounting Service Operations to ensure segregation of duties.

**Current Management Comments:** Nonconcur. TASO functions must be part of Operations because, in accordance with DFAS corporate Information Assurance (IA) policy then in affect during the audit, TASOs were intended to assist in implementing IA provisions for local users and systems and, therefore, had to be physically located in the same work area or organization as were the users. When the SABRS Program Office was part of the Accounting Business Line, the TASO functions were performed by PMO personnel. In November 2005 an SLA was established between the DFAS CIO and the DFAS ABL (Operations). Within the SLA was a functions list identifying what functions would remain in Operations and those that would transfer to the CIO. Function "L" from that list identified the TASO function as remaining with the business line. System access procedures involve multiple roles and persons, all of which together provide an appropriate measure of segregation of duties.

**Recommendation A1b:** Develop performance plans that:

(1) Incorporate security duties as performance measurements for personnel with security responsibilities, including but not limited to the Program Management Office.

**Current Management Comment:** Concur. The requirement to develop performance plans that incorporate security duties as performance measurements for personal with security responsibilities will be added to the DFAS Information Assurance Workforce Improvement Program (IAWIP).

(2) Management can use to evaluate personnel and hold them accountable for security operations.

**Current Management Comment:** Concur. The requirement to develop performance plans that incorporate security duties as performance measurements for personnel with security responsibilities will be added to the DFAS Information Assurance Workforce Improvement Program (IAWIP).

**Estimated Completion Date:** September 30, 2008.

**Recommendation A1c:** Identify and clearly delegate to specific offices the responsibility for establishing and executing policy and procedural authorities over the Standard Accounting, Budgeting, and Reporting System information technology security operations.

**Current Management Comment:** Concur. The Director, Information and Technology, DFAS, updated and published DFAS 8500.1-R, Information Assurance, November 2007, which corrects this finding. The updated policy assigns clear security responsibilities to program/system managers, as well as to system information assurance managers, site information assurance managers, and other security officials.

**Recommendation A1d:** Direct applicable offices to create, document, implement, and approve policies and procedures in accordance with National Institute of Standards and Technology, DoD, and Government Accountability Office guidance to address:

- access authorizations,
- periodic reviews of access authorizations,
- data encryption, and
- detecting and investigating security violations and activities.

**Current Management Comments:** Concur. Appropriate policies and procedures for each of the above subject areas have been documented and implemented as explained below:

The first Monday of each month, an automated process is executed that identifies ACcessor Identification (ACIDs) that have SABRS access but are not loaded to Top Secret Software (TSS) Security (orphans), ACIDs that have SABRS access but are set to VACANT (unassigned) in TSS Security and ACIDs that have SABRS access but the name on the ACID in SABRS does not match the name on the ACID in TSS Security. All ACIDs in these 3 categories have all SABRS access purged, including removal from the SABRS tables. A task is created and retained in Systems AHS Security each month that documents the validation showing the ACIDs removed, how many Natural Security entries were removed, and how many SABRS table entries were removed. The SABRS PMO and SABRSHELP@usmc.mil are notified each month when the validation is completed and the task is closed. They receive all the information (ACIDS/NATURAL SECURITY/TABLE ENTRIES removed) with the notification.

In addition, each time we receive a request for new SABRS access, all ACIDs in the ACID Group are reviewed (TSS Security to SABRS) to ensure names/users match. I.e. if we receive a new access request for ACID BK6B31, we will review all ACIDs in TSS Security and SABRS that begin with BK6B and ensure the names match. If we find a name miss-match, all SABRS access is immediately removed.

Marine Corps users must submit a DD 2875 and SABRS\_ReportNet Access Request.xls form to SABRSHELP@usmc.mil. HQMC/RFA retains the DD 2875, approves the request, and passed it to Systems AHS Security for granting the access. Comptroller office or HQMC/RFA loads the local SABRS tables as required to complete the access request.

For DFAS users, the supervisor submits a DD 2875 to Systems AHS Security. We assign the ACID, load the local SABRS tables, and then file the DD 2875 in a directory on the K: shared drive with a file name that indicates the system, users last name, and the ACID assigned (i.e. SABRS\_FRYER TGF0A1.pdf). I also maintain a master file of ACIDs assigned to DFAS users that indicates if we have a DD 2875 for the user/ACID. Once DFAS-KC closes permanently, we will go to each remaining DFAS SABRS user that does not have a DD 2875 on file and request that they provide one to retain SABRS access. I expect this process to be completed NLT October 31, 2008. The plan then is to annually review the DD 2875s and ensure users still require SABRS access. We began the DD 2875 requirement during November 2007 so the majority of DFAS-CL users that have been obtaining SABRS and ReportNet access have been providing DD 2875s for their access.

In regard to data encryption, all relevant data encryption requirements were identified in the System Security Authorization Agreement (SSAA) for SABRS. Relevant encryption requirements were identified in each of the following baseline IA controls as established in DoDI 8500.2 and as included in the SSAA: DCNR-1 Non-repudiation, ECCR-1 Encryption for Confidentiality (Data at Rest), ECCT-1 Encryption for Confidentiality (Data in Transit), EBRU-1 Remote Access for User Functions, IAKM-1 Key Management, and IAIA-1 Individual Identification and Authentication. Additional encryption requirements were identified and documented in the DITSCAP-based SSAA under the certification task, "COMSEC Compliance Verification." Since the above controls are inherited, their implementation is being done as required by entities outside of the C&A boundary for SABRS, and no further development of procedures is required. For example, as stated in the SSAA, the required encryption of transmissions is being provided via a secure VPN. The VPNs are implemented and managed jointly by DISA and DFAS infrastructure officials. The encryption requirements related to federal standards is being implemented via the DoD PKI program and the conforming encryption products that are part of the VPNs. ECCR-1 Encryption for Confidentiality (Data at Rest) is required only at the discretion of the data owner, and there were no data at rest encryption requirements established for SABRS data during the time of the audit.

Likewise, in regard to detecting and investigating security violations and activities, detection is accomplished via several baseline enclave and enclave boundary defense controls, all of which were identified in the SSAA. Investigating security violations is addressed in baseline IA control, VIIR-1, Incident Response, which is another inherited control. The SSAA includes the Incident Response Plan for SABRS as an attachment (Attachment K), which explains that investigations are done by the appropriate Computer Emergency Response Team (CERT) whether at DISA or DFAS, where each established CERT has its own documented procedures. Either CERT may report security

---

incidents to the DoD CERT and Defense Criminal Investigative Service (DCIS) as appropriate.

**Recommendation A1e:** Provide training to Defense Finance and Accounting Service Kansas City personnel regarding DoD and Defense Finance and Accounting license agreements and waivers.

**Current Management Comments:** Concur. Software licensing requirements are part of the mandatory IA Awareness training that is provided annually to all DFAS IT users. DFAS also broadcasted DFAS wide and posted on its ePortal educational information related to software piracy.

**Recommendation A1f:** Maintain license agreements and waivers for software to ensure only authorized software is present on the Defense Finance and Accounting Service computer system.

**Current Management Comment:** Concur. The requirement to maintain license agreements and waivers is stated in DFAS 8400.1-R, Information Technology. We will initiate a review of all installed software to confirm that all workstations are in compliance with software licensing agreements.

**Estimated Completion Date:** September 30, 2008.

**Recommendation A.2a:** Perform a risk assessment of Standard Accounting, Budgeting, and Reporting System at least every 3 years or when a major change occurs. This risk assessment should include identifying risks, the likelihood of the identified risks, and appropriate cost-effective countermeasures to mitigate the risks.

**Current Management Comments:** Concur. A Risk Assessment for SABRS is performed, as required, through the certification and accreditation (C&A) process at least every 3 years or when a major change occurs. We would like to suggest a clarification regarding the finding behind this recommendation, however. The DITSCAP-required threat analysis that was cited in the report as the basis for this recommendation was substantially altered when DoDI 8500.2 was issued subsequent to the DITSCAP. The banded sets of baseline controls established in DoDI 8500.2 were developed as a result of threat and risk analyses performed at the DoD level. These banded sets of baseline controls incorporated appropriate cost-effective countermeasures in response to a wide variety of anticipated threats to DoD IT systems, and negated the mandatory requirement to conduct a separate threat and risk assessment for each system. Accordingly, the DIACAP, which has since replaced the DITSCAP, does not require a threat analysis as part of the C&A process.

**Recommendation A2b:** Prepare and document a security plan.

**Current Management Comments:** Concur. In accordance with the DITSCAP, our security plan is the SSAA (in its entirety). The last SSAA was completed on 9 June,

---

2006. As part of the DFAS corporate transition to the DIACAP, all DFAS systems with current DITSCAP-based accreditations – including SABRS -- must complete by June 30, 2008, a DIACAP Implementation Plan (DIP), which will become the new security plan for SABRS.

**Recommendation A2c:** Identify the critical data and resources that support Standard Accounting, Budgeting, and Reporting System. The critical data and resources should be used to identify recovery priorities. This information should be documented in the Standard Accounting, Budgeting, and Reporting System contingency plan.

**Current Management Comments:** Concur. We update the SABRS contingency plan annually and also perform COOP tests. The last update and test was conducted on 7 November, 2007.

**Recommendation A2d:** Prepare an intrusion detection policy for the Standard Accounting, Budgeting, and Reporting System, including who is responsible for monitoring intrusion detection. The policy should address the recording and auditing of users' activities and intrusion incidents.

**Current Management Comments:** Concur. Intrusion detection and monitoring requirements are included in the SSAA as part of the DoDI 8500.2 baseline control, EBBD-1, Boundary Defense. For SABRS operations, this control is inherited from entities outside of the C&A boundary, as intrusion detection is implemented and performed by DISA personnel at DISA data processing centers and by DFAS and USMC network personnel at user enclaves.

**Recommendation A2e:** Ensure that all Standard Accounting, Budgeting, and Reporting System users have attended annual computer security awareness training and implement a method to verify that all users are adequately completing the required training.

**Current Management Comments:** Concur. An effective tracking mechanism is in place. All DoD Components, including DFAS and the USMC, are required by DoD policy to provide annual IA awareness training to all IT system users. DFAS is managing and tracking the completion of IA awareness training for its own users centrally using an automated method, which helps us to report this metric for inclusion in the DoD annual FISMA report. The USMC also must report for inclusion into the DoD annual FISMA report the percentage of its own users who receive annual IA awareness training, which promotes the highest compliance rate possible. Evidence of each user having completed the required awareness training also is documented on the system access authorization request forms, which are kept on file at USMC user locations.

**Recommendation B1a:** Determine if the Standard Accounting Budgeting, and Reporting System password parameters meet the Joint Task Force Global Networks requirements.

**Current Management Comment:** Concur. DISA provides password support over mainframe applications using Top Secret Software. This software meets the Joint Task Force Global Networks requirements to the best extent possible.

**Recommendation B1b:** Establish password parameters and maintain relevant documentation

**Current Management Comment:** Concur. As stated within comments for B1a; DISA provides password support over mainframe applications using TSS. This software meets the Joint Task Force Global Networks requirements to the best extent possible.

**Recommendation B2a:** Identify security controls performed by responsible organizations.

**Current Management Comments:** Concur. The identification of responsible organizations for the implementation of required security controls are implied in the current SSAA, but will be made explicitly clear in the DIACAP Implementation Plan for SABRS, which is due to be completed by June 30, 2008, as described in our response to Recommendation A.2.b.

**Recommendation B2b:** Assess the security controls to ensure risks are identified and appropriate countermeasures are implemented.

**Current Management Comments:** Concur. Assessments are embedded activities in the C&A process and the FISMA reporting process.

**Recommendation B2c:** Identify all Terminal Area Security Officer account holders maintained within the Standard Accounting, Budgeting, and Reporting System.

**Current Management Comment:** Concur. DFAS is already compliant with this recommendation.

**Recommendation B2d:** Document Terminal Area Security Officer account holders with formal appointment letters.

**Current Management Comment:** Concur. DFAS is already compliant with this recommendation.

**Recommendation B2e:** Periodically reconcile the appointment letters with Terminal Area Security officer account holders identified within the Standard Accounting, Budgeting, and Reporting System to ensure Terminal Area Security Officer access is removed on a timely basis.

**Current Management Comment:** Concur. DFAS is already compliant with this recommendation.

**Recommendation B2f:** Rescind appointment letters for personnel who have been relieved of Terminal Area Security Officer account holder duties.

**Current Management Comment:** Concur. DFAS is already compliant with this recommendation.

**Recommendation B3:** We recommend the Program Management Office in conjunction with the Technology Services Organization and United States Marine Corps create documentation requirements for acceptance testing including what documentation needs to be maintained and for how long. This testing documentation should include results of the tests performed in terms of pass or fail.

**Current Management Comments:** Concur. The TSO maintains all of the test plans and test results for the SIT testing. The PMO does the acceptance testing and authorizes it for release. The PMO tests the functionality requested in the System Change Request and keeps the test documentation for that SCR. After all SCRs for the release have passed acceptance testing, the PM signs a Memo indicating that the software can be loaded to the production environment.

**Recommendation B4a:** Provide training to Defense Finance and Accounting Service Kansas City Personnel regarding DoD policies about unauthorized software.

**Current Management Comment:** Concur. DFAS is required by DoD policy to attend annual IA awareness training which provides the policies regarding unauthorized software.

**Recommendation B4b:** Determine, document, and implement procedures to identify and restrict the load of unauthorized software.

**Current Management Comments:** Concur. The TSO maintains all of the test plans and test results for the SIT testing. The PMO does the acceptance testing and authorizes it for release. The PMO tests the functionality requested in the System Change Request and keeps the test documentation for that SCR. After all SCRs for the release have passed acceptance testing, the PM signs a Memo indicating that the software can be loaded to the production environment.

**Recommendation C:** We recommend the PMO representing the Defense Finance and Accounting Service Accounting Serviced-Marine Corps coordinate with Defense Information Systems Agency to obtain approval of the Service Level Agreement by all applicable parties which includes authorized signatures of designated individuals.

**Current Management Comments:** Concur. The PMO has an annual SLA with DISA. The CIO corporately also has an SLA with DISA.

## **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  
Edward A. Blair  
Cecelia M. Ball  
Michael Adams  
Beverly Smythe  
Denny Moore  
Cassandra Lane  
Erin Hart



# Inspector General Department of Defense

