December 7, 2005

Financial Management

Defense Finance and Accounting Service Corporate Database User Access Controls
(D-2006-033)

Department of Defense
Office of Inspector General

Constitution of the United States

A Regular Statement of Account of the Receipts and Expenditures of all public Money shall be published from time to time.

Article I, Section 9

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, Audit Followup and Technical Support 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 Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

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

Acronyms

ACL	Access Control List
BEIS	Business Enterprise Information Services
CEFT	Corporate Electronic Funds Transfer
DCD	Defense Finance and Accounting Service Corporate Database
DCII	Defense Finance and Accounting Service Corporate Information Infrastructure
DFAS	Defense Finance and Accounting Service

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

December 7, 2005

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Report on Defense Finance and Accounting Service Corporate Database User Access Controls (Report No. D-2006-033)

We are providing this report for your information and use. We considered management comments on a draft of this report in preparing the final report. The comments conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Carmelo G. Ventimiglia at (317) 510-3855 (DSN 699-3855) or Mr. Jack L. Armstrong at (317) 510-3846 (DSN 699-3846). For the report distribution, see Appendix B. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Patricia A. Marsh
for Paul J. Granetto, CPA
Assistant Inspector General
Defense Financial Auditing
Service

Department of Defense Office of Inspector General

Report No. D-2006-033 **December 7, 2005**
(Project No. D2005-D000FI-0052.000)

Defense Finance and Accounting Service Corporate Database User Access Controls

Executive Summary

Who Should Read This Report and Why? This report should be read by all Defense Finance and Accounting Service (DFAS) personnel with information assurance responsibilities and by all personnel assigned to the DFAS Corporate Database Project Management Office. The report identifies an internal control weakness involving the DFAS Corporate Database and suggests methods for improving user access security.

Background. This is the first in a series of reports related to our audit of the compilation process for financial reporting for the Army General Fund. It discusses the internal controls over DFAS Corporate Database user access. The DFAS Corporate Database will process accounting and financial information for various DoD Components. DFAS planned to start using the DFAS Corporate Database to process information for the compilation of the FY 2005 Army General Fund financial reports. However, a problem with establishing beginning account balances has caused system implementation to slip into FY 2006.

Data within the DFAS Corporate Database are segregated into various database tables. A database table is a single store of related information. Information assurance personnel assign user access roles that limit users' access to the database tables and system capabilities. For instance, users can be assigned database view and edit (write and delete information) capabilities. As of April 15, 2005, there were 2,323 user accounts that could access data stored in the DFAS Corporate Database tables. The user accounts were assigned by DFAS business or operational areas. Vender Pay Services, Travel Pay Services, and Army Accounting Services are the three business areas that use the Corporate Electronic Funds Transfer and Army accounting database tables. These database tables contain information regarding DoD financial transactions, including sensitive financial and tax information for 339,000 DoD contractors and 3.5 million DoD employees.

Results. DFAS internal controls over access to corporate electronic funds transfer and Army accounting data processed by the DFAS Corporate Database were not adequate. Specifically:

- inactive user accounts were not deactivated when DFAS Corporate Database access was no longer needed, and
- users were assigned edit capability although they did not need it to perform their duties.

As a result, the risk of misuse of sensitive information, such as bank routing and account numbers, was increased. The Director of DFAS should revise the "System Access

Control Policy and Standard Operating Procedures for DFAS Acquisition Management Organization" to require that functional information owners and supervisors certify that the monthly access control list has been reviewed and used to identify and deactivate inactive user accounts.

The Director should also require that functional information owners forward the certifications to the Business Enterprise Information System Production Support Office and review job responsibilities to ensure that user access to the DFAS Corporate Database is appropriately limited. In addition, the Director should require that user access to the DFAS Corporate Database be reported as a material internal control weakness until corrective actions have been taken and verified. (See the Finding section of the report for the detailed recommendations.)

Management Comments. The Component Acquisition Executive of Defense Finance and Accounting Service concurred with the recommendations and stated that the next version of the "System Access Control Policy and Standard Operating Procedures for DFAS Acquisition Management Organization" will require that functional information owners and supervisors certify the review of the monthly access control list. Functional information owners will also be required to forward the list to the Business Enterprise Information Services Production Support Office and maintain electronic evidence of the certification. He also stated that functional information owners will be directed to perform a one-time review of all job responsibilities, and DFAS will validate compliance with user access controls during preparation of the FY 2006 Annual Statement of Assurance. (See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.)

Table of Contents

Background

This is the first in a series of reports related to the audit of the compilation process for financial reporting for the Army General Fund. This report addresses access authorization to Defense Finance and Accounting Service (DFAS) Corporate Database (DCD). DCD is one of the systems that DFAS plans to use for compiling Army General Fund budget reports and financial statements. DFAS initially planned to use DCD to process information for the compilation of the FY 2005 Army General Fund financial reports. However, a problem with establishing beginning account balances caused the implementation to slip into FY 2006.

Department of Defense Business Enterprise Information Services. DCD is part of the DoD Business Enterprise Information Services (BEIS), which builds upon existing infrastructure to provide timely, accurate, and reliable business information from across DoD to support auditable financial statements. BEIS replaces the DFAS Corporate Information Infrastructure (DCII). DCII was the initial DFAS attempt to consolidate finance and accounting into a single, integrated financial management system.

The DCD Project Management Office is responsible for developing DCD. When fully implemented, DCD will make DoD Component accounting and finance information available to multiple users and applications at the same time. Approximately 80 percent of the financial information processed in DCD will originate from feeder systems,[1] and the remainder will originate from DFAS systems. DCD will eliminate multiple databases and the inefficiencies and reconciliation processes that can result when data are passed back and forth between information systems.

System Access Administration. Data within DCD are segregated into various database tables. A database table is a single store of related information. DCD information assurance personnel use Oracle internal role-based security to control user access to the database tables. DCD information assurance personnel assign user access roles that limit users'access to the database tables and functions. Users' roles are associated with job responsibilities that are contained in the job responsibility matrix. For example, the "GET_AY_GEN_FUND" database role is associated with the Army General Fund job responsibility. The Army General Fund job responsibility provides access to specific database tables and functional capabilities to edit (write and delete information) the data contained in those tables. The April 26, 2005, job responsibility matrix had 65 job responsibilities. Users can be assigned database view and edit capabilities. User access should be restricted to the minimum necessary to conduct business.

As of April 15, 2005, there were 2,323 user accounts that could access data stored in the DCD database tables. The user accounts were assigned by DFAS business

[1] Feeder systems are information systems, such as Standard Finance System and Standard Operation Maintenance Army Research and Development System, which transfer accounting data into DCD from field accounting activities.

or operational areas. Vender Pay Services, Travel Pay Services, and Army Accounting Services are the business areas that use the corporate electronic funds transfer (CEFT) and Army accounting database tables. As of April 15, 2005, 2,271 user accounts had access to CEFT and Army accounting database tables.

Information Assurance Policy. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, implements policy, assigns responsibilities, and prescribes procedures for the protection of DoD information systems. DoD Instruction 8500.2 requires that information assurance personnel establish and manage authorized user accounts for DoD information systems. This requirement includes deactivating user accounts when the user no longer needs access to DoD information systems.

"System Access Control Policy and Standard Operating Procedures for DFAS Corporate Information Infrastructure," November 2003, (DFAS policy)[2] implements DoD Instruction 8500.2 and provides instructions for managing system access for DCD. DFAS supervisors, functional information owners,[3] and the BEIS Production Support Office[4] personnel have responsibilities for controlling user access to DCD. The DFAS policy requires the following.

- User access will be limited to those who need to know and limited to information needed to perform assigned duties.

- The BEIS Production Support Office will maintain an access control list (ACL) of all user accounts to include the user's full name, the assigned database role, and the date the system was last accessed, and provide the ACL to the functional information owners and terminal access security officers.

- Functional information owners, who serve as the data stewards for the information in DCD that directly supports their business operations, will approve new users and identify the appropriate database roles assigned to each user. Functional information owners are also responsible for auditing user accounts against assigned roles.

- DFAS supervisors will review the ACL to ensure departed personnel have been removed and to account for each name within their division.

- Terminal area security officers, who serve as the focal points for local terminal security matters, along with the functional information owners, will notify the BEIS Production Support Office to terminate a user's account immediately upon the user's retirement, departure, or promotion.

[2] Superseded by DFAS "System Access Control Policy and Standard Operating Procedures for DFAS Acquisition Management Organization," July 21, 2005.

[3] Functional information owners were previously known as functional data owners.

[4] The BEIS Production Support Office was previously known as the DCII Production Support Office.

Objective

The overall audit objective was to determine whether the internal controls over the financial information processed by DCD and the Defense Departmental Reporting System-Budgetary were adequate for Army General Fund financial reporting. This report discusses the internal controls over user access to DCD and includes the results of our review of the Management Control Program as it relates to user access to DCD. We plan to issue another report addressing the overall control environment of DCD and the Defense Departmental Reporting System-Budgetary. See Appendix A for a discussion of the scope and methodology and for prior coverage related to the objective.

Managers' Internal Control Program

We identified a material internal control weakness for DFAS as defined by DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996. DFAS internal controls were not adequate to ensure that information assurance personnel deactivated user accounts when DCD access was no longer required. Recommendations 1. and 2., when implemented, will correct the identified weaknesses and result in improved access controls over sensitive DCD data. In addition, the DCD Project Management Office did not identify user access as an internal control weakness in its FY 2005 Annual Statement of Assurance dated June 14, 2005. The Finding section of this report discusses the details of the internal control weakness and the adequacy of management's self-evaluation process. A copy of the report will be provided to the senior official responsible for the Internal Control Program at DFAS.

System User Access Controls

DFAS internal controls over access were not adequate to protect CEFT and Army accounting data processed in DCD. Specifically:

- terminal area support officers and functional information owners did not notify the BEIS Production Support Office to deactivate inactive user accounts when DCD access was no longer needed, and
- functional information owners assigned edit capability to users who did not need it to perform their duties.

This occurred because procedures used for controlling access to the DCD did not ensure that DFAS personnel complied with DoD information assurance requirements and DFAS policy. As a result, the lack of adequate controls increased the risk of misuse of sensitive information, such as bank routing and account numbers.

Inactive User Accounts

Unneeded User Accounts. DCD information assurance personnel did not follow DFAS policy to deactivate user accounts with access to DCD CEFT and Army accounting data when users no longer needed access. Of the 2,271 user accounts on the CEFT and Army accounting ACLs, 585 (25.8 percent) had not accessed DCD since December 31, 2004. Of the 585 inactive user accounts, we judgmentally sampled 214 user accounts for current or former DFAS personnel. The following table shows the results of our validation of the need for those 214 users to access DCD.

Table. Validation of DFAS User Accounts

Determination	CEFT	Army Accounting	Total	Percentage of Total
No longer DFAS employees	19	9	28	13.1
Required access	26	17	43	20.1
No longer required access	41	46	87	40.7
Did not respond to inquiries	38	18	56	26.1
Total	**124**	**90**	**214**	**100.0**

DFAS Human Resources personnel determined that 28 of the 214 personnel with inactive user accounts either no longer worked at DFAS or were taking extended leave without pay. We attempted to contact the remaining 186 DFAS personnel with inactive user accounts to determine if they still needed DCD access. Of the 186 users, 43 responded that they still needed access, while 87 responded that they no longer needed access. The remaining 56 personnel did not respond to our inquiries. A total of 115 (87 who no longer required access plus 28 who are no longer active DFAS employees) user accounts remained active longer than necessary. Of these 115 user accounts, 61 (6-CEFT and 55-Army accounting) had the ability to edit data.

Deactivation Procedures. DFAS needs to improve its internal controls to ensure that inactive user accounts are promptly deactivated and monthly ACLs are routinely provided to DFAS supervisors and functional information owners as required by DFAS policy. DFAS policy did not contain sufficient controls to ensure that information assurance personnel took appropriate action to deactivate inactive user accounts.

Deactivating Inactive User Accounts. The CEFT functional information owner did not correctly deactivate inactive user accounts. Rather than request the BEIS Production Support Office to deactivate unneeded user accounts, the CEFT functional information owner removed all permissions except the "DCII User" role. The CEFT functional information owner stated that it was easier to reactivate access to DCD if the "DCII User" role was retained. However, the CEFT functional information owner was not aware that the "DCII User" role allowed users to view accounting data within the DCD database tables.

Access Control List. DFAS supervisors, functional information owners, and terminal area security officers did not always request that the BEIS Production Support Office deactivate inactive user accounts. The information in the table illustrates that DFAS personnel were not adequately following DFAS policy to identify and request deactivation of inactive user accounts. A contributing factor was that the BEIS Production Support Office did not provide a monthly ACL to DFAS supervisors and functional information owners as required by DFAS policy. The CEFT functional information owner received an ACL dated March 15, 2005, but had not received a list for the previous 6 months. Other functional information owners had not received monthly ACLs for at least 1 year. Because the functional information owners and DFAS supervisors did not receive the monthly ACLs, they did not have important information necessary to identify and to deactivate inactive user accounts.

DFAS Deactivation Policy. DFAS did not establish sufficient controls to ensure that information assurance personnel took appropriate action to deactivate inactive user accounts. Specifically, the DFAS policy did not require that:

- supervisors and functional information owners certify that they reviewed the monthly ACLs and requested that the BEIS Production Support Office deactivate inactive user accounts,

- supervisors and functional information owners provide the certified monthly ACLs to the BEIS Production Support Office, and

- the BEIS Production Support Office retain copies of the certified ACLs.

User Edit Capabilities

The functional information owner assigned Army accounting users edit capability that was not commensurate with their duties. The ACL dated April 15, 2005, had 482 users with Army General Fund job responsibility. Between April 17, and August 11, 2005, the Army accounting functional information owner removed edit capabilities for 464 of the users. One user had edit capability from January 10, 2003. Of the 464 users, 403 had edit capability removed on May 10, and May 11, 2005. Only 18 users were left with edit capabilities.

The Army accounting functional information owner did not ensure that users were assigned edit responsibility in accordance with DFAS policy. DFAS should perform a one-time review of all the job responsibilities for DCD to ensure that edit capabilities are assigned only to those who need it to perform their duties. The Army General Fund job responsibility is only 1 of the 65 job responsibilities with access to Army accounting data in DCD.

System Vulnerabilities

DCD access controls did not comply with DoD Instruction 8500.2, increasing the risk that sensitive information would be misused. Unnecessary access to the database tables provides users an opportunity to make unauthorized changes to accounts and files, or to use sensitive information to perpetrate financial fraud or other abuse. The DCD contains sensitive financial and tax information for 339,000 DoD contractors and 3.5 million DoD employees. Through DCD, users have access to sensitive accounting data, and vendor and employee tax identification numbers, bank routing and account numbers, names, addresses, and phone numbers.

Management Actions

On July 21, 2005, DFAS issued revised policy on access controls titled "DFAS System Access Control Policy and Standard Operating Procedures for DFAS Acquisition Management Organization." The revised policy addresses controls for all DFAS-owned financial management systems. The policy did not include our recommendation that functional information owners and supervisors certify that the monthly ACL has been reviewed and that they forward the certifications to the BEIS Production Support Office. In addition, the revised policy did not require that the BEIS Production Support Office retain evidence of certifications.

On May 20, 2005, the DCD Project Management Office initiated a system change request, titled "CSF IA Policy Deactivate Users Inactive for 120 Days," for DCD that will improve user access controls. The DCD will be reprogrammed to automatically notify functional information owners when user accounts have not been used for 60 days. If the account remains inactive for a total of 90 days, the system will automatically deactivate the user account. The DCD Project Management Office originally planned to execute the system change request in July 2005; however, the system change request was implemented September 19, 2005.

We provided the CEFT functional information owner with the names of employees who had departed DFAS or had been reassigned. The BEIS Production Support Office deactivated those inactive user accounts.

Adequacy of Management's Self-Evaluation

The FY 2005 self-evaluation of internal controls prepared by the DCD Project Management Office did not identify and report DCD user access as an internal control weakness. The DCD Project Management Office had been identified as the assessable unit; however, DCD access controls had not been assessed since July 2003, when the management self-evaluation was first prepared. At that time, DCD was still in the system development test phase and the internal controls were being initially established. The DCD Project Management Office has included an assessment of internal controls over DCD access in its FY 2005 self-evaluation; however, it did not report DCD access as a material internal control weakness in its FY 2005 Annual Statement of Assurance. The June 14, 2005, transmittal memorandum stated that the evaluation did not identify any material weaknesses although the self-evaluation indicated that the system change would not be implemented until September 2005.

The DCD Project Management Office has responsibility for reporting DCD user access as a material weakness because it is identified as the assessable unit. However, the DCD Project Management Office does not have the authority to ensure that DFAS supervisors and functional information owners comply with user access policy because this is a DFAS management issue. Until the recommendations in this report have been implemented and the internal control weakness has been corrected, DFAS should report DCD access as a material internal control weakness in the Annual Statement of Assurance.

Recommendations, Management Comments, and Audit Response

We recommend that the Director of Defense Finance and Accounting Service:

1. Revise the "System Access Control Policy and Standard Operating Procedures for DFAS Acquisition Management Organization" to require that:

a. Functional information owners and supervisors certify that the monthly access control list has been reviewed and that action has been taken to deactivate user accounts no longer needed.

b. Functional information owners forward the certifications to the Business Enterprise Information Services Production Support Office.

c. The Business Enterprise Information Services Production Support Office maintains evidence of the certifications.

Management Comments. The Component Acquisition Executive at DFAS concurred and stated that DFAS will revise procedures to require that functional information owners certify that they have reviewed the monthly access control list, forward certifications to the Production Support Office, and maintain evidence of the certifications.

Audit Response. The DFAS comments are responsive. The updated procedures will require functional information owners, instead of the BEIS Production Support Office, to maintain electronic evidence of certifications. This action meets the intent of the recommendation.

2. Require that the functional information owners perform a one-time review of all job responsibilities to ensure that user access is restricted to the minimum necessary to conduct business.

Management Comments. The Component Acquisition Executive at DFAS concurred and stated that functional information owners will be directed to perform a one-time review of all job responsibilities to ensure that user access is restricted to the minimum necessary to conduct business.

3. Report user access to the Defense Finance and Accounting Service Corporate Database as a material internal control weakness in the Annual Statement of Assurance until Recommendations 1. and 2. have been implemented and it has been verified that the weakness has been corrected.

Management Comments. The Component Acquisition Executive at DFAS concurred and stated that the actions taken in response to Recommendations 1. and 2. have corrected the material internal control weakness. He stated that DFAS will validate compliance with the recommendations during preparation of the FY 2006 Annual Statement of Assurance.

Appendix A. Scope and Methodology

We reviewed the internal controls for deactivating user accounts when the user no longer needed to access DCD. We reviewed the CEFT ACL as of March 15, 2005, and the Army accounting ACL as of April 15, 2005. These two ACLs listed 2,271 (97.8 percent) of the 2,323 total DCD user accounts as of April 15, 2005, that could access the CEFT and Army accounting data. We identified 585 users with access to the CEFT and Army accounting database tables that had not accessed the DCD since December 31, 2004. Of these 585 users, we judgmentally sampled 214 current and former DFAS employees to determine if they required access to the system. Of the 214 users, 186 had DFAS email accounts. We attempted to contact the 186 users with DFAS email accounts. For the 28 users without DFAS email accounts, DFAS Human Resources personnel determined that 27 users were former DFAS employees and 1 user was on extended leave without pay.

We reviewed the Army General Fund job responsibility to determine if view and edit capabilities were properly assigned to users. The Army General Fund job responsibility was 1 of 65 reported on the April 26, 2005, Job Responsibility Matrix. We selected Army General Fund job responsibility because it accounted for 482 (88.3 percent) of the 546 user accounts with access to Army accounting data as of April 15, 2005.

We also reviewed DFAS policies on information assurance and determined whether DFAS procedures complied with DoD requirements. We also discussed procedures for assigning access capabilities and identifying and deactivating inactive user accounts with DFAS supervisors, BEIS Production Support Office personnel, DCD Project Management Office personnel, and functional information owners.

We performed this audit from October 2004 through September 2005 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We relied on the CEFT and Army accounting ACLs generated by BEIS Production Support Office to identify users who had not accessed DCD since December 31, 2004. We used other information to determine if personnel with inactive user accounts needed access to DCD. Because we only relied on the computer-processed data to determine if inactive user accounts existed, we did not perform detailed tests to confirm the reliability of the computer-processed data. Nothing came to our attention as a result of specific procedures that caused us to doubt the reliability of the computer-processed data.

Management Control Program. DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, require DoD organizations to implement a comprehensive system of management (internal) controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls. We evaluated the DFAS internal controls over user access to DCD. Specifically, we reviewed procedures

that DFAS used to assign access responsibilities to users and to deactivate users who no longer required access to DCD. We also reviewed the adequacy of management's self-evaluation of those controls.

Government Accountability Office High-Risk Area. The Government Accountability Office (GAO) has identified several high-risk areas in DoD. This report provides coverage of the Financial Management high-risk area.

Prior Coverage

During the last 5 years, the GAO and the Department of Defense Inspector General (DoD IG) have issued three reports discussing the DCD. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO-03-465, "DoD Business System Modernization, Continued Investment in Key Accounting Systems Needs to be Justified," March 28, 2003

DoD IG

DoD IG Report No. D-2002-014, "Development of Defense Finance and Accounting Service Corporate Database and Other Financial Management Systems," November 7, 2001

DoD IG Report No. D-2001-030, "Oversight of Defense Finance and Accounting Service Corporate Database Development," December 28, 2000

Appendix B. Report Distribution

Office of the Secretary of Defense

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

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Other Defense Organization

Director, Defense Finance and Accounting Service

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 Government Reform

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Defense Finance and Accounting Service Comments

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

OCT 25 2005

MEMORANDUM FOR PROGRAM DIRECTOR, DEFENSE FINANCIAL AUDITING SERVICE, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Report of Defense Finance and Accounting Service Corporate Database User Access Controls (Project No. D2005-D000FI-0052.000)

In accordance with subject audit, the Acquisition Management Office has implemented recommendations contained in the draft report.

My point of contact for additional information is Greg Williams at 317-510-3135.

Timothy J. Harp
Component Acquisition Executive

DFAS Management Comments to DoDIG Draft Report, "Defense Finance and Accounting Service Corporate Database User Access Control (Project No. D2005-D000FI-0052.000) dated September 30, 2005

Recommendation 1: Revise the "System Access Control Policy and Standard Operating Procedures for DFAS Acquisition Management Organization" to require that:

a. Functional information owners and supervisors certify that the monthly access control list has been reviewed and that action has been taken to deactivate user accounts no longer needed.

b. Functional information owners forward the certifications to the Business Enterprise Information Services Production Support Office.

c. The Business Enterprise Information Services Production Support Office maintains evidence of the certifications.

Management Comments: Item A. Concur. The next revision of the System Control Policy and Standard Operating Procedure for DFAS Acquisition Management Organization will require that functional information owners and supervisors begin certifying (electronically, e.g., via email) that their monthly access control list has been reviewed and action taken to deactivate user accounts no longer needed. Additionally, to further augment this area, SCR 3006 was implemented on September 19th per direction from the DoDIG. DCD/DCW system change implemented generates report going to Functional Information Owners when the user has not accessed system in 60 days. The DCD/DCW automatically deactivates user accounts which have not been accessed for over 90 days.

ECD: December 2, 2005

Item B. Concur. The updated procedures will require Functional Information Owners to forward certifications (electronically, e.g., via email) to the Production Support Office.

ECD: December 2, 2005.

Item C. Concur. The updated procedures will require Functional Information Owners to maintain electronic evidence of the certifications.

ECD: December 2, 2005.

Recommendation 2: Require that the functional information owners perform a one-time review of all job responsibilities to ensure that user access is restricted to the minimum necessary to conduct business.

Management Comments: Concur. Functional Information Owners will be directed to perform a one-time review of all job responsibilities to ensure that user access is restricted to the minimum necessary to conduct business.

EDC: December 2, 2005.

Recommendation 3: Report user access to the Defense Finance and Accounting Service Corporate Database as a material control weakness in the Annual Statement of Assurance until recommendations 1 & 2 have been implemented and it has been verified that the weakness has been corrected.

Management Comments: Believe that we have satisfactory implemented Recommendations 1 and 2 in a manner that corrects any material internal control weaknesses that would have been applicable to the Annual Statement of Assurance. We will review/validate implementation of recommendations 1 & 2 during the FY06 Annual Statement of Assurance.

ECD: September 2006.

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
Carmelo G. Ventimiglia
Jack L. Armstrong
Mark A. Ives
John T. Ferguson