Audit Report

OFFICE OF THE INSPECTOR GENERAL

GENERAL AND APPLICATION CONTROLS OVER THE MECHANIZATION OF CONTRACT ADMINISTRATION SERVICES SYSTEM

Report No. 98-007

October 9, 1997

Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate 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 Planning and Coordination Branch, Analysis, Planning and Technical Support Directorate, at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ADP	Automated Data Processing
DFAS	Defense Finance and Accounting Service
DLA	Defense Logistics Agency
DLAR	Defense Logistics Agency Regulation
DMC	Defense Megacenter
DSDC	Defense Logistics Agency Systems Design Center
ID	Identification Code
IG	Inspector General
MOCAS	Mechanization of Contract Administration Services
RACF	Resource Access and Control Facility
TASO	Terminal Access Security Officer
TIS	Total Information System

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

October 9, 1997

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE,
DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Audit Report on the General and Application Controls Over the Mechanization of Contract Administration Services System (Report No. 98-007)

We are providing this report for information and use. We considered management comments on a draft of this report when preparing the final report.

The Defense Finance and Accounting Service and Defense Logistics Agency comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the cooperation extended by staffs from the Defense Finance and Accounting Service and the Defense Logistics Agency Systems Design Center. Questions on the audit should be directed to Mr. Christian Hendricks, Audit Program Director, at (703) 604-9140 (DSN 664-9140) or Mr. Carl Zielke, Audit Project Manager, at (703) 604-9147 (DSN 664-9147). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-007 **October 9, 1997**
(Project No. 6FG-0083.00)

Audit of General and Application Controls Over the Mechanization of Contract Administration Services System

Executive Summary

Introduction. This is the first in a series of audit reports on controls for the Mechanization of Contract Administration Services (MOCAS) system. We announced the audit on August 16, 1996, and subsequently revised our objectives and reannounced the audit on December 11, 1996. We reviewed the MOCAS production system at the Defense Finance and Accounting Service Center in Columbus, Ohio (DFAS Columbus Center), and the MOCAS development environment at the Defense Logistics Agency Systems Design Center in Columbus, Ohio.

Audit Objectives. The overall audit objective was to evaluate general and application controls over the Mechanization of Contract Administration Services system to ensure that MOCAS data are complete, accurate, and prevent and detect potential fraudulent payments. Specifically, we reviewed access controls, security administration, software change management, and contingency planning. We also reviewed application controls over transactions processed in the MOCAS system. We evaluated the management control program as it relates to the MOCAS system.

Audit Results. Control deficiencies in MOCAS previously reported by the Inspector General, DoD, and by the Internal Review office of the DFAS Columbus Center have not been corrected. User identification codes in MOCAS are not being deleted when an employee resigns or is terminated. Employees also have access to MOCAS-sensitive tables not related to their current assignment, such as nonsupervisory personnel with access to tables reserved only for supervisors (Finding A).

The Defense Logistics Agency Systems Design Center had not designated application programming positions as critical-sensitive in the organization and in the contractor organizations that have requested access to the Defense Logistics Agency systems. Critical-sensitive positions require background investigations to be in compliance with DoD Regulation 5200.2-R and Defense Logistics Agency regulations (Finding B).

Summary of Recommendations. We recommend that the DFAS Columbus Center issue security guidance to the personnel responsible for implementing employee-level security, periodically review the MOCAS system reports which state the employees who have access to supervisory files and other sensitive files, and terminate user accounts and sensitive file access that are no longer required by the employee's position. We also recommend that the Defense Logistics Agency Systems Design Center designate the

employee and contractor application programming positions as critical-sensitive and require background investigations of the personnel in those positions.

Management Comments. We received comments on this report from the Deputy Director for Finance, Defense Finance and Accounting Service (DFAS). The DFAS management concurred with the report's recommendations. DFAS Columbus Center will issue security guidance to the personnel responsible for implementing employee-level security, periodically review the MOCAS system to verify employee access to supervisory files and other sensitive files, and terminate user accounts and sensitive file access that are no longer required by the employee's position.

We also received comments on this report from the Defense Logistics Agency. The Defense Logistics Agency management concurred with the audit finding concerning background investigations of critical-sensitive application programming positions at the Defense Logistics Agency Systems Design Center (DSDC). The Defense Logistics Agency stated that they would direct the Commander, DSDC, to prepare a plan to obtain background investigations of DSDC application programmers and appropriate contractor programmers. Please refer to Part I for a complete discussion of the management comments and to Part III for the complete text of the management comments.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objectives 3
Finding A. Control Over Access to MOCAS at DFAS Columbus 4
Finding B. Position Classifications at the Defense Logistics Agency Systems Design Center, Columbus, Ohio 9

Part II - Additional Information

Appendix A. Audit Process
Scope and Methodology 13
Management Control Program 14
Appendix B. Summary of Prior Coverage 15
Appendix C. MOCAS Data Tables Reviewed 18
Appendix D. Report Distribution 19

Part III - Management Comments

Under Secretary of Defense (Comptroller) Comments 22
Defense Finance and Accounting Service Comments 23
Defense Logistics Agency Comments 25

Part I - Audit Results

Audit Background

The Mechanization of Contract Administration Services (MOCAS) system is an integrated system designed to support the administration of contracts after they have been awarded. The MOCAS system is used by contract administration offices, contract payment offices, procurement managers, funding stations, consignees, and other personnel needing access to contract and payment data. As of September 1996, MOCAS performed contract administration on approximately 387,000 contracts valued at more than $810 billion.

Responsible Organizations. The Defense Finance and Accounting Service Columbus Center, Ohio (DFAS Columbus), is the MOCAS functional proponent and administers the system. DFAS Columbus processes MOCAS transactions on computers at the Defense Megacenter, Columbus, Ohio (DMC Columbus).

The DMC Columbus has an interservice agreement with DFAS to provide computer resources and customer support for various data processing services. The DMC Columbus reports to the Defense Information Systems Agency, Western Hemisphere. The DMC Columbus processes data for MOCAS and for other DoD financial and logistics information systems. DMC Columbus also processes payroll transactions for DoD civilian and military employees as well as DoD orders and payments for goods and services.

The Defense Logistics Agency System Design Center (DSDC), Columbus, Ohio, is the central design organization for MOCAS and is responsible for development and maintenance of MOCAS software.

General Controls. General controls are management controls that apply to multiple software applications and to the overall computer operations of an agency, organization, or installation. General controls include:

- organization and management controls such as planning, policies, and procedures;
- development controls, including change management; and
- operation controls such as physical and logical security.

Application Controls. Application controls are computerized steps within the application software and related manual procedures to control the processing of various types of transactions. For example, some application controls depend on computerized edit checks, which consist of format, existence, reasonableness, and other checks on the data. The edit checks are built into

each application during its development. Application controls provide control over the data to ensure that it meets specific criteria before it is accepted into the system.

Audit of Application Controls. Application controls in MOCAS were addressed in Inspector General, DoD, Report No. 95-046, "Data Input Controls for the Mechanization of Contract Administration Services System," November 30, 1994. Fifty-seven data entry fields were determined to have insufficient data input controls. The report recommended several corrective actions, such as rewriting portions of employee desk procedures, requiring supervisors to more closely monitor the listings of rejected input provided by MOCAS, and establishing additional automated edit and validation controls for the data input fields that accepted invalid data. The Deputy Comptroller (Financial Systems) concurred with the recommendations respective to the updates of employee desk procedures and greater monitoring of rejected listings and partially concurred with the recommendation pertaining to additional edit and validation controls, stating that DFAS would complete a study on the data input fields in MOCAS and determine whether any changes were appropriate. We reviewed the updates that were made to the employee desk procedures and the study that was performed regarding the additional controls over the data entry fields and took no exception to the updates of the desk procedures and the changes recommended by the study of the edit fields.

Compliance with DoD Year 2000 Program. The Mechanization of Contract Administration Services system may process date-related data incorrectly for dates beginning in the year 2000. However, the Defense Logistics Agency Systems Design Center (the central design authority for MOCAS) has identified and is actively working on the actions needed to ensure that MOCAS correctly processes these dates.

Audit Objectives

The overall audit objective was to determine the adequacy of selected general and application controls. We also examined the management control program of the DFAS Columbus Center, DMC Columbus, and DSDC as it applied to the overall audit objective. See Appendix A for the audit scope and methodology and a discussion of the management control program. See Appendix B for a summary of prior audit and review coverage related to the audit objectives.

Finding A. Control Over Access to MOCAS at DFAS Columbus

Control weaknesses over access to the Mechanization of Contract Administration Services (MOCAS) system would allow unauthorized users access to sensitive data in the system. Specifically:

o user identification codes (user IDs) of former employees of the DFAS Columbus Center were not removed, and

o access to sensitive MOCAS tables related to an employee's duties were not removed when duty requirements changed.

These conditions occurred because the Terminal Area Security Officers (TASOs) did not have appropriate guidelines for removing an employee's user ID and access to sensitive MOCAS tables at the end of a job assignment. In FY 1996, of 96 employees at the DFAS Columbus Center who were terminated or resigned, 26 (27 percent) still had authorized access to MOCAS-sensitive data. Additionally, 80 employees had access to MOCAS tables that were not related to their current assignment. As a result, sensitive MOCAS payment data were vulnerable to inappropriate access and manipulation, which allowed for potential fraudulent activity.

Criteria Regarding Access Control

DFAS Regulation 8000.1-R. The DFAS Columbus Center uses Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management Policy and Instructional Guidance," August 21, 1996, which directs, in part, that when a user no longer requires access to a data table or a system to remove the user from the access lists for the data tables and, if necessary, delete the user account.

Terminal Area Security Officers. TASOs at the DFAS Columbus Center assist Information System Security Officers at the Defense Megacenter, Columbus (DMC, Columbus), in ensuring that remote terminal access complies with security procedures. The TASOs request user IDs and passwords for personnel at DFAS Columbus Center and request termination of user IDs and passwords that are no longer needed. The TASOs also request access to sensitive MOCAS tables for personnel at DFAS Columbus Center.

Inspector General, DoD Report No. 95-046, "Data Input Controls for the Mechanization of Contract Administration Services System." Inspector General, DoD, Report 95-046, dated November 30, 1994, states that user identification codes of former employees of the DFAS Columbus Center were not canceled promptly. The report states that this condition occurred because TASOs did not have guidelines for the termination of user IDs and because the MOCAS access listings were not periodically reviewed to ensure that only valid users maintained access. The report recommended that the access for the former DFAS employees be terminated and that the list of user IDs be reviewed semiannually. Management at the DFAS-Columbus Center concurred, stating that the user IDs of the former employees would be deleted and that the semiannual reviews of user IDs would begin in January 1995. The report also states that DFAS-Columbus had completed a draft procedure containing updated guidance for the TASOs; therefore, no recommendations in this area were made.

DFAS Columbus Center Internal Review Report, "Contract Entitlement Directorate, MOCAS System Access Review." This report, dated March 1996, states that inconsistent and unauthorized access has been granted to MOCAS sensitive tables based on instructions from individual supervisors without adherence to the access charts published by the DFAS-Columbus Contract Entitlement Directorate. These charts define the access to sensitive MOCAS tables needed by various position descriptions. The report recommends that all TASOs should be instructed not to authorize access outside of these charts. DFAS-Columbus management concurred, stating that a 100 percent review of all access in the Contract Entitlement Directorate was completed and all access not required by the employees' position description was deleted. However, the TASO desk procedures were still in draft at the time of the release of the subject report.

Audit Procedures

Our review of user IDs was based on the "Total Information System Extended Security System Batch Utilities Application to User Relationship Report" (the TIS report). The TIS report is a computerized report on the security of MOCAS data tables; it identifies all MOCAS data tables by file number, identifies the users who have access to each file and shows their user IDs. To perform our review, we used nonstatistical methods to select 5 MOCAS data tables from the TIS report and reviewed all DFAS Columbus Center users who had update access to these tables. Update access allows users to change existing MOCAS data or to input data on contractor invoices and disbursements. We then identified user IDs that began with the initials DDM or DDP, which indicated that the users were DFAS Columbus Center employees. Appendix C lists the data tables we reviewed.

Access Controls

Controls over access to MOCAS-sensitive data were inadequate. Of the 96 employees who were terminated or resigned during FY 1996, 26 (27 percent) still had MOCAS authorized access to sensitive payment data.

Employees were given access that was inappropriate for their job description, such as access reserved for supervisory personnel. For example, we determined that 51 nonsupervisory employees had update access to the supervisory tables for the contract input functions, the line item schedule summary report functions, and the contract research functions. We also found that 29 employees had update access to the contractor remit-to address table which was not required by their current duties. The remit-to address table contains the contractor billing addresses to which payment checks are sent. All 80 employees could circumvent established procedures, avoid supervisory reviews, and make other unauthorized changes.

Causes of Inadequate Access Controls

These access control weaknesses occurred because the TASOs did not receive adequate guidance on when and how user IDs should be canceled and they did not regularly review the lists of users with access to MOCAS.

TASO Guidance. Although overall control of MOCAS access is the responsibility of the Defense Megacenter, Columbus, the TASOs at the DFAS Columbus Center provide input to the Megacenter regarding maintenance of MOCAS user IDs and MOCAS access granted to DFAS employees. The TASOs need guidance in this area to ensure a consistently secure environment.

Desk procedures that will provide proper guidelines to the TASOs to effectively control access to the MOCAS system are in draft awaiting final issue. However, the procedures have been in management review since March 1995.

Reviewing Lists of Users with Access to MOCAS. TASOs at the DFAS Columbus Center did not periodically review the TIS report. As a result, invalid user IDs and user access were not appropriately removed as required by DFAS Regulation 8000.1-R.

Actions Taken By Management

Management at DFAS Columbus Center has initiated actions to remove the 26 user accounts that are no longer needed and has issued inquiries to the user departments to determine the necessity of access to the sensitive MOCAS tables.

Conclusion

Controls over access to MOCAS sensitive contract and payment data were not adequate to prevent unauthorized access. Until user IDs are properly managed and controlled, the potential will exist for unauthorized changes to be made in MOCAS data. Accordingly, the desk procedures need to be issued and enforced.

Recommendations and Management Comments

A. We recommend that the Director, Defense Finance and Accounting Service, Columbus Center:

1. Issue the desk procedure for the Terminal Area Security Officers and train all Terminal Area Security Officers in its use within 90 days of issuance.

2. Direct the Terminal Area Security Officers at the Defense Finance and Accounting Service Columbus Center to:

a. Periodically review the "Total Information System Extended Security System Batch Utilities Application to User Relationship Report" for all supervisory files and other sensitive files in the Mechanization of Contract Administration Services system.

b. Terminate user IDs that are no longer required by the employee's position and access to files that is no longer required by the employee's position.

Management Comments. The Deputy Director for Finance, Defense Finance and Accounting Service, concurred. The Defense Finance and Accounting Service (DFAS) Columbus Center management will issue security guidance to the personnel responsible for implementing employee-level security, will review the MOCAS system reports which state the employees who have access to supervisory files and other sensitive files, and terminate user accounts and sensitive file access that are no longer required by the employee's position. Management plans to complete the security training by November 15, 1997, and to complete a 100-percent review of all supervisory tables for unauthorized access by December 31, 1997.

Finding B. Position Classifications at the Defense Logistics Agency Systems Design Center, Columbus, Ohio

MOCAS application software positions with access to critical-sensitive contract payment program code did not receive the required access designations and background investigations. This condition existed because the Defense Logistics Agency Systems Design Center (DSDC), Columbus, Ohio, did not comply with DoD Regulation 5200.2-R, "Personnel Security Program." The noncompliance occurred because DSDC follows Defense Logistics Agency Regulation 5200.11, "DLA Personnel Security Program," which did not contain the personnel security guidance in DoD Regulation 5200.2-R regarding ADP position classification, but is currently being updated. As a result, there was increased risk that uncleared application programmers could modify DoD information systems, including MOCAS, that routinely process sensitive information and large disbursements.

Criteria Regarding Personnel Security

DoD Regulation 5200.2-R. DoD Regulation 5200.2-R, "Personnel Security Program," February 23, 1996, defines personnel security policies and procedures. The regulation defines ADP-I, ADP-II and ADP-III positions and states that background investigations should be performed if the position involves the following:

> ...responsibility for the development and administration of agency computer security programs,...relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the ADP-I category,...[or] other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

DoD Regulation 5200.2-R also applies to consultants and contractor personnel. The regulation states "consultants and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (Appendix K)."

Defense Logistics Agency Regulation (DLAR) 5200.11. DLA Regulation 5200.11, "DLA Personnel Security Program," December 9, 1988, implements

DoD Directive 5200.2-R, "Personnel Security Program" and assigns responsibilities and establishes procedures for the conduct of personnel security operations for DLA. The regulation states "[ADP position] sensitivity will be designated according to the criteria in DoD 5200.2-R ... Refer to Appendix K for guidance on determining the sensitivity level of positions associated with Federal Computer Systems (ADP-I, ADP-II, and ADP-III positions)."

Defense Logistics Agency Regulation (DLAR) 5200.17. DLA Regulation 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," October 9, 1991, implements DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)" and identifies guidelines for determining personnel security position sensitivities of individuals involved in the design, operation, use, or maintenance of AIS software and hardware. This regulation advises that "contractor personnel requesting access to DLA systems are to be processed the same as DLA employees."

Designation of Programmer and Contractor Positions

DSDC Columbus employs approximately 110 MOCAS application programmers. Nationwide the DSDC employs an additional 230 application programmers involved in development and maintenance programming on the MOCAS system and several other accounting and information systems. The MOCAS system at DFAS Columbus Center disbursed about $67 billion in FY 1996.

DSDC Columbus follows the guidance in DLA Regulation 5200.11 concerning personnel security issues. This document states that Appendix K of DoD Directive 5200.2-R is to be referenced regarding position sensitivity for information systems personnel. The guidance in Appendix K states that personnel performing relatively high risk assignments associated with information systems which perform accounting tasks, disbursements, or authorizations for disbursement in amounts of $10 million or greater should be rated ADP-I. The disbursements from the MOCAS system at DFAS Columbus Center routinely exceeded the $10 million threshold. The application programmers at DSDC Columbus and the other DSDC operating locations perform relatively high risk assignments on information systems. DSDC Columbus has not classified these positions as ADP-I and, as a result, 340 application programmers are allowed to modify major DoD information systems, including MOCAS, without the proper access designations and without undergoing the required background investigations. Accordingly, the Commander, DSDC, should comply with the requirements in DLAR 5200.11 and assign the proper ADP ratings and obtain the required background investigations.

The DSDC Columbus uses contractor organizations in its application programming functions. Application programmers in these organizations are also subject to the sensitivity designations in DoD Regulation 5200.2-R. DLA Regulation 5200.17 cited previously advises "contractor personnel requesting access to DLA systems are to be processed the same as DLA employees." DSDC Columbus has not classified the programmers in contractor organizations as ADP-I which allows the contractor application programmers to modify major DoD information systems without having undergone the required background investigations. Accordingly, the Commander, DSDC, should comply with the requirements in DLAR 5200.17 by assigning the proper ADP ratings for critical-sensitive positions occupied by contractor personnel and by requiring background investigations.

Recommendations and Management Comments

B. We recommend that the Commander, Defense Logistics Agency Systems Design Center:

1. Designate the application programming positions at the Defense Logistics Agency Systems Design Center as critical-sensitive and obtain the required background investigations in compliance with DoD Regulation 5200.2-R and Defense Logistics Agency Regulation 5200.11.

2. Assign the required ADP ratings to contractor application programmers in critical-sensitive positions and require the contractor organizations to obtain the required background investigations in compliance with DoD Regulation 5200.2-R and DLA Regulation 5200.17.

Management Comments. The Director, Defense Logistics Agency, concurred. The Commander, Defense Logistics Agency Systems Design Center will be directed to prepare a plan to obtain background investigations of application programmers and appropriate contractor programmers. DLA plans to have the background investigations completed on or around August 31, 1998.

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

Use of Computer-Processed Data. We used standard utility programs and reports generated by commercial security software packages to achieve our objectives on general controls. To assess security privileges and access roles assigned to DFAS Columbus and DSDC personnel, we used data from two security software packages, Resource Access and Control Facility (RACF) and the Total Information Systems Extended Security System. RACF is a commercial security package marketed by International Business Machines (IBM) Corporation; Total Information Systems Extended Security System is a database security system for use with the SUPRA database system (marketed by Cincom Corporation). We had on-line, read-only access to the RACF security system, using special privileges intended for use by auditors. All system testing and use of audit software were done in a controlled environment with management's approval. Based on those tests, we concluded that the data were sufficiently reliable to meet the audit objectives and support our audit conclusions.

Audit Universe. We reviewed selected general and application controls related to the MOCAS system. At the DFAS Columbus Center, we reviewed access control and security administration of the MOCAS production system. At the DSDC, we reviewed access control of approximately 110 application programmers to the MOCAS developmental systems. We also reviewed software change management and contingency planning at the DSDC. We reviewed both organizations' compliance with the DoD management control program.

Audit Period and Standards. We performed this financial related audit from August 26, 1996, through March 21, 1997. The audit was performed in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD. We did not use statistical sampling procedures to conduct this audit. We included such tests of management controls as were considered necessary.

Contacts During the Audit. We visited or contacted individuals and organizations within the DoD. Further details are available on request.

Management Control Program

DoD Directive 5010.38, "Management Control Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of the Management Control Program. We reviewed management control procedures relating to access to MOCAS at DFAS Columbus. We reviewed the adequacy of the DFAS Columbus Annual Statement of Assurance for FY 1996 and the implementation of the DFAS Columbus management control program. We also reviewed the implementation of the DSDC management control program.

Adequacy of Management Controls. We identified material management control weaknesses, as defined by DoD Directive 5010.38, relating to access to MOCAS at DFAS Columbus. Weaknesses in access control to the MOCAS system threatened the integrity of the DFAS Columbus contract and payment data. Recommendations A.1. and A.2., if implemented, will correct these weaknesses. A copy of this report will be provided to the senior management control officials at DFAS Columbus.

Adequacy of the DFAS Columbus Self-Evaluation. The DFAS Columbus self-evaluation for FY 1996 reported that material weaknesses in access control to MOCAS had been determined on September 30, 1994. A corrective action plan was implemented by management, and the control weakness was considered closed on September 13, 1996. We consider management's actions to be premature because the root cause of the weakness had not been corrected. As of the date of management's closure of the material weakness, the TASO guidance had not been issued.

Appendix B. Summary of Prior Coverage

We identified five prior Inspector General, DoD, reports relating to this audit.

Inspector General, DoD

Inspector General, DoD, Report No. 96-124, "Selected General Controls Over the Defense Business Management System," issued on May 21, 1996, states that the Defense Business Management System development environment had several security deficiencies. In addition, the Defense Finance and Accounting Service Financial Systems Organization did not adequately control program software changes to ensure that only authorized changes were made, and the Defense Megacenter, Columbus, Ohio, and the Defense Logistics Agency Systems Design Center, Columbus, Ohio, were not adequately prepared to react in the event of a disaster. The report recommended that the Defense Finance and Accounting Service Financial Systems Organization strengthen access controls to properly secure the development system for the Defense Business Management System; improve procedures used to control the software change authorization process; and review selected portions of the existing software code based on the risk of compromise. The report also recommended that the Defense Megacenter, Columbus, Ohio, and the Defense Logistics Agency Systems Design Center develop, finalize, and test a disaster recovery plan. The Defense Finance and Accounting Service concurred with the recommendations for computer security; software change management practices, and disaster preparedness. The Defense Megacenter, Columbus, Ohio, concurred with the recommendations to complete, finalize, and test the disaster recovery plan. The Defense Logistics Agency agreed to update their disaster recovery plan but chose to wait for the new location of their computer lab to be determined before performing a disaster recovery risk analysis. Testing of the plan will depend upon the disaster recovery risk analysis for the location of the test facility.

Inspector General, DoD, Report No. 95-280, "Management Control Program at Defense Information Systems Agency, Western Hemisphere," issued on July 26, 1995, states that the Defense Information Systems Agency, Western Hemisphere, and DFAS did not adequately review accounting system controls. The report recommended that the two organizations coordinate annual reviews of accounting system controls, to include specifying responsibilities for the DFAS system manager and system users at the Defense Information Systems Agency, Western Hemisphere; train system managers and users in performing annual reviews of accounting system controls; and document the controls during the reviews. The DFAS nonconcurred with the recommendation to coordinate reviews but provided acceptable alternative actions. DFAS generally concurred with the other recommendations and completed the corrective actions.

Inspector General, DoD, Report No. 95-046, "Data Input Controls for the Mechanization of Contract Administration Services System," issued on November 30, 1994, states that MOCAS controls over automated data input were not adequate. Specifically, MOCAS accepted invalid data in 57 of the 484 automated input fields tested, and edit tables available from the Military Departments, which could significantly improve the accuracy of MOCAS data, were not being used. As a result, negative unliquidated obligations, unmatched disbursements, and incorrect or duplicate payments could occur. Also, data rejected at initial input were not properly managed, corrected, and reentered in a timely manner, and access controls were not adequate to prevent unauthorized access to the MOCAS system. The report recommended the use of the Military Departments' edit and validation tables in MOCAS as controls over data accuracy and automated controls for the data input fields that accepted invalid data. The report also recommended issuing guidance concerning MOCAS reject listings, updating desk procedures for handling automated reject listings, increasing supervisory reviews, and implementing controls to ensure that user identifications are promptly canceled when no longer needed. The Deputy Comptroller (Financial Systems), responding to recommendations made to the DFAS, concurred with the need to issue guidance concerning MOCAS reject listings, updating desk procedures for handling automated reject listings, increasing supervisory reviews, and implementing controls to ensure that user identifications are promptly canceled when no longer needed. The Deputy Comptroller (Financial Systems) partially concurred with the three other recommendations.

Inspector General, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," issued on March 18, 1994, states that the DBMS users neglected to change their passwords within 180 days. In addition, numerous users had not changed their passwords in over 1 year. This occurred because security personnel did not periodically review the passwords or deny access to users whose passwords had not been changed in 180 days. The report recommended that employees be automatically required to change their passwords every 90 days. The Defense Information Services Organization concurred with the recommendation.

Inspector General, DoD, Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," issued on June 30, 1993, states that authorized program facility libraries and programs were not adequately monitored and controlled. In addition, the Defense Logistics Agency Systems Automation Center, the Defense Information Technology Services Organization-Dayton, and the Defense Information Technology Services Organization-Columbus had improperly implemented the features of RACF security software. Read and update access to RACF datasets were not limited to the system programmers responsible for maintenance. Security management for the tape management system had not been installed. Started tasks had update access to all authorized program facility datasets in order to keep the system running. In addition, management relied on system users to control the lengths of passwords. The Job Entry Subsystem 2 log-on identification and security option for password checking was not installed at the

Defense Information Technology Services Organization-Dayton, or the Defense Information Technology Services Organization-Columbus. The report recommended that DFAS periodically review the authorized program facility, limit access to the RACF utility to personnel who had a clearly defined need, and review the Job Entry Subsystem 2. Management concurred with the recommendations and agreed to take corrective action.

Appendix C. MOCAS Data Tables Reviewed

We reviewed the current assignments of personnel who had access to the following tables to determine whether their access was justified based on duty requirements.

Contract Input Supervisory Table (Table Name 9720). Update access to this table should be limited to supervisory personnel only. We found that several nonsupervisory employees had update access to this table.

Line Item Schedule Summary Report (LISSR) Supervisory Table (Table Name 9728). Update access to this table should be limited to supervisory personnel only. We found that several nonsupervisory employees had update access to this table.

Contract Research Supervisory Table (Table Name 9730). Update access to this table should be limited to supervisory personnel only. We found that several nonsupervisory employees had update access to this table.

Contractor Remit-To Address Table (Table Name 9723). Update access to this table should be limited to contract control clerks. We found that several employees who were not contract control clerks had update access to this table.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Assistant Secretary of Defense (Public Affairs)

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

Office of Management and Budget
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on National Security
House Committee on Government Reform and Oversight
House Subcommittee on Government Management Information and Technology, Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security

Part III - Management Comments

Under Secretary of Defense (Comptroller) Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100

COMPTROLLER

JUL 11 1997

MEMORANDUM FOR ACTING DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE, OFFICE OF THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Draft Audit Report on the General Application Controls Over the Mechanization of Contract Administration Services System (Project No. 6FG-0083.00)

In light of the fact that there are no accounting or financial management policy issues involved in the subject draft report, this office will not submit comments. This office has notified the Defense Finance and Accounting Service and the Defense Logistics Agency that they are to respond directly to your request for comments (copy attached).

The staff point of contact for this issue is Mr. Henry Bezold. He may be reached by e-mail at bezoldh@ousdc.osd.mil or by phone at (703) 614-3523.

Nelson Toye
Deputy Chief Financial Officer

Attachment

*Attachment same as cover letter.

Defense Finance and Accounting Service Comments

DFB 9/18

DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

SEP - 9 1997

DFAS-HQ/FCC

MEMORANDUM FOR DEPUTY DIRECTOR FOR AUDIT FOLLOW-UP, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: DoDIG Draft Report, "Audit of General and Application Controls Over the Mechanization of Contract Administration Services System," dated June 23, 1997 (Project No. 6FG-0083.00)

In response to your memorandum of June 23, 1997, the Defense Finance and Accounting Service has provided the attached comments on recommendations 1 and 2.

Our point of contact is Mr. Jack Foust. He can be reached at (703) 607-5030.

for Roger W. Scearce
Brigadier General, USA
Deputy Director for Finance

Attachment:
As stated

Defense Finance and Accounting Service
Comments on Information Requested by DoDIG for
Audit Report on General and Application Controls over the
Mechanization of Contract Administration Services System
(Project No. 6FG-0083.00)

Recommendation A.1: We recommend that the Director, Defense Finance and Accounting Service-Columbus Center (DFAS-CO) issue the desk procedure for the Terminal Area Security Officers (TASOs) and train all TASOs in its use within 90 days of issuance.

DFAS Response: Concur The TASO desk procedure has been issued in draft form for comments. Estimated completion date for final copy and training is November 15, 1997. TASOs have been instructed to operate under the draft desk procedures until the final copy is issued.

Recommendation A.2.a: We recommend that the Director, DFAS-CO direct the TASOs to periodically review the "Total Information System Extended Security System Batch Utilities Application to User Relationship Report (TIS Report)" for all supervisory files and other sensitive files in the Mechanization of Contract Administration Services System.

DFAS Response: Concur The draft TASO desk procedure requires the TASOs to conduct a review of the TIS Report on a semi-annual basis. Action complete.

Recommendation A.2.b: We recommend that the Director, DFAS-CO terminate user Ids that are no longer required by the employee's position and access to files that is no longer required by the employee's position.

DFAS Response: Concur A complete review and deletion of all unauthorized access to the supervisory tables previously reviewed by the DoDIG is being finalized. A complete 100 percent review of all systems will be completed no later than December 31, 1997.

Defense Logistics Agency Comments

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD, SUITE 2533
FT. BELVOIR, VIRGINIA 22060-6221

IN REPLY REFER TO DDAI

03 SEP 1997

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
DEPARTMENT OF DEFENSE

SUBJECT: Draft Report: General and Application Controls Over the Mechanization of Contract Administration Services System (Project No. 6FG-0083.00)

This is in response to the June 23, 1997 request. If you have any questions, please contact Mrs. LaVaeda Coulter, (703) 767-6261.

Encl

JEFFREY GOLDSTEIN
Chief (Acting), Internal Review

Federal Recycling Program Printed on Recycled Paper

AUDIT TITLE: Audit of General and Application Controls Over the Mechanization of Contract Administration Services System. 6FG-0083.00

RECOMMENDATION B: We recommend that the Commander, Defense Logistics Agency Systems Design Center:

1. Designate the application programming positions at the DSDC as critical-sensitive and obtain the required background investigations in compliance with DoD Regulation 5200.2-R and DLAR 5200.11.

2. Assign the required ADP ratings to contractor application programmers in critical-sensitive positions and require the contractor organizations to obtain the required background investigations in compliance with DoD Regulation 5200.2-R and DLA Regulation 5200.17.

DLA COMMENTS: Concur. The Chief Information Officer will direct the DSDC Commander to prepare a plan to obtain background investigations of application programmers and appropriate contractor programmers. When DoD Regulation 5200.2-R, DLA Regulation 5200.11, and DLA Regulation 5200.17 are revised and released, the plans will be reevaluated based on new guidance.

DISPOSITION: Action is Ongoing. ECD: 31 Aug 98

ACTION OFFICER: Ms. Mickey Slater, CANP, 767-2171
PSE APPROVAL: Mr. Thomas J. Knapp, CAN, 767-3100
COORDINATION: Mr. Patrick McCarthy, CANP, 767-2131
Mrs. LaVaeda Coulter, DDAI, 767-6261

DLA APPROVAL: 9/3/97
DDAI

Audit Team Members

This report was produced by the Finance and Accounting Directorate, Office of the Assistant Inspector general for Auditing, DoD.

F. Jay Lane
Christian Hendricks
Carl F. Zielke
John E. Byrd
Steven L. Johnson
Geoffrey L. Weber
Traci Y. Sadler