Audit Report

OFFICE OF THE INSPECTOR GENERAL

SELECTED GENERAL CONTROLS OVER THE DEFENSE BUSINESS MANAGEMENT SYSTEM

Report No. 96-124 May 21, 1996

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 of the 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 the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DBMS	Defense Business Management System
DBOF	Defense Business Operations Fund
DFAS	Defense Finance and Accounting Service
DMC	Defense Megacenter
DSDC	Defense Logistics Agency Systems Design Center
FSA	Financial Systems Activity
FSO	Financial Systems Organization
IG	Inspector General
ISSO	Information System Security Officer
RACF	Resource Access Control Facility

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

May 21, 1996

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Audit Report on Selected General Controls Over the Defense Business Management System (Report No. 96-124)

We are providing this final report for review and comments. We made this audit in support of audits of the FY 1995 Defense Business Operations Fund financial statements. We will address application controls in a subsequent report. We considered comments on a draft of this report in preparing the final.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We received comments from the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency. Management concurred with all recommendations except two. We request that the Defense Finance and Accounting Service provide additional comments on revised Recommendation B.4. and that the Defense Logistics Agency provide additional comments on Recommendation C.2.c. by July 22, 1996.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Christian Hendricks, Audit Program Director, at (703) 604-9138 (DSN 664-9138), or Ms. Victoria C. Hara, Audit Project Manager, at (703) 604-9152 (DSN 664-9152). See Appendix E for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 96-124 **May 21, 1996**
(Project No. 5FG-2007.01)

Selected General Controls Over the Defense Business Management System

Executive Summary

Introduction. This report addresses selected general controls and issues related to the Defense Business Management System. A second report will address selected application controls. We made this audit in support of audits of the FY 1995 Defense Business Operations Fund financial statements. The Defense Business Management System performs appropriation accounting, cost accounting, personnel, payroll, manpower, and management information functions for the Navy, the Air Force, five Defense agencies, and six DBOF business areas. It also processes payroll for the Executive Office of the President.

Audit Objectives. The overall audit objectives were to determine the adequacy of the following for the Defense Business Management System:

o selected general and application controls,

o implementation of the DoD management control program,

o compliance with Title 2 of the General Accounting Office "Policies and Procedures Manual for Guidance of Federal Agencies," and

o compliance with the Joint Financial Management Improvement Program "Core Financial System Requirements."

Audit Results. Computer security at the Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio, did not adequately protect the Defense Business Management System development code from compromise. The Defense Finance and Accounting Service had previously identified general control weaknesses. Weaknesses remained unresolved in access control and security administration (Finding A). The Financial Systems Activity did not adequately control program software changes to ensure that only authorized changes were made (Finding B). In addition, 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 (Finding C). These general control weaknesses compromised the reliability of the Defense Business Operations Fund financial statements. These weaknesses also increased the risk of fraud, sabotage, and disruption to the operations of the DoD Components that rely on the Defense Business Management System.

The recommendations in this report will improve security and change control procedures over the development of the Defense Business Management System. The recommendations will also help to minimize the impact of a catastrophe over the operations of the Defense Megacenter Columbus, the Defense Logistics Agency Systems Design Center, and users of the Defense Business Management System.

Management is aware that improvements are needed to comply with Title 2 of the General Accounting Office "Policy and Procedures Manual for Guidance of Federal Agency" and the Joint Financial Management Improvement Program "Core Financial System Requirements." Because management is working to improve these areas, we are not making recommendations in this report. Appendix C provides details on our assessment of Defense Business Management System core requirements.

Summary of Recommendations. We recommend that the Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio, 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. We also recommend that the Defense Information Systems Agency, Defense Megacenter, and the Defense Logistics Agency Systems Design Center, both at Columbus, Ohio, develop, finalize, and test a disaster recovery plan. See Part I for details on management comments and Part III for the complete texts of the comments.

Management Comments. The Defense Finance and Accounting Service concurred with recommendations for computer security; software change management practices, except for a review of the existing software code; and disaster preparedness. The Defense Information Systems Agency 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 wish to wait for the determination of their new location for the computer lab before performing a disaster recovery risk analysis. Defense Logistics Agency nonconcurred with periodic testing of their disaster recovery plan.

Audit Response. Ongoing weaknesses in computer security and change management at the Financial Systems Activity Columbus provided programmers the opportunity to insert software routines to bypass application level security. Unless the current Defense Business Management System code is reviewed to verify that it does not contain this type of compromise, the Defense Finance and Accounting Service cannot be sure that application level security was not compromised. We revised our recommendation to perform a review of selected portions of the existing software code based on the risk of compromise.

Without testing, the Defense Logistics Agency Systems Design Center cannot be sure that their disaster recovery plan will limit lost productivity in the event of a catastrophe. Testing the plan does not imply that the Systems Design Center needs to reconstitute their operations at an alternate site. A test plan should be developed based on a risk assessment to address the most likely disaster conditions and how they should be responded to. Testing can also be done on a cost-effective modular basis to minimize cost and disruption. Virtually all of the individuals employed by the Systems Design Center depend on the availability of their computer system for day-to-day productivity. Further, periodic testing of disaster recovery plans is required by Government regulations.

We request that the Defense Finance and Accounting Service and the Defense Logistics Agency reconsider their positions and provide additional comments by July 22, 1996.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objectives 3
Finding A. Computer Security at FSA Columbus 4
Finding B. Software Change Management 15
Finding C. Disaster Preparedness 20

Part II - Additional Information

Appendix A. Scope and Methodology
Scope 28
Methodology 28
Management Control Program 29
Appendix B. Prior Audits and Other Reviews 30
Appendix C. DBMS Project Manager and Core Financial System Requirements 32
Appendix D. Organizations Visited or Contacted 33
Appendix E. Report Distribution 34

Part III - Management Comments

Defense Finance and Accounting Service Comments 38
Defense Information Systems Agency Comments 47
Defense Logistics Agency Comments 50

Part I - Audit Results

Audit Background

Defense Business Management System. The Defense Logistics Agency developed a multifunctional management system, now known as the Defense Business Management System (DBMS), in 1969 and 1970. Since then, the system software and technical components have been extensively upgraded. In December 1994, the Under Secretary of Defense (Comptroller) chose the DBMS as the interim migratory system for seven business areas of the Defense Business Operations Fund (DBOF). On July 10, 1995, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) announced that the DBMS had been selected as a migratory system for the finance business area.

The DBMS performs appropriation accounting, cost accounting, personnel, payroll, manpower, and management information functions for the Navy, the Air Force, five Defense agencies, and six DBOF business areas. It also processes payroll for the Executive Office of the President. The DBMS interfaces with other automated systems, including the Base Operations Support System, the Computerized Accounts Payable System, and the Standard Finance System Redesign. The DBMS supports over 40,000 on-line functional users and accounts for about $8.5 billion in DBOF funds.

Responsible Organizations. The Defense Finance and Accounting Service (DFAS) is the DBMS functional proponent and administers the system. The DFAS Columbus Center, Columbus, Ohio, and Defense agencies process DBMS data on computers at the Defense Megacenter, Columbus, Ohio, (DMC Columbus).

The DMC Columbus has an interservice agreement with the 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 the DBMS and for six other DoD financial and logistics information systems. Computers at DMC Columbus process payroll for DoD civilian and military employees and the Executive Office of the President. They also process DoD orders and payments for goods and services.

The DFAS Financial Systems Activity, Columbus, Ohio (FSA Columbus), is the central design activity for the DBMS. The FSA Columbus reports to the DFAS Financial Systems Organization (FSO), Indianapolis, Indiana.

The Defense Logistics Agency System Design Center (DSDC), Columbus, Ohio, has an interservice agreement with the FSA Columbus to provide software development, engineering support, and computer processing. The DSDC does emergency planning, maintains and updates the DSDC emergency notification chart, periodically tests the emergency notification system, and backs up files and programs to ensure continuity of operations.

Development and Production Systems. A development system consists of computers and related software used for developing applications such as the DBMS. The FSA Columbus uses a development system to design and test modifications to the DBMS before the modifications are incorporated into the production system. The production system is used to process the daily work of an organization. The separation of the development and production systems eliminates errors in the application program before the application program is used to process data.

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:

o organization and management controls such as planning, policies, and procedures;

o development controls, including change management; and

o operations controls such as physical and logical security.

Audit Objectives

The audit objectives were to determine the adequacy of the following for the DBMS:

o selected general and application controls,

o implementation of the DoD management control program,

o compliance with Title 2 of the General Accounting Office "Policies and Procedures Manual for Guidance of Federal Agencies," and

o compliance with the Joint Financial Management Improvement Program "Core Financial System Requirements."

A subsequent audit report will address application controls. All other objectives are addressed in this report.

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 coverage related to the audit objectives. Appendix C discusses the designation of a DBMS project manager and compliance with core financial system requirements.

Finding A. Computer Security at FSA Columbus

Computer security at FSA Columbus did not adequately protect the DBMS development code from compromise. Weaknesses existed in access control and security administration because the FSA Columbus:

o did not adequately control access to critical DBMS development libraries or security software attributes, and

o did not consistently administer system security to effectively control user accesses.

As a result, as many as 395 users at FSA Columbus could improperly access, modify, or destroy the DBMS development programs without risk of detection. These general control weaknesses compromised the integrity of a critical payroll and accounting system and the reliability of DBOF financial statements.

Access Control

Effective access control is the system of internal controls used by an organization to protect computer resources (including hardware, software, and data) from unauthorized use, modification, or destruction. The FSA Columbus uses its computer system to develop and test the DBMS application software and other software. Security administration is a system of manual controls that prevents access control from deteriorating as a result of organizational and administrative changes.

Resource Access Control Facility (RACF) security software aids in access control and system security. To protect data, RACF verifies the identities of users entering the system. RACF restricts user access to protected system resources and gives authorized users limited access to protected resources. RACF also maintains logs and generates reports on security-related events. At the FSA Columbus, the Information System Security Officer (ISSO) maintains the RACF security software settings.

Computer Security

The FSA Columbus did not adequately protect the DBMS development programming code from compromise. Weaknesses existed in access control and security administration.

Access Control. Access control for the DBMS development system was not adequate. FSA Columbus management did not restrict access to the computer and sensitive data files to personnel who needed access and who had received the required background checks. We identified weaknesses in access to software libraries and in the implementation of several features of the RACF security system.

Software Library Access. The FSA Columbus did not adequately limit access that could have allowed users to update critical DBMS development libraries. To limit access, computer programs are organized into logical groups called libraries. The FSA Columbus granted 395 (66 percent) of 603 users update or higher access to sensitive DBMS development and testing libraries. Similar organizations restrict this type of access to one or more individuals with software librarian duties. Because the FSA Columbus did not adequately limit access to DBMS development and testing libraries, users could:

- make unauthorized changes to the DBMS,
- modify, destroy, or corrupt DBMS application programs, or
- insert unauthorized code to compromise DBMS application-level security routines.

Since June 30, 1995, FSA Columbus has limited the number of individuals with access to these developmental libraries and eliminated any unauthorized access. On December 15, 1995, FSA Columbus implemented procedures that should prevent unauthorized changes to the DBMS in the future.

Security System Implementation. The FSA Columbus did not effectively implement the RACF security system to adequately control user access to the DBMS development system. The FSA Columbus did not effectively implement the RACF special attribute, operations attribute, revoke-date feature, and protect-all option.

RACF Special Attribute. The FSA Columbus did not limit the use of the RACF special attribute to the ISSO. The FSA Columbus granted the special attribute to the ISSO and two other employees, although the two employees did not need it for their work.

The special attribute allows virtually unlimited access to the system and gives users the ability to establish accounts, turn off logging of security-related incidents and other security features, and change information in the system without being detected. The special attribute should be granted only to individuals who are responsible for implementing RACF security rules.

FSO Policy TS-02, "Security Classifications for ADP Positions," May 18, 1994, requires system administrators to receive background investigations. The FSA Columbus did not ensure that all three employees who had been granted the RACF special attribute received the required background investigations.

Only one of the three employees with security administrator privileges had received a background investigation. The employee with the appropriate background investigation was not the ISSO.

By December 1995, the FSA Columbus had limited the use of the RACF special attribute to the ISSO. They had also ensured that the ISSO received a background investigation.

RACF Operations Attribute. FSA Columbus did not limit the use of the RACF operations attribute to users who maintained system libraries. The operations attribute allows users to copy or catalog a library, delete resources protected by the security software, or bypass security software protection. The FSA Columbus assigned the operations attribute to four users and three started tasks on the DBMS development system.

A started task is a program that runs while the system is being loaded and continues to run in the background on the mainframe computer system. Started tasks can perform various functions, but are normally limited to system utility functions. Started tasks are invoked either through a program call or an operator call. Without proper control, started tasks, although usually necessary, present a security risk to mainframe computers because they run continuously and numerous users can access them.

Of the four users assigned the RACF operations attribute, only one user had a valid need. One user had retired in August 1994, but his access had not been canceled. The FSA Columbus had granted temporary access to a second user in August 1993 for a testing project and had not canceled the access. FSA Columbus could not identify the third user. By November 1995, FSA Columbus eliminated all employees' access to the RACF operations attribute.

The FSA Columbus agreed that at least one of the three started tasks did not require the RACF operations attribute. FSA Columbus could not provide documentation or a rationale for the other two started tasks that possessed this sensitive attribute.

In a memorandum dated December 18, 1995, FSA Columbus management stated that they had eliminated RACF operations access for all but one started task. Management stated that this started task was the only one that required the operations attribute to function properly.

RACF Revoke-Date Feature. The FSA Columbus did not use the RACF revoke-date feature to control individuals who needed temporary accounts. The revoke-data feature allows the security administrator to specify a date when the account will cease to function. As part of the systems development and testing process, the FSA Columbus frequently allowed user activities, testing personnel, or contracting personnel to access the DBMS on a temporary basis. The RACF revoke-date feature allows temporary accounts to expire automatically when the testing period is over. Although this feature was

available, none of the 954 accounts maintained by the RACF security software were protected. In its memorandum of December 18, 1995, FSA Columbus management stated that they were using the revoke-date feature to control temporary users.

In addition, the FSA Columbus did not use the RACF revoke-date feature to enforce password control policies. The FSA Columbus delivers passwords for new accounts to users through interoffice mail. To prevent password compromise, the ISSO should require the user to complete and return a receipt when the password has been received. According to internal FSA Columbus procedures, if the user does not return the signed receipt within 7 days, the ISSO should revoke the account. The ISSO was not enforcing this procedure, which could help to protect the DBMS development system. Use of the revoke-date feature would enforce this procedure automatically.

In its memorandum of December 18, 1995, FSA Columbus management stated that they had begun using the RACF revoke-date feature and had implemented additional controls to aid in enforcing password control policies.

RACF Protect-All Option. The FSA Columbus did not implement all RACF features necessary to ensure the C2 security classification required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988 (DoD Directive 5200.28). DoD Directive 5200.28 requires mandatory, minimum security measures for automated information systems and requires a C2 security classification for systems that process sensitive unclassified information, such as the payroll software processed by FSA Columbus.

The C2 classification requires system resources to be isolated and users to be individually accountable through log-on procedures that identify each user. A C2 classification requires all computer libraries to be protected from access unless the individual has a need to know.

The RACF protect-all option automatically protects each new library created. If the ISSO does not use the protect-all option, the ISSO must create or assign rule profiles for each newly created library. Otherwise, the library is unprotected.

The DBMS development system did not meet the C2 security requirements of DoD Directive 5200.28 because the FSA Columbus did not activate the RACF protect-all option. By not activating this option, FSA Columbus increased the risk that sensitive libraries could be created without appropriate access protection.

The FSA Columbus had not activated the RACF protect-all option, although an August 30, 1994, DFAS internal audit had recommended that the RACF software package be implemented at the C2 level. The DFAS directed FSA Columbus to complete corrective action by April 1995. FSA Columbus managers agreed and stated that the RACF software package would be implemented at the C2 level by February 1995.

In July 1995, we informed the FSA Columbus managers that RACF software should be implemented at the C2 level. FSA Columbus managers again agreed to take corrective action. In November 1995, 9 months after the agreed-upon date of February 1995, FSA Columbus still had not implemented the RACF software package at the C2 level.

In its memorandum of December 18, 1995, FSA Columbus management stated that they had implemented the RACF protect-all option in warning mode prior to full implementation. Warning mode allows evaluation of the feature's effect on the system without disruption of processing. FSA Columbus stated that full implementation of the protect-all option was scheduled for early 1996.

Security Administration. The FSA Columbus did not effectively administer security for the DBMS development system. As a result, FSA Columbus did not maintain control over access to the system. Effective security administration ensures that organizational and personnel changes do not degrade existing access controls.

The FSA Columbus did not have adequate control over access to the DBMS development system because managers did not:

- o develop an access control policy based on identified vulnerabilities,
- o effectively control system access authorizations,
- o periodically review and revalidate user access,
- o classify positions and conduct appropriate background investigations,
- o provide regular training in security awareness, and
- o protect personal computers from potential compromise of the DBMS.

Access Control Policy. The FSA Columbus does not have a written policy or plan for access control based on identified vulnerabilities. DoD Directive 5200.28 states that, at a minimum:

> There shall be in place an access control policy for each [automated information system]. It shall include features and/or procedures to enforce the access control policy of the information within the [system]. . . . The Information System Security Officer shall . . . [e]valuate known vulnerabilities to ascertain if additional safeguards are needed [and] [m]aintain a plan for system security improvements and progress.

The FSA Columbus contracted with the DSDC to conduct a vulnerability analysis on December 1, 1994, which addressed the DBMS as a whole. However, the vulnerability analysis did not address the specific risks inherent in the development system at the FSA Columbus.

The FSA Columbus issued two internal security instructions, SEC.3005, "Automated Information System Security Policy," November 30, 1995, and

SEC.3007, "Internal Procedure on System Access," November 29, 1995. Although not based on specific vulnerabilities identified during a risk analysis, these instructions define responsibilities for security and access control at FSA Columbus.

System Access Authorizations. The ISSO could not demonstrate that access to sensitive development system libraries was based on written and approved requests. The ISSO also changed user authorizations based on telephone calls or electronic mail. In addition, records of approved authorizations were not reviewed and were not kept up-to-date. As a result, the ISSO lost control over access to the development system.

We judgmentally selected 30 out of 603 user accounts maintained at the FSA Columbus. We reviewed documentation maintained by the ISSO. The documentation did not support the access levels granted to the 30 selected user accounts. The documentation did not list group assignments or access that individuals should have to specific resources. Also, the ISSO could not locate written documentation for 10 of the 30 user accounts.

In its memorandum of December 18, 1995, FSA Columbus management stated that they had implemented internal security instructions to control system access authorizations (SEC.3007, "Internal Procedure on System Access," November 29, 1995). Prior to November 29, 1995, FSA Columbus did not have written instructions to control system access.

System Access Review and Revalidation. The FSA Columbus did not periodically review and revalidate user accounts to identify users who had retired or left the organization or whose need for access had changed. Informal procedures required the Terminal Area Security Officers to forward the names of departing employees to the ISSO for removal from the system.

The FSA Columbus provided us with a list of 46 employees who had left the organization after January 1, 1993. As of May 1995, 3 of the 46 employees continued to have access to the DBMS development system, which would enable them to alter or destroy critical program information without authorization.

In addition, the FSA Columbus did not delete access to the DBMS development system for 59 accounts that no longer required access. These 59 individuals could alter or destroy critical-sensitive files without proper authorization. The FSA Columbus also could not identify 228 other accounts; these accounts could access the DBMS development system, but were not authorized to access sensitive libraries.

In its memorandum of December 18, 1995, FSA Columbus management stated that a full review and revalidation of system access had been completed, and that the ISSO was conducting random audits of system access to ensure continued integrity.

Position Classifications and Background Investigations. The FSA Columbus did not designate positions with critical-sensitive access as ADP-I, and did not require background investigations as directed by FSO Policy TS-02, "Security Classifications for ADP Positions," May 18, 1994.

DoD Regulation 5200.2-R, "Personnel Security Program," July 14, 1993, defines personnel security policies and procedures. The regulation defines ADP-I positions and states that background investigations should be performed if the position involves the following:

> [r]esponsibility 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 dollar amounts of $10 million per year or greater, . . . [or] other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

FSO Policy TS-02, "Security Classifications for ADP Positions," May 18, 1994, states:

> Application programmers will be required to have Critical Sensitive [ADP-I] classifications if the nature of their work is such that they can modify or update programs and/or files which are part of a pay or disbursement system that handles dollar amounts in excess of 10 million dollars per year, in such a manner that they could achieve personal gain.

The FSA Columbus had informally designated a programmer as the ISSO, but did not designate the position as ADP-I or obtain the required background investigation. In addition, FSA Columbus did not include the ISSO duties in the programmers' performance standards.

In its memorandum of December 18, 1995, FSA Columbus management stated that the ISSO position had been designated critical-sensitive, that the incumbent had received the appropriate background investigation, and that the duties of security officer had been included in the incumbent's performance standards.

FSO Policy TS-02 also states that application programmers are not required to have the critical-sensitive classification if their work is subject to technical review by an individual with a critical-sensitive [ADP-I] classification.

The FSA Columbus granted 395 user accounts the ability to change the DBMS code during the development process. However, FSA Columbus designated only 82 FSA Columbus employees as critical-sensitive. This allowed 313 (79 percent) user accounts of individuals who had not received proper background investigations to access the DBMS development system. FSA Columbus did not require supervisors to review DBMS software changes performed by individuals without background investigations.

FSA Columbus issued internal instruction SEC.3001.1, "Software Security," on December 15, 1995. This procedure requires technical review of all software code changes by personnel in positions designated ADP-I to ensure that only authorized changes have been made.

The FSA Columbus did not review all positions to ensure that position descriptions and clearances were updated as required, although an August 30, 1994, DFAS internal audit had recommended the review. DFAS directed FSA Columbus to complete corrective action by April 1995. The FSA Columbus agreed and stated that they would review the guidelines for determining position classifications by February 1995. In July 1995, we informed FSA Columbus that employees' position descriptions and clearances still had not been updated. FSA Columbus again agreed to take corrective action. In November 1995, we briefed the FSA Columbus again about the same problem; 16 months after they knew the problem existed, FSA Columbus managers still had not reviewed all position descriptions and clearances.

FSA Columbus issued internal security instruction SEC.3003, "Security Classifications for ADP Positions," on November 29, 1995. This instruction requires that all FSA Columbus positions be reviewed and designated as ADP-I, ADP-II, or ADP-III.

Security Awareness Training. The FSA Columbus did not provide periodic security awareness training, as required by DoD Directive 5200.28. DoD Directive 5200.28 requires the ISSO to ensure that system users are familiar with internal security practices.

The FSA Columbus did not provide security awareness training for all employees, although an August 30, 1994, DFAS internal audit had recommended security awareness training. DFAS directed the FSA Columbus to provide security awareness training no later than April 1995. FSA Columbus managers agreed and stated that the security awareness training would be completed by February 1995.

Managers at FSA Columbus said they had made informal plans to implement security awareness training. However, at the time of our audit, FSA Columbus was not conducting any security awareness training. In July 1995, we discussed this matter with FSA Columbus managers, and they again agreed that periodic security awareness training was needed. They stated that they would draft and implement a security plan, which would include periodic security awareness training. In November 1995, we again briefed FSA Columbus managers on the lack of security awareness training. The FSA Columbus still had not provided security awareness training, 9 months after FSA Columbus managers told the FSO that security awareness training would be completed.

On November 29, 1995, FSA Columbus issued internal instruction SEC.3008, "Security Awareness Training." This instruction requires initial and periodic security awareness training for all employees and contractors. On December 18, 1995, FSA Columbus management stated that they had recently conducted formal security awareness training for all employees.

Personal Computer Security. The FSA Columbus did not protect personal computers from unauthorized use, as required by DoD Directive 7920.5, "Management of End-User Computing (EUC)," March 1, 1989. This Directive states that standards for general-purpose computers, including security, shall be applied to personal computers. Because personal computers used as terminals were not protected, they could be used to compromise system security.

Because FSA Columbus uses personal computers rather than dumb terminals (terminals lacking their own central processing units and disk drives) for mainframe access, the risk of compromising individual passwords is increased. Unauthorized programs that monitor terminal sessions and capture the password of an authorized user can be placed on unprotected personal computers. The unauthorized user can then retrieve the password and use it to compromise a mainframe computer's security. Currently, the only protections against this type of compromise are security education and a policy requiring hardware passwords for personal computers. In its memorandum of December 18, 1995, FSA Columbus management stated that a study was being conducted jointly with the FSO to determine additional methods of preventing this type of system compromise.

FSA Management's Commitment to Security

Management at FSA Columbus needs to show a strong commitment to implementing policies and correcting known security weaknesses in order to protect the DBMS development system from compromise. An August 30, 1994, DFAS internal audit identified weaknesses in access control and security administration at FSA Columbus. FSA Columbus agreed to take corrective action, but failed to do so.

In July 1995, we informed FSA Columbus of the security weaknesses identified during our audit. FSA Columbus again agreed to take corrective action. In November 1995, we again briefed the FSA Columbus on the unresolved security weaknesses we had identified. Although FSA Columbus managers knew that computer security needed improvement and had agreed to correct the weaknesses, they did not take corrective action.

Conclusion

By not recognizing the need to properly secure the DBMS development system, FSA Columbus managers did not properly protect the integrity of a critical payroll and logistics system that accounts for $8.5 billion annually in DBOF funds. Individuals who were not associated with FSA Columbus and who did not have software programming duties could change the DBMS software during its development. Programmers could insert unauthorized software routines into

the DBMS, possibly compromising the security of the production system. The weaknesses in access controls are management control weaknesses that compromise the reliability of the DBOF financial statements. These weaknesses also increase the risk of fraud, sabotage, and disruption to the operations of the DoD Components that rely on the DBMS.

Recommendations, Management Comments, and Audit Response

A.1. We recommend that the Director, Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio:

a. Review all user access for the Defense Business Management System development system and restrict access to the computer and sensitive files to personnel who need access and for whom the required background investigations have been completed.

b. Limit access to the Resource Access Control Facility special attribute to the Information System Security Officer, who has had a background investigation and does not have programming responsibilities.

c. Limit access to the Resource Access Control Facility operations attribute to:

(1) Individuals with library management responsibilities who have had background investigations, and

(2) Started tasks with an identified need for this attribute.

d. Use the Resource Access Control Facility revoke-date feature to control temporary accounts and enforce receipts for passwords.

e. Activate the Resource Access Control Facility protect-all option required for a C2 security rating on the Defense Business Management System development system, or obtain a waiver of C2 security requirements from the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), as established in DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988.

f. Develop and implement a formal, written policy for access control; the policy should include enforcement procedures and a plan for continuously improving system security.

g. Develop and implement written procedures that require periodic access review and revalidation of user accounts, written and approved access requests, and written records to document the granting of access.

h. Develop and implement written procedures to ensure that when individuals retire, leave the organization, or have their system access requirements changed because of personnel actions, these individuals are identified and their access is appropriately altered.

i. Designate positions with critical-sensitive access as ADP-I and require background investigations in accordance with Financial Systems Organization Policy TS-02, "Security Classifications for ADP Positions," May 18, 1994.

j. Implement plans to conduct regular training in security awareness for employees as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988.

k. Implement policies and procedures for management of end-user computing resources, as required by DoD Directive 7920.5, "Management of End-User Computing (EUC)," March 1, 1989, to ensure the integrity of the Defense Business Management System development system.

A.2. We recommend that the Director, Defense Finance and Accounting Service, conduct periodic follow up on weaknesses in access control and security administration identified in the Defense Finance and Accounting Service August 30, 1994, internal audit report that the Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio, identified as completed.

Management Comments. The Defense Finance and Accounting Service concurred with the recommendations. Implementation of recommendations occurred between November 1995 and January 1996 for all recommendations except Recommendation A.2. which is scheduled to be completed by December 1996.

Finding B. Software Change Management

The FSA Columbus did not adequately control DBMS software changes to ensure that only authorized changes were made. This inadequate control occurred because weaknesses existed in software librarian functions, procedures for reviewing software changes, and procedures for authorizing software moves. As a result, DBMS software integrity was weakened, and critical DoD pay and personnel records were not adequately protected.

Software Change Management

Software change management is the system of management controls used by a software development organization, such as the FSA Columbus, to ensure the correctness of changes to the software code. The objectives of software change management are to ensure that:

- o requested changes are analyzed and processed in order of priority,
- o individual programmers have access only to portions of the software needed to complete a software change,
- o software changes are not implemented without supervisory approval,
- o no unauthorized changes are processed, and
- o all authorized changes operate as intended.

Effective software change management satisfies these objectives by recording and tracking each change request, reviewing programmer changes before a change is moved from one library to another, and testing each authorized change before the change is incorporated into the development code. Separation of duties between programmers and software librarians is critical to the effectiveness of these controls.

In software development, segregation of duties should exist between the functions of initiating software changes, programming the changes, reviewing programmer changes and authorizing software moves, and testing required changes. Segregation of the responsibility and authority for these functions, combined with adequate supervision, helps to maintain the integrity of systems and programs.

Software Librarian Function

The FSA Columbus did not have a librarian dedicated to software development who performed all software moves and compiles. A software librarian is an employee who controls the software and has access to move software from one library to another. The function of a software librarian is to ensure that individuals have access only to portions of the software needed to perform their duties.

Instead, each FSA Columbus programmer moved his or her own software from source libraries into development status, and then moved changes from development status into testing. As a result, FSA Columbus did not have adequate control over the software change process.

On August 11, 1995, FSA Columbus proposed limiting the authority to move software from development status into testing status. These changes, if implemented and combined with software change reviews, would significantly improve the change management procedures at FSA Columbus. In its memorandum of December 18, 1995, FSA Columbus management stated that programmers no longer had the authority to move software from development into testing. That authority is now limited to the software librarian.

Software Change Review

Managers at FSA Columbus did not review programmer changes to DBMS code to ensure that only authorized changes were made. At FSA Columbus, program changes were completed, compiled, and moved from development into testing with no formal reviews. FSA Columbus managers stated that although they did not formally review software changes for unauthorized code, they occasionally made informal reviews. However, FSA Columbus managers had no documentation for those informal reviews.

Because FSA Columbus did not review programmer changes, programmers could insert unauthorized code without detection in order to circumvent the production system's security. As a result, FSA Columbus managers did not know whether any DBMS program modules, which consisted of 2.1 million lines of program code, contained unauthorized code inserted for fraudulent or malicious purposes.

FSA Columbus issued internal security instruction SEC.3001.1, "Software Security," on December 15, 1995. This instruction requires that personnel in ADP-I positions review all software code changes to ensure that only authorized changes have been made. The instruction, combined with limitations on the software librarian function, should significantly improve the procedures for software change management at FSA Columbus.

Authorization Procedures for Software Moves

At FSA Columbus, authorization procedures for software moves did not prevent unauthorized changes to the DBMS. FSA Columbus managers did not clearly establish responsibility and authority for the content of program changes. When a programmer completed a software change to the DBMS development code, the programmer moved the software change from development into testing. The software move was completed without a formal supervisory review of the content of the program change, and without authorization from a supervisor. Therefore, unauthorized changes could be made without detection and eventually moved into production.

FSA Columbus managers believed that their testing process ensured that no unauthorized changes were made to the DBMS. However, the FSA Columbus should not rely on its testing process to identify unauthorized changes to the DBMS code. The FSA Columbus testing process was designed to identify whether authorized changes to the code would perform as intended, not to identify unauthorized changes to the code.

The FSA Columbus Systems Management Office issued internal instruction SMO002, "Systems Management Office Procedures," on November 9, 1995. This instruction requires both the programmer and the supervisor (ADP-I) to certify that only authorized changes were made and that the program was tested and obtained the desired results.

The instruction, combined with limitations on the software librarian function, should significantly improve the procedures for software change management at FSA Columbus.

Conclusion

The management of software changes was not adequate to prevent unauthorized changes to the DBMS. Weaknesses existed in software librarian functions, review of software changes, and authorization of software moves. The FSA Columbus lacked a dedicated software librarian and could not ensure that individuals with system accounts had access only to portions of the software needed to perform their duties. In addition, FSA Columbus managers did not review programmer changes to the DBMS development program to determine whether these changes contained unauthorized code. Because FSA Columbus procedures for software moves were weak, programmers could move unauthorized routines (designed to circumvent DBMS security) from development to testing, and eventually into the DBMS production code. Consequently, FSA Columbus could not provide reasonable assurance that DBMS integrity was intact. DFAS should review selected portions of the existing DBMS software code based on the risk of compromise to verify that the code does not contain unauthorized routines designed to circumvent DBMS security.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Director, Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio:

1. Segregate the responsibility for moving all software from source libraries into development and into testing.

Management Comments. The Defense Finance and Accounting Service concurred and stated that they have completed action to segregate responsibilities for software moves.

2. Implement procedures for software development, requiring a supervisor to:

a. Review programmer changes to ensure that only authorized changes are included in software updates, and

b. Authorize software moves from source libraries to development status and from development status to testing to ensure that all moves are based on approved changes.

Management Comments. The Defense Finance and Accounting Service concurred and stated that they have completed action to update formal change procedures.

3. Update procedures for software change management to:

a. Define responsibilities for the content of program changes,

b. Specify authority for moves from source libraries into development and into testing, and

c. Ensure that moves are performed only with the proper authorization.

Management Comments. The Defense Finance and Accounting Service concurred and stated that they have completed action to update formal change procedures.

4. Based on the risk of compromise, review selected portions of the existing software code for the Defense Business Management System to verify that routines designed to compromise the integrity of the system are not present.

Management Comments. The Defense Finance and Accounting Service non-concurred and stated that the auditors did not provide documented evidence

of compromise in the DBMS code. Further, they stated that the DBMS system had been in operation for 25 years and they are not aware of any documented instances of compromise to the software code.

Audit Response. DFAS comments did not adequately address the recommendation. DFAS has a responsibility to its customers to ensure that the DBMS code is secure and is free of routines designed to circumvent system security. The DBMS relies almost exclusively on application level security routines hard-coded into the data base access system to prevent system compromise. Application level security is usually more efficient and convenient to implement than system level security. However, application level security is inherently weaker because it could allow a programmer to insert routines to bypass authorization and compromise the program's security. This type of attack can be particularly damaging because it is normally accomplished by a sophisticated insider and it is very difficult to detect.

This application level security risk was identified to FSA Columbus in a December 1, 1994, Security Test and Evaluation Report performed for FSA Columbus by the DLA Systems Design Center. The report recommended that FSA Columbus test the application code for unauthorized routines every time a program which contains authorization code is modified. Despite this recommendation, when we briefed FSA Columbus in June of 1995 they had not implemented any formal procedures for testing programmer changes for the presence of unauthorized code. Management at that time stated that they only performed this type of test informally. FSA Management further stated that they had never had a formal requirement to test for this type of compromise. Management was unable to provide any assurance that the DBMS software had not already been compromised.

The recommendations that FSA Columbus implemented as a result of Findings A and B of this report will minimize the possibility of this type of compromise being inserted into existing DBMS program code in the future. Without actually checking the code, however, the DFAS has no assurance that the DBMS application level security has not already been compromised. Whether we identified specific instances of compromise during our limited review is immaterial. This type of compromise is subtle and potentially devastating. For many years, the possibility existed for this type of compromise to be made. Once such a compromise is inserted, it remains in the production code until specifically identified.

Without a review of selected portions of the existing software code, FSA Columbus cannot be certain that the integrity of the DBMS system is intact and cannot provide the necessary assurances that their customers assets will be safeguarded. We ask that DFAS management reconsider its position and provide additional comments on the final report.

Finding C. Disaster Preparedness

The DMC Columbus and the DSDC were not adequately prepared to react in the event of a disaster. This inadequacy occurred because neither the DMC Columbus nor the DSDC had:

o analyzed the risks and the potential for catastrophic events that could result in loss of data and processing capability,

o prepared adequate, detailed disaster recovery plans to provide for orderly recovery in the event of a catastrophe,

o backed up software data files to an off-site storage location frequently enough to minimize loss, or

o tested disaster recovery plans under realistic conditions to determine whether the plans were realistic and that employees knew how to proceed if a catastrophe occurred.

As a result, in the event of a catastrophe, computer service could be significantly interrupted and critical data lost by the DMC Columbus, the DSDC, and the critical procurement, personnel, pay, and logistics systems they support.

Continuity-of-Operations Planning

Continuity-of-operations planning consists of plans, reviews, and preparations made by a data processing organization to minimize loss of data and interruption of service in the event of a catastrophe. Continuity-of-operations planning should be ongoing. The Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," July 15, 1994 (OMB Circular No. A-130), and DoD Directive 5200.28 require agencies to:

o perform a disaster risk analysis to identify potential catastrophes and the risk that each might occur,

o develop disaster recovery plans to prepare for each catastrophe and minimize potential adverse effects,

o implement cost-effective preparations to minimize losses in the event of a catastrophe,

o conduct tests under operational conditions to determine whether the plans are realistic and achieve their objectives, and

o review the plans on a periodic basis and modify them to reflect organizational changes and lessons learned from testing.

Continued availability of the DMC Columbus and DSDC computer systems and the data stored on them is essential to DBMS processing and development and to the mission of DoD, DMC Columbus, DSDC, and FSA Columbus. In the event of a catastrophe at DMC Columbus or the DSDC, computer service could be significantly interrupted and critical data lost by procurement, personnel, payroll, and logistics systems.

In FY 1996, Congress appropriated $12 million for the Defense Information Systems Agency's continuity-of-operations and test facility at Slidell, Louisiana. The site will provide backup operational support for the Defense Information Systems Agency's megacenters, including DMC Columbus, and will test new software for the megacenters and the Naval Reserve.

Disaster Risk Analysis

Neither the DMC Columbus nor the DSDC had performed a disaster risk analysis, as required by OMB Circular No. A-130, to analyze the risks and determine expected losses from catastrophic events. DMC Columbus and the DSDC had prepared disaster recovery plans without the benefit of a risk analysis. A disaster risk analysis is intended to determine:

o the frequency and risk of a potential catastrophe,

o the impact a potential catastrophe may have on operations,

o whether resources are effectively distributed to minimize loss, and

o the cost factors to be used in developing a disaster recovery plan.

Without a disaster risk analysis, the DMC Columbus and the DSDC do not have a basis for their disaster recovery plans. The DMC Columbus has made plans for a contractor to perform the risk analysis in FY 1996.

Disaster Recovery Plans

The DMC Columbus and the DSDC did not prepare adequate disaster recovery plans to provide for orderly recovery in the event of a catastrophe.

A disaster recovery plan gives detailed steps that an organization should take in the event of a catastrophe. It specifies preventive measures and realistic plans for reacting to each risk identified in the disaster risk analysis. The disaster recovery plan should specify individuals or teams responsible for each phase of recovery and should name points of contact, with alternates, for each action to be taken. A copy of the plan should be stored off-site.

On January 14, 1994, the Defense Information Systems Agency issued a model plan with guidelines and examples to help DMC Columbus write a disaster recovery plan. As of November 9, 1995, the DMC Columbus draft disaster recovery plan was not based on a risk analysis and had not been finalized or tested under realistic conditions. Therefore, the disaster recovery plan may not adequately protect critical data or ensure system availability in the event of a catastrophe.

The DSDC disaster recovery plan, issued on April 1, 1990, is inadequate. The DSDC disaster recovery plan was not based on a disaster risk analysis. The DSDC did not review and update the plan to reflect organizational changes, and has not tested the plan under realistic conditions. DSDC managers believe that testing the plan is not cost-effective, and therefore have no plans to do so.

Data File Backup and Off-Site Storage

The DMC Columbus and the DSDC did not back up software data files to an off-site storage location frequently enough to minimize loss. Interservice support agreements between DFAS and DMC Columbus, and between DSDC and FSA Columbus, specify the services and support to be provided.

Frequent backup of data files and off-site storage are critical elements of any disaster recovery plan. Adequate backups stored at an off-site location allow complete rebuilding of computer systems even if a processing facility is totally destroyed.

Neither the DFAS-DMC Columbus nor the DSDC-FSA Columbus interservice support agreement specified how frequently backups should be made or data files sent to off-site storage locations. In addition, the DSDC did not have written backup procedures to ensure that frequent backups were done and that the correct files were backed up.

The DMC Columbus backed up data files every 2 weeks and sent data to off-site storage every 3 weeks to minimize data loss in the event of a catastrophe. The DSDC performed off-site backup of critical development and test data for FSA Columbus on a monthly basis. The FSA Columbus estimated that if data were destroyed by a catastrophe, $600,000 in staff hours would be lost.

Both DFAS and FSA Columbus should increase data file backups and off-site storage of backup tapes. In addition, both interservice support agreements should be modified to stipulate the frequency of data file backups and off-site storage.

Testing of Disaster Recovery Plans

Neither DMC Columbus nor DSDC tested their disaster recovery plans under realistic conditions, as required by OMB Circular No. A-130 and DoD Directive 5200.28.

Disaster recovery plans must be tested regularly to ensure that the plans will work effectively in the event of a catastrophe. Testing a disaster recovery plan under realistic conditions allows the strengths and weaknesses of the plan to be identified and allows employees to practice the procedures they would use if a catastrophe occurred.

Without adequate testing of disaster recovery plans DMC Columbus and DSDC managers cannot demonstrate that their plans can be implemented as intended and that data can be recovered and operations returned to normal.

Conclusion

The DMC Columbus and the DSDC are not prepared to react in the event of a catastrophe. The DMC Columbus and the DSDC do not have:

- adequate disaster recovery plans based on risk analyses,
- adequate backup of data files and off-site storage of backups, and
- adequate testing of disaster recovery plans.

Consequently, neither organization is prepared to react in the event of a catastrophe. Both would have difficulty recovering data and resuming services to support critical functions after a service interruption. As a result, significant service interruptions are more likely, and any service interruption could continue much longer than necessary.

Because computer processing missions are concentrated at these two data centers, a single catastrophe could significantly affect procurement, personnel, payroll, and logistics systems, which could experience significant service interruptions and lose critical data. Also, the lack of disaster preparation at the DMC Columbus is a material management control weakness.

Recommendations, Management Comments, and Audit Response

C.1. We recommend that the Director, Defense Megacenter, Columbus, Ohio:

a. Develop a detailed disaster risk analysis of all threats and vulnerabilities to aid in completing a disaster recovery plan.

b. Finalize the disaster recovery plan currently in development and implement it as required by the Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," July 15, 1994, and DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988.

c. Begin periodic testing of the disaster recovery plan as required by the Office of Management and Budget Circular No. A-130 and DoD Directive 5200.28, to refine the plan and ensure continuity of operations in the event of a disaster.

DISA Comments. The Defense Information Systems Agency concurred with the recommendations. They are currently preparing a detailed risk analysis and designing a disaster recovery plan. They expect these actions to be complete by June 1996. They intend to test the plan once it has been completed.

C.2. We recommend that the Director, Defense Logistics Agency Systems Design Center, Columbus, Ohio:

a. Develop a detailed disaster risk analysis of all potential threats and vulnerabilities to aid in refining the Systems Design Center's disaster recovery plan.

b. Review and update the disaster recovery plan to reflect organizational changes.

c. Begin periodic testing of the Systems Design Center's disaster recovery plan under realistic operating conditions as required by the Office of Management and Budget Circular No. A-130 and DoD Directive 5200.28, to refine the plan and ensure continuity of operations in the event of a disaster.

DLA Comments. DLA concurred with Recommendation C.2.a., stating that the Systems Design Center computer lab will be moving. This action is scheduled to occur in October 1996. Once the new site is determined, DLA will perform a detailed disaster risk analysis. DLA also concurred with Recommendation C.2.b., stating that the disaster recovery plan will be updated. The estimated completion date for this action is September 30, 1996.

DLA nonconcurred with Recommendation C.2.c., stating that system availability is unimportant because the emergency customer hotline is the only

function DSDC must support in the event of a disaster. Hotline support may be provided at an alternate site. DLA states that the mission of the DSDC is not critical enough to justify reconstitution at an alternate site.

Audit Response. The DLA response to Recommendation C.2.c. did not adequately address the issues. The DLA Systems Design Center provides many more functions than just hotline response. The losses experienced as a result of a disaster are not limited to just lost customer support. The productivity of the individuals who use a computer system for everyday work is often the highest cost of a disaster. Disaster recovery plan testing is the only way to ensure that a recovery plan works. Testing the plan is also the best way to minimize lost productivity costs in the event of a disaster. Without testing, DLA cannot be confident that their disaster recovery plan will limit lost productivity in the event of a catastrophe. Testing the plan does not imply that the Systems Design Center needs to reconstitute their operations at an alternate site. A test plan should be developed based on a risk assessment to address the most likely disaster conditions and how they should be responded to. Testing can also be done on a cost-effective modular basis to minimize cost and disruption. Finally, periodic testing of disaster recovery plans is required by regulations.

We ask that DLA management reconsider their responses and provide additional comments on the final report.

C.3. We recommend that the Director, Defense Finance and Accounting Service, Columbus, Ohio, modify and fund the interservice agreement with the Defense Megacenter, Columbus, Ohio, to back up and send critical Defense Business Management System data files to an off-site location at least once each week.

DFAS Comments. The Defense Finance and Accounting Service concurred and stated that the interservice agreement with the Defense Megacenter Columbus was modified and backups are now performed on a weekly basis.

C.4. We recommend that the Director, Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio, modify and fund the interservice agreement with the Defense Logistics Agency Systems Design Center to back up and send Defense Business Management System development files to an off-site location at least twice each month.

DFAS Comments. The Defense Finance and Accounting Service concurred and stated that backups were now being performed on a weekly basis. Negotiations with the Defense Logistics Agency Systems Design Center, Columbus, Ohio, to modify the inter-service agreement were expected to be completed by September 1996.

Part II - Additional Information

Appendix A. Scope and Methodology

Scope

Audit Scope. We reviewed selected general controls and issues related to the DBMS. We also reviewed compliance with the requirements of Title 2 of the General Accounting Office's "Policies and Procedures Manual for Guidance of Federal Agencies," compliance with the Joint Financial Management Improvement Program's "Core Financial System Requirements," and implementation of the DoD management control program.

Audit Period, Standards, and Locations. We performed this financial-related audit from March through December 1995. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General (IG), DoD. We did not use statistical sampling procedures to conduct this audit. We included tests of management controls that we considered necessary. Appendix D lists the organizations visited or contacted.

Use of Computer-Processed Data. We used standard utility programs and reports generated by commercial security software packages to satisfy our objective on general controls. To assess security rules and features, we used data from two security software packages, 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 marketed by the Cincom Corporation for use with the SUPRA database system. 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 we found were sufficiently reliable to meet the audit objectives and support our audit conclusions.

Methodology

At FSA Columbus, we reviewed:

- access to critical DBMS development libraries,
- security software attributes,
- security administration,

- software change management, and
- the use of a change management software package.

In addition, we reviewed disaster preparedness at the DMC Columbus and the DSDC. We also reviewed policies, procedures, and the implementation of Title 2 of the General Accounting Office's "Policies and Procedures Manual for Guidance of Federal Agencies" and the Joint Financial Management Improvement Program's "Core Financial System Requirements." We reviewed pertinent laws and regulations and other related documentation, and we interviewed managers and employees.

Management Control Program

DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, 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 Management Control Program. We reviewed the DFAS Annual Statement of Assurance for FY 1994 and the implementation of the DFAS Columbus management control program.

Adequacy of Management Controls. We identified material management control weaknesses, as defined by DoD Directive 5010.38, relating to computer security at FSA Columbus and disaster preparation at DMC Columbus. At FSA Columbus, weaknesses in access control threatened the integrity of the DBMS software. At DMC Columbus, lack of disaster preparation threatened the survivability and availability of critical computer systems. Recommendations A.1. and C.1., if implemented, will correct these weaknesses. A copy of the report will be provided to the senior official responsible for management controls in the Defense Finance and Accounting Service and the Defense Information Systems Agency.

The DFAS Annual Statement of Assurance for FY 1994 reported management control weaknesses in the DBMS. These issues were addressed in IG, DoD, Report No. 95-280, "Management Control Program at Defense Information Systems Agency, Western Hemisphere," July 26, 1995, and are therefore not addressed in this report.

Appendix B. Prior Audits and Other Reviews

We identified six prior IG, DoD, reports relating to this audit.

IG, DoD, Report No. 95-280. This report, "Management Control Program at Defense Information Systems Agency, Western Hemisphere," was issued on July 26, 1995. The report stated that the Defense Information Systems Agency, Western Hemisphere, and DFAS did not adequately review accounting system controls. The report recommended that those 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 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 corrective actions.

IG, DoD, Report No. 94-161. This report, "Consolidated Statement of Financial Position of the Defense Business Operations Fund for FY 1993," was issued on June 30, 1994. The report identified a $1.88 billion discrepancy between DFAS and the Defense Logistics Agency's records, and a difference of $1.9 billion in collections and disbursements related to the Defense Logistics Agency supply management business area. Neither discrepancy could be reconciled. The audit report made no recommendations.

IG, DoD, Report No. 94-082. This report, "Financial Management of the Defense Business Operations Fund for FY 1992," was issued on April 11, 1994. The report stated that the Military Departments and other DoD Components were using unique charts of accounts and crosswalking the financial data from their general ledger accounts to the U.S. Standard General Ledger to prepare management reports and financial statements. In addition, the accounting systems used by the organizations did not include the new general ledger account codes. The report recommended full implementation of the U.S. Standard General Ledger. Management concurred and agreed to take corrective action.

IG, DoD, Report No. 94-081. This report, "Controls Over Access to Personnel and Payroll Data for the Defense Commissary Agency," was issued on April 11, 1994. The report stated that controls did not prohibit unauthorized access and did not prevent users from adding, changing, and deleting data in payroll and personnel subsystems. In addition, some employees had access to both payroll and personnel subsystems in the data bases. Users were still holding passwords issued by the Defense Information Technology Service Organization as long as 16 months after receipt. The report recommended that the number of employees with access to the payroll and personnel subsystems be limited, and that software be modified to require employees to periodically change their passwords. Management fully concurred with the report and recommendations.

IG, DoD, Report No. 94-060. This report, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," was issued on March 18, 1994. The report stated that the DBMS users neglected to change their password within 180 days. In addition, numerous users had not changed their passwords in over 1 year. This occurred because security personnel at the Defense Information Services Organization-Columbus Center did not periodically review the age of passwords, nor 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.

IG, DoD, Report No. 93-133. This report, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," was issued on June 30, 1993. The report stated 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 the system and 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 APF datasets in order to keep the system running. In addition, management relied on system users to control password lengths. The Job Entry Subsystem 2 log-on identification and security option for password checking was not installed at Defense Logistics Agency Systems Automation Center, 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 RACF utilities to personnel who have a clearly defined need, and review Job Entry Subsystem 2. Management concurred with all recommendations and agreed to take corrective action.

Appendix C. DBMS Project Manager and Core Financial System Requirements

On September 5, 1995, a DBMS Project Manager was appointed for the first time.

Core Financial System Requirements

DBMS does not meet the core requirements for an agency's integrated financial management system, as specified in Title 2 of the General Accounting Office's "Policies and Procedures Manual for Guidance of Federal Agencies" (Title 2) or the Joint Financial Management Improvement Program.

Title 2 establishes accounting principles, standards, and related requirements. Title 2 also incorporates the uniform requirements for an agency's integrated financial management system. Title 2 provides a comprehensive basis of accounting for preparing financial statements. The Joint Financial Management Improvement Program establishes uniform requirements for financial information, reporting, and financial systems and organization.

In December 1994, when the Under Secretary of Defense (Comptroller) selected the DBMS as the interim migratory system for seven DBOF business areas, the DBMS was not in compliance with the core financial system requirements. The system evaluation report for the DBMS, "Interim Migratory System for the Defense Business Operations Fund," August 1994, concluded that approximately $8 million and more than 39 staff years (470 months) of work would be required to meet the core requirements. DoD plans to make extensive software and technical upgrades to meet the core requirements. Funding for the software and technical upgrades depends on the enactment of DoD appropriations. Therefore, no recommendations are included in this report.

Appendix D. Organizations Visited or Contacted

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller), Washington, DC
Assistant Secretary of Defense (Command, Control, Communications and Intelligence), Washington, DC

Other Defense Organizations

Defense Finance and Accounting Service, Arlington, VA
- Defense Finance and Accounting Service Center, Columbus, OH
- Defense Finance and Accounting Service Financial Systems Organization, Indianapolis, IN
  - Defense Finance and Accounting Service Financial Systems Activity, Columbus, OH

Defense Information Systems Agency, Arlington, VA
- Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, MD
  - Defense Megacenter, Columbus, OH

Defense Logistics Agency, Fort Belvoir, VA
- Defense Logistics Agency Systems Design Center, Columbus, OH

Non-Defense Federal Organizations

Federal Emergency Management Agency, Baltimore, MD
Department of Commerce, Washington, DC
- National Weather Service, New Orleans, LA

Non-Government Organizations

City Planning Commission, Slidell, LA

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Assistant to the Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Finance and Accounting Service
  Director, Defense Finance and Accounting Service Columbus Center
  Director, Defense Finance and Accounting Service Financial Systems Organization
    Director, Defense Finance and Accounting Service Financial Systems Activity Columbus
Director, Defense Information Systems Agency
  Director, Defense Megacenter Columbus
Director, Defense Logistics Agency
  Defense Logistics Agency Systems Design Center

Non-Defense Federal Organizations

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

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 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

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

APR 18 1996

DFAS-HQ/AC

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL (ANALYSIS AND FOLLOW-UP)

SUBJECT: Audit Report on Selected General Controls over the Defense Business Management System (Project No.5FG-2007.01)

This is in response to your memorandum of February 6, 1996, pertaining to the subject above. We concur in the findings and the recommendations pertaining to DFAS. Our detailed comments are attached.

If you need additional information, my point of contact is Bharpur Grewal, DSN 327-1525 or (703) 607-1525.

Edward A. Harris
Deputy Director for Business Funds

Attachment

ATTACHMENT

DFAS-HQ RESPONSE TO DoDIG DRAFT AUDIT FINDINGS AND RECOMMENDATIONS

DBMS Project 5FG-2007.01

The findings addressed in the DoDIG's audit review regarding the adequacy of Selected General Controls over the Defense Business Management System at Financial Systems Activity Columbus, Ohio (FSACO) relate to the software development efforts which are conducted on the development system rather than on the actual DBMS production system.

The areas addressed in the review included access to critical DBMS development libraries, security software attributes, security administration, software change management, and the use of a change management software package. The draft audit states that FSA Columbus lost control over access because managers did not: develop an access control policy based on identified vulnerabilities, effectively control system access authorizations, periodically review and revalidate user accesses, classify positions and conduct appropriate background investigations, provide regular training in security awareness, and protect personal computers from potential compromise of the DBMS.

Our specific responses to these concerns are as follows:

Computer Security. DFAS has always had a strong commitment to security measures to protect the DBMS developmental system. Formal and desk level working procedures existed prior to the audit review protecting computer security at FSACO. Non-active user accounts, including personnel no longer with FSACO, were previously revoked after 180 days of non-use. We have recently enhanced our security controls by reducing the 180 day period to a 30 day period. We have implemented several other security controls to further enhance our security in the areas identified by the DoDIG audit report.

Software Change Management. We "formally" documented our long standing working procedures relating to functional alignment which separates functional responsibility relating to those who write code, who approve code and who move the formal software

code to test libraries. The FSACO has, both currently and in the past, an effective software change process to ensure that released DBMS software changes to production are what was ordered by the customer/program manager for all systems.

RESPONSE TO RECOMMENDATION A - COMPUTER SECURITY AT FSA COLUMBUS:

Recommendation:

A.1. We recommend that the Director, Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio:

a. Review all user access for the Defense Business Management System development system and restrict access to the computer and sensitive files to personnel who need access and for whom the required background investigations have been completed.

b. Limit access to the Resource Access Control acility special attribute to the Information System Security Officer, who has had a background investigation and does not have programming responsibilities.

c. Limit access to the Resource Access Control Facility operations attribute to:

(1) Individuals with library management responsibilities who have had background investigations, and

(2) Started tasks with an identified need for this attribute.

d. Use the Resource Access Control Facility revoke-date feature to control temporary accounts and enforce receipts for passwords.

e. Activate the Resource Access Control Facility protect-all option required for a C2 security rating on the Defense Business Management System development system, or obtain a waiver of C2 security requirements from the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), as established in DoD

Directive 5200.28, "Security requirements for Automated Information System (AIS)," March 21, 1988.

f. Develop and implement a formal, written policy for access control; the policy should include enforcement procedures and a plan for continuously improving system security.

g. Develop and implement written procedures that require periodic access review and revalidation of user accounts, written and approved access requests, and written records to document the granting of access.

h. Develop and implement written procedures to ensure that when individuals retire, leave the organization, or have their system access requirements changed because of personnel actions, these individuals are identified and their access is appropriately altered.

i. Designate positions with critical-sensitive access as ADP-I and require background investigations in accordance with Financial Systems Organization Policy TS-02, "Security Classifications for ADP Positions," May 18, 1994.

j. Implement plans to conduct regular training in security awareness for employees as required by DoD Directive 5200.28, "Security Requirements for Automated Information systems (AIS)," March 21, 1988.

k. Implement policies and procedures for management of end-user computing resources, as required by DoD Directive 7920.5, "Management of End-User Computing (EUC)," March 1, 1989, to ensure the integrity of the Defense Business Management System development system.

A.2. We recommend that the Director, Defense Finance and Accounting Service, conduct periodic follow up on weaknesses in access control and security administration identified in the Defense Finance and Accounting Service August 30, 1994, internal audit report that the Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio, identified as completed.

We concur with recommendation A.1.a. User accesses have been reviewed, corrected, and validated; position sensitivity

definition has been accomplished; required background investigation requests for personnel not already approved were forwarded to the proper personnel for further action. Our internal policy "Policy on Security Classifications for Automated Data Processing (ADP) Positions", with procedure SEC.3003, "Security Classifications for ADP Positions", was published and implemented on November 29, 1995. Action complete.

We concur with recommendation A.1.b. The Resource Access Control Facility (RACF) special attribute is restricted to two (2) SAC5 users (the RACF administrator, and the support person, who also serves as backup administrator), an emergency "backup" account (available only to the regular and backup RACF administrator), and a "batch" account used exclusively for security batch jobs. All actions by those with the special attribute are audited. Both RACF administrators have undergone the required background investigations. Action complete.

We concur with both recommendations A.1.c.(1) and A.1.c.(2). Effective in December 1995 the operation attribute was assigned to a single task, the monthly backup. Action complete.

We concur with the recommendation A.1.d. The RACF revoke-date feature is in effect for new and temporary user accounts. Manual revocation occurs when the "FSACO Acknowledgment of System Access" form 1003 is not received within a prescribed timeframe. In February 1996 we changed the deactivation of accounts not used "within 180 days" to "within 30 days". Action complete.

We concur with recommendation A.1.e. On January 16, 1996, the protect-all option was fully activated in the "fail" mode. Action complete.

We concur with recommendation A.1.f. Our formal internal policy "System Access Policy", with procedure, SEC.3007 "System Access Control", and policy SEC.3005 "Automated Information System Security Policy", with document "DFAS-FSACO Internal Automated Information Systems(AIS) Security Program", were published and implemented consecutively on November 29, 1995, and November 30, 1995. Action complete.

We concur with recommendation A.1.g. Our formal internal policy "System Access Policy", with procedure SEC.3007, "System Access Control", was published and implemented on November 29,

1995. The first of the semi-annual security access reverification reviews was completed in December 1995. Hard copy of all DBMS user request forms are being maintained by the ISSO. Action complete.

We concur with recommendation A.1.h. Formal policies and procedures were published and implemented on November 29, 1995, that addressed these issues. Action complete.

We concur with recommendation A.1.i. Our formal internal policy "Policy on Security Classifications for ADP Positions", with procedure SEC.3003, "Security Classifications for ADP Positions", was published and implemented November 29, 1995. Background investigation paperwork for personnel not already satisfying this requirement was submitted to the centralized personnel office located in Indianapolis for action. Action complete.

We concur with recommendation A.1.j. Our formal internal policy "Security Awareness Training Policy", with procedure SEC.3008, "Security Awareness Training", was published and implemented on December 11, 1995. Security training is now being provided through a variety of media. The ISSO retains signed attendance records for all formal security training. Action complete.

We concur with recommendation A.1.k. A conjoint review between FSO headquarters and FSACO is currently being worked to address the issue of hardware passwords for personal computers. Implementation depends on the outcome of that review. However, we issued Internal Procedure SEC.3011, "Protection of Sensitive/ Unclassified Information", on November 29, 1995. Estimated completion date is December 1996.

We concur with recommendation A.2. Our Internal Control and Audit Directorate periodically conducts internal reviews. We will request them to conduct follow up on weaknesses in access control and security administration identified in your recommendation A.2. Action complete.

RESPONSE TO RECOMMENDATION B - SOFTWARE CHANGE MANAGEMENT

Recommendation:

B. We recommend that the Director, Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio:

1. Segregate the responsibility for moving all software from source libraries into development and into testing.

2. Implement procedures for software development, requiring a supervisor to:

a. Review programmer changes to ensure that only authorized changes are included in software updates, and

b. Authorize software moves from source libraries to development status and from development status to testing to ensure that all moves are based on approved changes.

3. Update procedures for software change management to:

a. Define responsibilities for the content of program changes,

b. Specify authority for moves from source libraries into development and into testing, and

c. Ensure that moves are performed only with the proper authorization.

4. Review the existing software code for the Defense Business Management System to ensure that routines designed to compromise the integrity of the system are not present.

We concur with recommendation B.1. However, we feel that the current FSACO environment provides adequate separation. The software librarian function is tasked to the System Management Office, and not to a particular individual. The Systems

Management Office is comprised of technical and data base support personnel ensuring separation of duties from the program development staff. While programmers can move programs into development status, they cannot move these programs into test status. This part of the cycle is controlled, preventing unauthorized users from making unauthorized changes to programs and moving those programs into production. Action complete.

We concur with recommendation B.2 A formal internal policy and procedure SEC.3012, "Release Control Policy", was signed in November 1995. We are implementing formal code reviews for all program changes. Action complete.

We concur with recommendation B.3. A formal internal policy and procedure SEC.3012, "Release Control Policy", addresses these issues and was implemented November 30, 1995. Action complete.

We nonconcur with recommendation B.4. The draft audit report presents no evidence that routines exist in the DBMS production software code which have compromised the integrity of the system. Additionally, we specifically asked the audit team leader for any such evidence and none was provided. The DBMS system has been in operation for over 25 years and we are aware of no documented instances of compromise to the source code or to the financial statements produced by the system. Action complete.

RESPONSE TO RECOMMENDATION C - DISASTER PREPAREDNESS

Recommendation:

C.3. We recommend that the Director, Defense Finance and Accounting Service, Columbus, Ohio, modify and fund the interservice agreement with the Defense Megacenter, Columbus, Ohio, to back up and send critical Defense Business Management System data files to an off-site location at least once each week.

C.4. We recommend that the Director, Defense Finance and Accounting Service Financial Systems Activity, Columbus, Ohio, modify and fund the interservice agreement with the Defense Logistics Agency Systems Design Center to back up and send Defense Business Management System development files to an off-site location at least twice each month.

We concur with recommendation C.3. When the audit was being conducted, Defense Megacenter, Columbus was backing-up DBMS data every third week of the month and sending it off-site. Since that time, the procedure has been modified; they are backing-up data dumps each week. This includes all critical files and the Direct Access Storage Device (dumps). Service Level Agreement (LA) Appendix A states, by application, the frequency of each system back-up. The DMC is sending DFAS-CO weekly status reports to ensure they are in compliance with the SLA on the backing-up application. Action complete.

We concur with recommendation C.4 and anticipate that the FSACO/DSDC interservice support agreement can be negotiated and modified by September 1996. Estimated completion date is September 1996.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO:

Inspector General 5 April 1996

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
Attn: Director, Finance and Accounting Directorate

SUBJECT: Draft Audit Report, "Selected General Controls Over the Defense Business Management System," (Project No. 5FG-2007.01)

Reference: DODIG Report, subject as above, 6 Feb 96

We have reviewed the subject report and concur with the findings and recommendations. Our detailed management comments which identify corrective actions to be taken are at the enclosure. If you have questions, the point of contact for this action is Ms. Sandra J. Leicht, Audit Liaison, on (703) 607-6316.

FOR THE DIRECTOR:

Marlene M Tate
for RICHARD T. RACE
Inspector General

1 Enclosure a/s

Quality Information for a Strong Defense

Management Comments to DODIG Draft Audit Report on Selected General Controls Over the Defense Business Management System (Project No. 5FG-2007.01)

Finding C, Recommendation 1.a: Develop a detailed risk analysis of all threats and vulnerabilities to aid in completing a Disaster Recovery Plan (DRP).

Comments: Concur. When the migrations first began, Defense Megacenter (DMC) Columbus was required to bring the applications to the DMC "as is". The requirement to perform a risk analysis on the application itself still remains with the designing activity.

DMC Columbus has been selected to be a prototype DMC for the MISSI/Fortezza advanced authentication and data encryption cards for the mainframe MVS platforms. A contractor with expertise in risk analysis will perform a detailed risk analysis of DMC Columbus as part of the MISSI/Fortezza contract prior to implementation of the Fortezza hardware and software. In addition, the DISA WESTHEM Deputy Chief of Staff for Security, will perform a detailed risk analysis of DMC Columbus. The estimated completion date for this analysis is 28 June 1996. At that time, the risk analysis will be added to DMC Columbus' DRP and the Disaster Recovery Planning Team will execute a plan to reduce risks and vulnerabilities.

Finding C, Recommendation 1.b: Finalize the DRP currently in development and implement it as required by the OMB Circular No. A-130, and DOD Directive 5200.28.

Comments: Concur. During the audit, the auditors were given a draft copy of the DRP, which was in its first stages. Since that time, the DRP has been further developed. DISA WESTHEM is planning to provide a copy of the DRP to their customers by 30 April 1996 for concurrence and approval. The DRP is scheduled for completion by 1 June 1996. A clause will be added prior to signature of the DRP indicating that if the risk analysis is not completed by the time the DRP is finalized, the risk analysis will be incorporated in the next update of the DRP. The DRP Team will continue to update the DRP as necessary while performing disaster recovery exercises.

Finding C, Recommendation 1.c: Begin periodic testing of the DRP, as required by the OMB Circular No. A-130 and DOD Directive 5200.28, to refine the plan and ensure continuity of operations in the event of a disaster.

Comments: Concur. Although DMC Columbus has not performed a DBMS disaster recovery exercise at a backup site, the DMC has successfully performed similar exercises on other applications processed at the DMC. The DBMS disaster recovery exercise scheduled for May 1996 has been canceled by the customer, DFAS. Plans are currently underway to reschedule the exercise with Comdisco Disaster Recovery Services. We will provide a date once plans become finalized.

FINDING C, Recommendation 3: Recommend that the Director, Defense Finance and Accounting Service, Columbus, Ohio, modify and fund the interservice agreement with DMC Columbus to back up and send critical DBMS data files to an offsite location at least once a week.

Comments: Concur. DISA WESTHEM has been working with DFAS-Columbus to send critical data files off-site once a week. In fact, the backup files, full DASD dumps which include all critical files, are currently being sent offsite on a weekly basis. The DMC Columbus is in the planning process of sending the daily post cycle dumps offsite each week and plans to implement the daily offsite storage in May 1996. DISA will work with DFAS to ensure that the interservice agreement is modified to reflect this arrangement.

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

5 APRIL 1996

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING, DEPARTMENT OF DEFENSE

SUBJECT: OIG Draft Report on *"Selected General Controls Over the Defense Business Management System,"* **(Project No. 5FG-2007.01)**

This is in response to your 6 February 1996. If you have any questions, please contact LaVaeda Coulter, (703) 767-6261.

1 Encl

JACQUELINE G. BRYANT
Chief, Internal Review Office

cc:
CA
CANP, Jane Johannsen

Federal Recycling Program Printed on Recycled Paper

Subject: Selected General Controls Over the Defense Business Management System (Project No. 5FG-2007.01)

Finding C: The DMC Columbus and the DSDC were not adequately prepared to react in the event of a disaster. This occurred because neither the DMC Columbus nor the DSDC had:

- analyzed the risks and the potential for catastrophic events that could result in loss of data and processing capability,

- prepared adequate, detailed disaster recovery plans to provide for orderly recovery in the event of a catastrophe,

- backed up software data files to an off-site storage location frequently enough to minimize loss, or

- tested disaster recovery plans under realistic conditions to determine whether the plans were realistic and that employees knew how to proceed if a catastrophe occurred.

As a result, in the event of a catastrophe, computer service could be significantly interrupted and critical data lost by the DMC Columbus, the DSDC, and the critical procurement, personnel, pay, and logistics systems they support.

DLA Comments:

As a Central Design Activity (CDA), the mission of DSDC includes development and deployment of system software. DSDC performs limited disaster recovery planning due to the nature of their mission. Unlike the DMC Columbus, DSDC would not reconstitute their development software at an alternate site. DSDC reconstitution efforts would be limited to emergency hotline support for their customers. Should a disaster render the computer lab inoperable, DSDC's software development mission would temporarily cease until the computer lab became operational. DSDC agrees to update their local emergency plan and they will perform a disaster risk analysis when the new location of their computer room is determined. DSDC is planning to relocate their computer lab within the next six months. DSDC is awaiting HQ DLA to approve the proposed site.

DSDC *nonconcurs* that a research and development (R&D) mission

requires reconstitution. Should a major disaster occur, the DSDC resources would be deployed to support DLA at other DLA sites. Once stabilization occurred, the DSDC resources would resume their mission.

DSDC agrees to continue current disaster planning support for the Defense Finance and Accounting Service, Financial Systems Activity Columbus, Ohio (FSACO). For a reimbursable fee, DSDC will perform more frequent backups of FSACO data files and ship these files off-site. Additionally, periodic testing of DSDC's disaster recovery plan, as applicable to FSACO, will be conducted as defined in the ISA. The degree of disaster recovery planning support will be commensurate with FSACO funds reimbursed to DSDC as specified in the Interservice Support Agreement (ISA).

Internal Management Control Weakness: *Nonconcur*

Action officer: Ms. Jane Johannsen, CANP, 767-2161
Review/Approval: Mr. Thomas J. Knapp, CAN, 767-3100
Coordination: DDAI, 2Apr96

DLA Approval:

RAY E. MOODY
Major General, USA
Principal Deputy Director

Subject: Selected General Controls Over the Defense Business Management System) (Project No. 5FG-2007.01

Recommendation C.2.a: We recommend that the Director, Defense Logistics Agency Systems Design Center, Columbus, Ohio develop a detailed disaster risk analysis of all potential threats and vulnerabilities to aid in refining the Systems Design Center's disaster recovery plan.

DLA Comments:

The DSDC computer lab will be moving from its Building 27 location in Columbus, Ohio. The new site for the computer lab has not yet been determined nor has a date for the relocation been scheduled. Once the relocation site has been identified, DSDC will perform a disaster recovery analysis of the new site.

Disposition:
Action is ongoing. **ECD: March 15, 1997**

Action officer: Ms. Jane Johannsen, CANP, 767-2161
Review/Approval: Mr. Thomas J. Knapp, CAN, 767-3100
Coordination: [illegible], DDAI, 2 Apr.

DLA Approval:

[illegible]
Major General, USA
Principal Deputy Director

Subject: Selected General Controls Over the Defense Business Management System (Project No. 5FG-2007.01)

Recommendation C.2.b: We recommend that the Director, Defense Logistics Agency Systems Design Center, Columbus, Ohio review and update the disaster recovery plan to reflect organizational changes.

DLA Comments:

DSDC *concurs* that organizational updates should be made to their Field Activity Basic Emergency Plan (FABEP) dated September 22, 1993. The plan will be thoroughly reviewed for currency and all needed changes will be incorporated.

Disposition:
Action is ongoing. **ECD: September 30, 1996**

Action officer: Ms. Jane Johannsen, CANP, 767-2161
Review/Approval: Mr. Thomas J. Knapp, CAN, 767-3100
Coordination: DDAJ, 2 Apr 96

DLA Approval:

FAYE E. MOORE
Major General, USA
Principal Deputy Director

Subject: Selected General Controls Over the Defense Business Management System (Project No. 5FG-2007.01)

Recommendation C.2.c: We recommend that the Director, Defense Logistics Agency Systems Design Center, Columbus, Ohio begin periodic testing of the Systems Design Center's disaster recovery plan under realistic operating conditions as required by the Office of Management and Budget Circular No. A-130 and DoD Directive 5200.28, to refine the plan and ensure continuity of operations in the event of a disaster.

DLA Comments:

DSDC *nonconcurs* with periodic testing of their disaster recovery plan. The only DSDC reconstitution efforts performed in a disaster would be those necessary to support emergency customer hotlines. Hotline support would only be provided from an alternate site if the hotline could not be resolved at the customer's site. Due to the very limited scope of DSDC's reconstitution requirements, testing at an alternate site is considered unnecessary. Although DSDC nonconcurs with testing, they will continue to maintain a disaster recovery plan and submit both ADP and hard copy media to an off-site storage location.

Disposition:
Action is considered complete.

Action officer: Ms. Jane Johannsen, CANP, 767-2161
Review/Approval: Mr. Thomas J. Knapp, CAN, 767-3100
Coordination: JBT, DDRT, 2 Apr 96

DLA Approval:

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
Victoria C. Hara
Maureen F. Hollingsworth
Elaine M. Jennings
James D. Stockard
Edward J. Lustberg
Ira C. Gebler
Marvin J. Sun
Ivette Reick
Susanne B. Allen
Traci Y. Sadler