Audit Report

OFFICE OF THE INSPECTOR GENERAL

CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE AND OTHER GENERAL CONTROLS FOR COMPUTER SYSTEMS SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE

Report No. 95-263 June 29, 1995

Department of Defense

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit, Audit 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, Audit 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:

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

DoD Hotline

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

Acronyms

ABENDS	Abnormal Endings
ADP	Automated Data Processing
AFAA	Air Force Audit Agency
AIS	Automated Information System
APF	Authorized Program Facility
BLP	Bypass Label Processing
CA-ACF2	Computer Associates, Incorporated, Access Control Facility 2
CA-TOP SECRET	Computer Associates, Incorporated, TOP SECRET
DISA WESTHEM	Defense Information Systems Agency Western Hemisphere
DLA-DSDC	Defense Logistics Agency, Systems Design Center
DMC	Defense Megacenter
FSA	Financial Systems Activity
IBM	International Business Machines Corporation
ID	Identification
IG	Inspector General
JES2	Job Entry Subsystem 2
MVS	Multiple Virtual Storage
PPT	Program Properties Table
RACF	Resource Access Control Facility
SVC	Supervisor Call

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

June 29, 1995

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

SUBJECT: Report on the Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service (Report No. 95-263)

We are providing this report for management's review and comments. We performed the audit in response to a request from the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be promptly resolved. The Defense Logistics Agency did not comment on a draft of this report in time for the comments to be included in this final report. Comments from the Defense Information Systems Agency were not fully responsive. Therefore, additional comments are requested by July 31, 1995, from these two organizations, as indicated at the end of each finding in Part I of the report. Comments from the Defense Finance and Accounting Service, Denver Center, and the Defense Finance and Accounting Service, Financial Systems Activity Denver, conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are requested from these two organizations.

We appreciate the courtesies extended to our audit staff. Questions about the audit should be directed to Mr. David C. Funk, Audit Program Director, at (303) 676-7445 (DSN 926-7445), or Mr. W. Andy Cooley, Audit Project Manager, at (303) 676-7393 (DSN 926-7393). See Appendix G for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Audit Report No. 95-263 **June 29, 1995**
(Project No. 4FD-5068)

Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service

Executive Summary

Introduction. This audit was made to evaluate the corrective actions taken by the Defense Information Systems Agency Western Hemisphere and the Defense Logistics Agency, Systems Design Center, in response to prior audits of computer security and other general controls. A separate audit was made on the corrective actions taken in response to these prior audits of the Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado; and the Defense Information Systems Agency Western Hemisphere's Defense Information Processing Center, Pensacola, Florida. The audits were requested by the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence).

Objectives. Our objective was to determine whether corrective actions taken or planned by the Defense Information Systems Agency, Western Hemisphere, and the Defense Logistics Agency, Systems Design Center to improve computer security adequately responded to the recommendations made in prior audit reports. The audit also evaluated the effectiveness of applicable internal controls and each organization's implementation of the DoD management control program as it pertained to our audit objectives.

Audit Results. Despite other demands on their resources, the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency made commendable efforts to implement prior audit recommendations. However, additional corrective actions were required in some areas. Including the results of the separate audit, we followed up on 87 of the 112 recommendations made in prior audit reports. Audit followup on 25 recommendations was deferred because the organizations to which the recommendations were made were being consolidated into various Defense Information Systems Agency megacenters. Of the 87 recommendations, the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency had taken adequate corrective actions on 67 recommendations (77 percent), and additional corrective actions were required on 20 (23 percent). Moreover, although incomplete, planned actions on 5 of the 26 recommendations requiring additional corrective action were considered adequate. One recommendation previously made to the Defense Information Systems Agency was partially redirected to the Defense Finance and Accounting Service.

Because of their sensitive nature, the deficiencies discussed in this report are presented in general terms only; specific details of the findings were separately provided to management. Although no quantifiable monetary benefits were disclosed, the audit showed that opportunities existed for improving computer security at the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency. Excluding the separate audit, the results of our audit of actions taken on the recommendations made to the Defense Information Systems Agency and the Defense Logistics Agency are summarized below and in more detail in Part I of the report.

o Controls over sensitive features of the operating systems needed improvement at the Defense Information Processing Center-Cleveland; the Defense Logistics Agency, Systems Design Center; the Defense Megacenter-Columbus; and the Defense Megacenter-Denver. As a result, application programs and data such as pay records could be added, modified, or deleted without detection (Finding A).

o Although significant improvements had been made, some additional improvements were required in security software and environmental controls at the Defense Finance and Accounting Service Denver Center; the Defense Finance and Accounting Service, Financial Systems Activity Denver; the Defense Information Processing Center-Cleveland; the Defense Megacenter-Columbus; and the Defense Megacenter-Denver. Because of these weaknesses, knowledgeable users could gain unauthorized system access or perform unauthorized tasks, and computer assets valued at over $40 million were vulnerable to damage or destruction (Finding B).

o Required system reviews, change controls, and other procedures had not been performed or developed by the Defense Finance and Accounting Service; the Defense Information Systems Agency, Western Hemisphere; and the Defense Logistics Agency, Systems Design Center. As a result, operational efficiency could be reduced, and application and operating system integrity could be compromised (Finding C).

Summary of Recommendations, Management Comments, and Audit Response. Improvements were recommended in operating system and security software, environmental controls, and management controls. The Defense Finance and Accounting Service and its Financial Systems Activity Denver concurred with the recommendations to improve physical security at one Defense megacenter and to eliminate a security exposure on one application. The Defense Information Systems Agency concurred with all recommendations, except for three with which they partially concurred and proposed alternatives. Based on the comments received, we revised one recommendation to reflect an alternative proposed by the Defense Information Systems Agency. Although the Defense Information Systems Agency generally concurred with the recommendations, its comments did not adequately respond to nine recommendations. The Defense Logistics Agency did not respond to our draft report in time for comments to be included in this final report. We request that the Defense Information Systems Agency and the Defense Logistics Agency provide comments on this report by July 31, 1995. See Part I for our response to management's comments and Part III for the complete text of the comments.

Audit Followup. Implementing the recommendations made in this report to the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency will complete the corrective actions required in response to the prior recommendations we evaluated. Recommendations made in this report will be followed up as required by DoD Directive 7650.3. Therefore, the Office of the Assistant Inspector General for Analysis and Followup plans no further separate followup actions on the prior recommendations to the Defense Information Systems Agency and the Defense Logistics Agency.

Table of Contents

Part I - Audit Results

Background

Computer Security. During FYs 1990 through 1994, the Inspector General (IG), DoD, and the Air Force Audit Agency (AFAA) performed a series of five audits to evaluate controls over operating system and security software and other general controls for computer systems supporting the Defense Finance and Accounting Service (DFAS). The audits determined that financial computer systems critical to DoD were exposed to fraud and other risks. Knowledgeable users could exploit weaknesses in the operating system controls to improperly access, add, modify, or destroy sensitive computer data, programs, and other resources (accidentally or intentionally) without risk of detection. These computer systems were operated and managed by:

o the DFAS Financial Systems Activity in Denver, Colorado (DFAS FSA Denver);

o seven organizations that report to the Defense Information Systems Agency, Western Hemisphere (DISA WESTHEM) (formerly the Defense Information Services Organization), as follows:

- the Defense Megacenters (DMCs) in Columbus, Ohio (DMC-Columbus), and Denver, Colorado (DMC-Denver); and

- the Defense Information Processing Centers (DIPCs) in Cleveland, Ohio (DIPC-Cleveland); Dayton, Ohio (DIPC-Dayton); Indianapolis, Indiana (DIPC-Indianapolis); Kansas City, Missouri (DIPC-Kansas City); and Pensacola, Florida (DIPC-Pensacola);

o the Defense Logistics Agency, Systems Design Center (DLA-DSDC), in Columbus, Ohio; and

o the Marine Corps Computer and Telecommunications Activity (MCCTA) in Quantico, Virginia.[1]

Many of the above organizations were reorganized after the original audits; in some cases, they no longer exist. For example, the DIPC-Dayton no longer exists because its workload migrated to DMC-Columbus during FY 1994. For details of these reorganizations, see Appendix F.

Congressional and DoD Oversight. Heightened concern over DoD computer security surfaced during FY 1994. As a result, the Inspector General, DoD, was asked to follow up on prior computer security audits.

[1]In September 1994, the production and test systems at the Marine Corps Computer and Telecommunications Activity, discussed in IG, DoD, Report No. 94-065, migrated to the Defense Megacenter-St. Louis.

o In April 1994, the Deputy Inspector General (IG), DoD, testified on Defense financial management issues before the Senate Governmental Affairs Committee. The Deputy IG advised the Committee that inadequate controls over computer security were among several high-risk problems requiring the immediate attention of DoD. In May 1994, the Committee Chairman requested that the IG, DoD, closely monitor DoD efforts to correct weaknesses in computer security and other financial management problems.

o Also in April 1994, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested a briefing on computer security from the IG, DoD. As a result of that briefing and directions from the Assistant Secretary, DISA created an Information Security Task Force (the DISA Task Force) to improve information systems security at all Defense megacenters and legacy sites. One of the DISA Task Force's objectives was reviewing and implementing prior audit recommendations related to computer security at those sites.

o In June 1994, the Senior Financial Management Oversight Council, chaired by the Deputy Secretary of Defense, was briefed on the computer security of DoD financial management systems. Among other actions, the Deputy Secretary of Defense directed DISA and DFAS to ensure that problems in computer security were corrected by October 1, 1994. The Deputy Secretary of Defense also stated that the IG, DoD, needed to provide oversight to ensure that compliance was improved.

Audit Request. On July 12, 1994, in response to directions from the Deputy Secretary of Defense, the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested that the IG, DoD, confirm that DFAS and DISA had corrected the previously reported problems with computer security. The IG, DoD, expanded the audit's scope to include evaluating corrective actions taken by DLA-DSDC in response to the prior IG, DoD, report, and by DMC-Denver in response to a prior Air Force Audit Agency report. The prior reports are listed in Appendix C.

This report summarizes the audit of corrective actions performed by DISA WESTHEM and DLA-DSDC in response to recommendations made to them in prior IG, DoD, and AFAA reports.[2]

Technical Terms. See Appendix B, "Glossary," for definitions of the technical terms used in this report.

[2]Corrective actions taken in response to recommendations made in IG, DoD, Reports No. 94-060 and No. 94-065 to DFAS FSA Denver and DIPC-Pensacola (formerly DFAS FSA Pensacola) were separately evaluated in IG, DoD, Project No. 4FG-5060, "Corrective Action on System and Software Security Deficiencies." Our report incorporates the results of the other audit.

Objectives

Specific Objectives. The objective of our audit was to determine whether corrective actions taken or planned by DISA WESTHEM and DLA-DSDC to improve computer security adequately responded to prior audit recommendations. Specifically, we evaluated the corrective actions taken by DISA WESTHEM, Fort Ritchie, Maryland; DIPC-Cleveland; DMC-Columbus; DMC-Denver; and DLA-DSDC. These organizations needed to take corrective action in response to recommendations made in the four reports listed in Appendix C, "Prior Audit Reports Subject to Audit Followup."

In addition, we evaluated the effectiveness of applicable management controls and each organization's implementation of DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, as it related to our audit objectives.

Revision of Audit Objectives. Audit followup was deferred on 25 recommendations made in IG, DoD, Reports No. 93-002 to DIPC-Indianapolis and No. 94-065 to DIPC-Kansas City and MCCTA. The operations of those three organizations were scheduled to migrate to two Defense megacenters during the audit. For details, see the discussion of scope limitations in Appendix A.

Finding A. Operating Systems

DIPC-Cleveland, DLA-DSDC, DMC-Columbus, and DMC-Denver had significantly improved their operating system controls. However, additional corrective actions were needed on 6 of 27 prior audit recommendations. Specifically, at DIPC-Cleveland, authorized program facility (APF) libraries and programs had not been adequately monitored, and access to the APF libraries was not adequately controlled. DLA-DSDC and DMC-Denver programmers had not eliminated all supervisor calls (SVCs) that compromised system integrity at their locations and at DIPC-Cleveland and DMC-Columbus. The APF control weaknesses resulted from shortages of system programmers and overly lenient rules for security access. Supervisor calls with integrity exposures had not been eliminated; this occurred because system programmers had underestimated the complexity of securing the supervisor calls. Also, DMC-Denver did not act on revised recommendations made by the auditors when the auditors determined that a previously recommended control technique for supervisor calls was flawed. The auditors provided alternative solutions for controlling the supervisor calls. As a result of all these weaknesses, application programs and data such as pay records could be added, modified, or deleted without detection, and the integrity of systems was not ensured. The control weaknesses over supervisor calls constitute a material management control weakness.

Operating System Function and Summary of Results

Function of Operating System. The operating system is a major component of any computer system. It is an integrated collection of computer programs, service routines, and supervisory procedures that directs the sequence and processing of computer applications (scheduling jobs, loading programs, allocating computer memory, managing files, and controlling input and output operations). The Multiple Virtual Storage (MVS) operating systems also isolate and protect individual user programs. When the operating system features are properly administered and controlled, only authorized programs can modify the processing of other programs. However, operating systems are not intended to guarantee that only authorized users can execute authorized programs. As discussed in Finding B, commercial security software packages control authorized users.

Summary of Audit Results. Prior audits at DLA-DSDC and DISA-WESTHEM organizations had identified computer security problems because of inadequate controls over the APF, SVCs, and other operating system features (Appendix D). Some of those management control weaknesses were material in nature. This followup audit determined that DIPC-Cleveland, DLA-DSDC, DMC-Columbus, and DMC-Denver had adequately implemented 21 of the 27 prior audit recommendations made to improve the operating system controls. However, additional corrective actions were required in order to

adequately implement six recommendations related to controlling APF-authorized libraries and programs and SVCs. Though still in process, the corrective actions planned on one of those six recommendations were adequate. Details of our findings are presented below and in Appendix D.

Authorized Program Facility

The DMC-Columbus, DMC-Denver, and DLA-DSDC had adequately monitored and limited access to APF libraries. However, at DIPC-Cleveland, APF libraries and programs were not adequately monitored, and update access to the APF libraries was not properly controlled. APF maintenance was not performed due to personnel shortages caused by the upcoming migration of DIPC-Cleveland's work load to DMC-Chambersburg (Pennsylvania). In addition, security personnel had applied lenient security rules to APF libraries, and had not limited the APF access of operating system personnel as they moved to other jobs. Without implementing adequate control procedures, users could create unauthorized programs in APF libraries; bypass access security; and add, modify, or delete sensitive pay and financial data files without detection.

APF Library Controls. Five nonexistent libraries and 116 different-sized, duplicate programs in 45 libraries were installed on the DIPC-Cleveland system. A nonexistent APF library may allow users to assign that APF library name to their libraries, making the libraries APF-authorized. Management control procedures normally require that only system programmers assign libraries to the APF list. Different-sized programs in different libraries could cause program errors. Reviews to identify undocumented and duplicate APF-authorized libraries and programs were not performed because of shortages of system programmers. At DIPC-Cleveland, vacancies existed because the employees in those positions had left their jobs in anticipation of the upcoming migration of computer operations from DIPC-Cleveland to DMC-Chambersburg. DIPC-Cleveland managers stated that they would review the problem after the contractor personnel were hired and trained for the vacant system programmer positions. Without adequate control procedures, users could accidentally or intentionally access, modify, or destroy information, programs, or other sensitive computer resources. Also, program errors could result.

APF Library Access. Security personnel at DIPC-Cleveland had not adequately limited update access to the APF libraries. As many as 61 user identifications (IDs) could make changes to APF libraries that could perform sensitive tasks. Security personnel stated that, in order to ensure maintainability of the operating system, update access to APF libraries was given to programmers who had vacated system programming positions, as well as their replacements. To ensure system integrity, update access to APF libraries must

be limited to the software specialist's (that is, the system programmer's) area of responsibility, as stated in the draft DISA WESTHEM Policy Letter 95-3, "Control of Access to Authorized Program Facility (APF) Library Files."

User/Vendor Supervisor Calls

Although supervisor calls provided by International Business Machines Corporation (IBM) were adequately controlled, user/vendor SVCs that were installed on systems at DIPC-Cleveland, DMC-Columbus, DMC-Denver, and DLA-DSDC compromised the integrity of the operating systems and DFAS applications. Specifically, 24 integrity exposures caused by user/vendor SVCs existed on 8 systems, which were used by DFAS payroll programs and other financial applications. System programmers secured many previously reported SVCs. However, program complexities, application rehosting, and untimely scheduling hindered system programmers' reviews and reprogramming of the SVC exposures. Also, DMC-Denver did not act on revised recommendations from the auditors when the auditors determined that the SVC control technique recommended in a prior audit report was flawed. When the prior audit was made, embedded passwords in SVCs were an accepted control technique within the computer industry. However, we later determined that the passwords could be extracted from the SVC by knowledgeable users. The application rehosting workload had decreased, allowing system programmers to work on the SVC exposures. In addition, DISA had provided good guidance for identifying SVC problems. At the conclusion of our fieldwork, the centers were implementating that guidance. Because of the integrity exposures, any knowledgeable user could bypass normal controls on the operating system and security software and could add, modify, or delete system data.

Table 1 shows the system integrity exposures caused by user/vendor SVCs.

Table 1. System Integrity Exposures Caused by User/Vendor SVCs

Organization	Number of Deficient SVCs	Number of Systems	System Integrity Exposures
DIPC-Cleveland	1[1]	1	1
DMC-Columbus	3	4	12
DMC-Denver	4[2]	2	8
DLA-DSDC	3	1	3
Total	**11**	**8**	**24**

[1]New deficiency not previously reported.
[2]Only one of these SVCs was previously reported.

DIPC-Cleveland. DIPC-Cleveland had corrected all of the SVC problems previously reported. However, a new integrity exposure existed at DIPC-Cleveland on one SVC provided with a DFAS Denver application. For details, see the discussion below of previously reported exposures at DMC-Denver. DMC-Denver system programmers planned to provide DIPC-Cleveland with a solution for the problem when they resolved the SVC integrity exposure.

DMC-Columbus. Three SVCs installed on 4 DMC-Columbus systems caused 12 system integrity exposures. However, DLA-DSDC was responsible for eliminating these integrity exposures, since DLA-DSDC provided the operating systems to DMC-Columbus. System programmers at DLA-DSDC were reviewing and reprogramming the SVC exposure problems.

DMC-Denver. Eight SVC integrity exposures existed on the two systems examined at DMC-Denver. Two of the eight were reported in AFAA Project No. 0195410, "Data Processing Center Operations and Security at the Air Force Accounting and Finance Center (AFAFC)," August 5, 1991. When these weaknesses were brought to their attention by the auditors, DMC-Denver promptly corrected four additional SVC integrity exposures (not among the eight) on the two systems.

Previously Reported Exposures. Two integrity exposures had been previously reported but still existed because DMC-Denver had not acted upon revised recommendations from the auditors that the SVC control technique (that is, embedded passwords) recommended by AFAA was flawed and should not be implemented. When the prior audit was made, embedded passwords in SVCs were an accepted control technique within the computer industry. However, the auditors later determined that the passwords could be extracted from the SVCs by knowledgeable users. Although the auditors recommended other corrective actions in discussions with management, DMC-Denver limited its corrective actions to those recommended in the AFAA report. Eliminating the two SVC exposures required reprogramming a large number of programs that used the SVCs. During the audit, system programmers at DMC-Denver began reprogramming some of those programs.

DMC-Denver provided the same SVC to DIPC-Cleveland with a DFAS application, thus compromising the integrity of one system at DIPC-Cleveland. DMC-Denver was responsible for reprogramming the application to eliminate the exposure or taking other corrective action. To resolve this problem, the IBM Executive Systems Branch at DMC-Denver will likely need application programming support from the DFAS Financial Systems Activity, Defense Joint Military Pay System Software Support Division, Denver, Colorado.

Other SVC Exposures. Four integrity exposures resulted from the use of embedded passwords in two SVCs installed on two systems. When the AFAA audit was performed, the use of embedded passwords by SVCs was accepted (and recommended by the auditors) as being an effective control technique for guarding system integrity. As discussed above, the auditors subsequently determined that the use of embedded passwords in SVCs did not safeguard system integrity because knowledgeable users could extract those passwords from the SVCs. Integrity exposures existed on the two SVCs because DMC-Denver did not develop other controls recommended by the auditors in May 1994 and on previous occasions. Upgrading system software should eliminate the four integrity exposures caused by these two SVCs.

During our audit, DMC-Denver managers said they planned to eliminate two other SVC exposures by replacing the software that used the SVC. To replace the existing software that caused the integrity exposure, DMC-Denver had ordered new vendor software that did not use an SVC. However, the system integrity was still compromised because the SVC had not been deleted from the two systems.

DLA-DSDC. DLA-DSDC had three SVC integrity exposures, all of which affected DMC-Columbus because DLA-DSDC provided the operating system to DMC-Columbus. System programmers adequately reprogrammed one of the SVCs and were evaluating the code of the other two SVCs. If needed, the Director of Security, DISA-WESTHEM, stated that he would provide contractors to assist in fixing the SVCs.

Integrity Guidelines

The DISA WESTHEM Defense megacenters and information processing centers had not fully implemented the installation integrity guidelines for MVS operating systems. The "DISA WESTHEM: Personnel and Security MVS Security Technical Implementation Standards," December 29, 1994, gave system programmers and security personnel good guidance on MVS integrity and on implementation procedures for the three major security software packages. In its DFAS Security Readiness Review, September 7, 1994, the DISA Task Force stated that using standards and procedures was one of the most effective methods of reducing the potential for integrity exposures. The DISA Task Force's report also noted that the standards must be followed and enforced. The installation integrity guidelines had not been fully implemented because the original guidelines were not issued until August 29, 1994, shortly before we began our audit. For that reason, we limited our audit to evaluating the adequacy of those guidelines. If the standards are not fully implemented, computer systems at DISA WESTHEM may continue to have their integrity compromised.

Recommendations, Management Comments, and Audit Response

Revised Recommendation. Based on the comments received, we revised Recommendation A.1.a. to be consistent with the alternative action proposed by management.

A.1. We recommend that the Commander, Defense Information Systems Agency, Western Hemisphere:

a. Rescind the draft Defense Information Systems Agency, Western Hemisphere, Policy Letter 95-3, "Control of Access to Authorized Program Facility (APF) Library Files," and incorporate its requirements in the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards."

b. Require that the Director of Security:

(1) Provide technical assistance, if requested, to the Defense Logistics Agency, Systems Design Center, Columbus, Ohio, and to the Defense Megacenter, Denver, Colorado, to solve the integrity problems caused by supervisor calls.

(2) Conduct and report on periodic quality assurance reviews on the Defense megacenters' compliance with "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards," December 29, 1994.

Management Comments. The DISA partially concurred with Recommendation A.1.a. to finalize draft Policy Letter 95-3. DISA stated that the policy letter would be rescinded. Its requirements would be incorporated in the next release of the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards," which was scheduled for August 1995. Management concurred with Recommendation A.1.b.(1) to provide technical assistance to DLA-DSDC and DMC-Denver. Management stated that technical assistance in securing SVCs was provided in response to a request from DMC-Denver. The DISA also concurred with Recommendation A.1.b.(2), stating that DISA WESTHEM had conducted compliance reviews at 16 Defense megacenters and had developed a followup process for taking corrective actions and reporting and tracking those actions. Compliance inspections will be conducted during FY 1996 without prior notice to the Defense megacenters. Also, DISA WESTHEM can provide real-time surveillance of the Defense megacenters.

Audit Response. Except in one respect, management's comments (including the proposed alternative to Recommendation A.1.a.) adequately respond to the recommendations made. We revised Recommendation A.1.a. to be consistent with the proposed alternative of incorporating draft policy guidance in "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards." Management did not fully respond to Recommendation A.1.b.(1)

to provide necessary technical assistance; they did not indicate whether they concurred with providing technical assistance to DLA-DSDC. Therefore, additional comments are requested from DISA on Recommendation A.1.b.(1).

A.2. We recommend that the Director, Defense Information Systems Agency, Western Hemisphere, Defense Information Processing Center, Cleveland, Ohio:

a. Direct the Chief, Technical Support, to review all authorized program facility libraries and programs and delete obsolete and undocumented programs.

b. Direct the Automated Information System Security Officer to review the access rules of all authorized program facility libraries and limit update access to authorized program facility datasets to the software specialist's area of responsibility, as required by "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards," revised in accordance with Recommendation A.1.a..

Management Comments. The DISA concurred with both recommendations. As suggested in Recommendation A.2.a., in April 1995, DISA WESTHEM reviewed all APF libraries and programs, and deleted obsolete and undocumented programs. In response to Recommendation A.2.b. to review APF access rules and limit update access, management stated that all DISA WESTHEM security officers will be required to review the next release of the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards," scheduled for release in August 1995.

Audit Response. Management comments adequately responded to Recommendation A.2.a. to delete obsolete and undocumented programs. However, management comments did not adequately respond to Recommendation A.2.b. to review access rules and limit update access to APF libraries and datasets at DIPC-Cleveland. Requiring DIPC-Cleveland and all other DISA WESTHEM security officers to review the next release of the MVS technical implementation standards is a necessary step in furthering compliance with those standards. However, when we recommended that access rules be reviewed, we were referring to the manner in which access was defined in the security software, not to written access rules such as the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards." Also, management's comments did not describe the actions taken or planned at DIPC-Cleveland to actually limit update access to APF datasets to the system programmer's area of responsibility. Therefore, additional comments are requested from DISA on Recommendation A.2.b.

A.3. We recommend that the Commander, Defense Logistics Agency, Systems Design Center, require the Director, Information Systems (Technology), to:

a. Develop and implement adequate controls over supervisor calls with integrity exposures in accordance with integrity guidelines. If

required, technical assistance in implementing these controls should be requested from the Director of Security, Defense Information Systems Agency, Western Hemisphere.

b. Export the corrected supervisor calls to the Defense Megacenter, Columbus, Ohio.

Management Comments. The Defense Logistics Agency did not respond to the draft of this report in time for the comments to be included in this final report. The comments we received will apply to the final report unless we receive an additional response.

A.4. We recommend that the Director, Defense Information Systems Agency, Western Hemisphere, Defense Megacenter-Denver, direct the Chief, IBM Executive Systems Branch, to:

a. Make the appropriate changes required to eliminate the integrity exposures existing on the four supervisor calls.

b. Request appropriate programming assistance from the Chief, Joint Military Pay System Software Support Division, at the Defense Finance and Accounting Service Financial Systems Activity, Denver, Colorado, in solving the problems with supervisor calls at the Defense Megacenter, Denver, Colorado, and at the Defense Information Processing Center, Cleveland, Ohio.

c. Export the corrected supervisor call to the Defense Information Processing Center, Cleveland, Ohio.

Management Comments. The DISA concurred with all three recommendations, stating that DMC-Denver was prioritizing the systems for making the changes. Management stated, "While all SVCs are being reviewed, the required work to adequately comply with the recommendations on SVC [number deleted], we estimate a completion date of 31 May 1996." Management noted that some corrective actions depend on the availability of support from DFAS FSA Denver. DMC-Denver stated that corrective actions will not be taken with respect to the SVC exposures on System B because that system will be eliminated by December 31, 1995.

Audit Response. Management comments did not adequately respond to Recommendations A.4.a., b., and c.; the comments were incomplete and vague. Additional management comments on this final report are requested, for the reasons stated below.

o In response to Recommendation A.4.a. concerning the four SVCs at DMC-Denver, management did not clearly indicate whether corrective actions would be completed by May 31, 1996, on the one SVC identified in the comments or on all four SVCs identified in the audit recommendation. DMC-Denver officials told us that the integrity exposures on three SVCs identified by the audit had been eliminated; however, the exposure caused by the remaining SVC will not be eliminated until May 31, 1996. In addition, management did

not provide specific actions and completion dates for eliminating the integrity exposures on all four SVCs. We agree with management that corrective action is not necessary on System B, since it will soon be eliminated.

o Regarding Recommendation A.4.b. to request programming assistance from DFAS FSA Denver, although DISA noted its need for support from that organization, DISA did not indicate whether assistance had been requested or give completion dates.

o Management comments did not state what actions were planned or taken, or give related completion dates on Recommendation A.4.c. to export the corrected SVC to DIPC-Cleveland.

Management Comments Required

Management is requested to comment on the items indicated with an X in Table 2.

Table 2. Management Comments Required on Finding A.

Recommendation Number	Organization	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issues
A.1.b.(1)	DISA	X	X	X	None
A.2.b.	DISA		X	X	None
A.4.a., b., c.	DISA		X	X	None

Finding B. Security Software and Environmental Controls

The DIPC-Cleveland, DMC-Columbus, DMC-Denver, and DLA-DSDC had significantly improved their security software and environmental controls. However, DMC-Columbus, DMC-Denver, and DIPC-Cleveland needed to take additional corrective actions on 6 of 36 prior audit recommendations:

o DMC-Denver did not have effective controls over bypass label processing (BLP) and the use of one special privilege attribute of the Computer Associates, Inc., TOP SECRET (CA-TOP SECRET) security software. This occurred because of a technical oversight in the BLP control technique and because the security personnel were unfamiliar with certain aspects of the special privilege.

o At DIPC-Cleveland, sensitive utilities were not adequately controlled because of personnel shortages and implementation problems.

o At DIPC-Cleveland, DMC-Columbus, and DMC-Denver, autoerase and erase-on-delete features had not been activated because of the adverse impact on operations. Although requested by the DISA WESTHEM security officer, a waiver of this security requirement was still under review by the Chief Information Officer, DISA, and had not been granted.

DFAS Denver also needed to take corrective actions to reduce the risk of water damage at DMC-Denver. The IG, DoD, previously recommended that DMC-Denver install overhead water shutoff valves. However, as a tenant at DFAS Denver, DMC-Denver was not responsible for making such building modifications. The recommendation was redirected to DFAS Denver. Corrective action by DFAS Denver was delayed because funding was not immediately available and the work had to be scheduled.

By improper use or setup of CA-TOP SECRET and CA-Access Control Facility 2 (CA-ACF2) security software, Defense megacenters increase the risk that knowledgeable users may gain unauthorized access or perform unauthorized tasks. Inadequate environmental controls make computer assets at DMC-Denver, valued at over $40 million, more vulnerable to accidental or deliberate damage or destruction.

Security Software Function and Summary of Results

Function of Security Software. Security software is used to protect computer resources such as files, programs, tapes, database definitions, libraries, readers, and processing capabilities. The security software used by DIPC-Cleveland is

known as CA-ACF2. DMC-Denver used CA-TOP SECRET security software. DLA-DSDC and DMC-Columbus used IBM software known as Resource Access Control Facility (RACF).

CA-TOP SECRET, CA-ACF2, and RACF security software offer a variety of control options and features to enhance system security. The control options and features of the security software should be set for the level of security needed. The level of protection achieved depends on how well the options and features of CA-TOP SECRET, CA-ACF2, and RACF are administered.

Summary of Audit Results. In prior audits, the AFAA and the IG, DoD, identified computer security problems at DLA-DSDC and DISA WESTHEM organizations. The problems were caused by inadequate controls over security software and weaknesses in environmental controls (Appendixes C and D). Some of these management control weaknesses were material in nature.

This followup audit determined that 30 of the 36 prior audit recommendations made to improve security software and environmental controls had been adequately implemented. DLA-DSDC implemented all seven recommendations made to them. All but 6 of the 29 recommendations addressed to DIPC-Cleveland, DMC-Columbus, and DMC-Denver had been adequately implemented. Though still in process, the corrective actions planned on three of the six recommendations were adequate. To implement our prior audit recommendations, corrective actions were also required from DFAS Denver and DFAS FSA Denver. Details of our findings are presented below and in Appendix D.

Security Software

As detailed in Part I (Background) of the report, as the result of heightened concern over computer security, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) required the Director, DISA, to establish a DISA Task Force to improve information systems security at all Defense megacenters and legacy sites. One objective of the DISA Task Force was to review and implement prior audit recommendations related to computer security at those sites. The DISA Task Force did not specifically address the recommendations made to DMC-Denver in the AFAA report that is included in the scope of this followup audit (Appendix C). However, many of the problem areas discussed in the AFAA report were covered by the DISA Task Force's review, which had a much larger scope than the previous audits. When the DISA Defense megacenters and legacy sites implement all of the DISA Task Force's recommendations, overall physical and computer security will be much improved. We commend DISA for the formation of the DISA Task Force to redress the problems identified.

Despite the significant strides made by DISA WESTHEM organizations in improving controls over security software, this followup audit determined that additional corrective actions were required, as discussed below.

Bypass Label Processing (BLP). DMC-Denver had implemented reasonable BLP control. However, in implementing the selected control technique, DMC-Denver allowed more access than intended because of a technical oversight. This exposure existed for 21 user IDs and 19 batch IDs. The batch IDs are production applications that need BLP. BLP is used when nonstandard tapes are sent to a data center for processing, and tape security has to be bypassed. Because of the technical oversight, these user IDs and batch IDs had read and write access to all files, not just tape files. After we notified the DMC-Denver Automated Information System (AIS) Security Officer, he developed a different approach that will resolve the exposure. DMC-Denver security personnel were making the correction. Instead of using a special ID to control BLP, the AIS Security Officer will use a security profile. The DISA Task Force also identified a BLP problem related to the "ALL" record and was monitoring the corrective actions taken.

Special Privilege Attributes. Except for one attribute, DMC-Denver controlled the use of special privilege attributes. The CA-TOP SECRET NOSUBCHK attribute used in conjunction with one major application presented a security exposure. NOSUBCHK allows one user to use another user's ID without permission. We discussed this security exposure with the AIS Security Officer and technical support personnel. The AIS Security Officer was unaware of this exposure. Eliminating this exposure will require action by DFAS FSA Denver and by security personnel at DMC-Denver.

Autoerase. The autoerase and erase-on-delete features at DMC-Columbus, DMC-Denver, and DIPC-Cleveland were not activated because doing so would have adversely affected operational efficiency. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988, requires all AIS that process sensitive unclassified information requiring controlled access protection to have C2 security classifications. For C2 controlled access protection, DoD Standard 5200.28, "DoD Trusted Computer System Evaluation Criteria," December 1985, requires that:

- o all computer files be protected,
- o residual information be erased from on-line disk devices, and
- o jobs entered through job entry subsystem 2 (JES2) be checked for a valid logon ID and password.

On February 3, 1995, the Security Officer at DISA WESTHEM asked the Chief Information Officer, DISA, to waive the requirement for the erasure of residual information. DISA WESTHEM documented two tests that showed the degradation of service that occurred when autoerase and erase-on-delete were activated. DoD Directive 5200.28 allows exceptions to C2 security requirements when computer operations are adversely affected. However, the waiver was still under review by the Chief Information Officer, DISA, and had not been granted. Because of the adverse impact on operations, we agree that this C2 requirement should be waived.

Sensitive Utilities. DIPC-Cleveland had not adequately controlled its sensitive utility programs due to personnel shortages and technical problems in controlling the utilities with the CA-ACF2 security software. Because DIPC-Cleveland's work load was scheduled to move to DMC-Chambersburg in August 1995, numerous personnel had transferred or taken new jobs. Controlling sensitive utilities through the CA-ACF2 protected program list also presented certain technical limitations. Certain users require access to some but not all sensitive utilities. However, user access cannot be restricted only to selected utilities using the CA-ACF2 protected program list. If a user has access to that list, then the user has access to all utilities in the list. In order to be selective, utility programs can also be protected by moving them to a separate library and writing appropriate access rules. Since some personnel need access only to selected utilities, a combination of special access rules and the protected program list would have to be used. The DISA Task Force also stated that sensitive utilities had not been controlled.

Environmental Controls

At DMC-Denver, overhead water shutoff valves had not been installed in the computer room.[3] As a tenant organization at DFAS Denver, DMC-Denver could not install the overhead shutoff valves because doing so was the responsibility of DFAS Denver. Accordingly, we redirected the audit recommendation to DFAS Denver. DFAS Denver concurred and planned to install the overhead water shutoff valves in FY 1995. Installation of the valves was delayed while obtaining funds and scheduling the building modifications. Until the overhead water shutoff valves are installed at DMC-Denver, computer assets valued at over $40 million are more vulnerable to accidental or deliberate damage or destruction.

Summary

Because security software was not properly implemented, the DIPC and DMC systems were subject to increased risk that knowledgeable users might gain unauthorized access and perform unauthorized tasks. Computer assets valued at over $40 million at DMC-Denver were exposed to increased risk of damage or destruction. DISA WESTHEM, DMC-Denver, DIPC-Cleveland, and DFAS Denver had substantially improved computer security. Management needed to resolve these problems previously identified.

---

[3]In Recommendation D.1. of Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994, the IG, DoD, recommended that DMC-Denver install those valves. Heat detectors were also recommended for DMC-Denver. However, based on the DISA Task Force's review at DMC-Denver, we are no longer making that recommendation because the heat detectors would be of limited value.

Recommendations, Management Comments, and Audit Response

B.1. We recommend that the Director, Defense Information Systems Agency, Western Hemisphere, Defense Megacenter, Denver, Colorado, direct the Automated Information System Security Officer to:

a. Implement bypass label processing control that limits access to tape files.

b. Remove the NOSUBCHK special privilege attribute from system software that supports Defense Finance and Accounting Service applications.

Management Comments. The DISA concurred with both recommendations, stating that bypass label processing was reviewed and corrective action was completed in April 1995. After certain changes are made in vendor software, DISA WESTHEM will remove the NOSUBCHK attribute from system software supporting DFAS applications by December 1995.

B.2. We recommend that the Director, Defense Finance and Accounting Service, Denver Center, require the Director, Directorate of Support Services, at the Defense Finance and Accounting Service, Denver Center, to install overhead shutoff valves in the computer room at the Defense Megacenter, Denver, Colorado.

Management Comments. The DFAS concurred, stating that contracting actions for the design and installation of the overhead shutoff valves should be completed by March 1997.

B.3. We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado, modify the application code to allow the removal of the NOSUBCHK special privilege attribute.

Management Comments. The DFAS concurred, stating that the Integrated Data Management System programs using the NOSUBCHK attribute had been identified. The programming effort to remove the NOSUBCHK attribute had been tested. We were told that corrective actions were completed on May 1, 1995.

B.4. We recommend that the Director, Defense Information Systems Agency, Western Hemisphere, Defense Information Processing Center, Cleveland, Ohio, direct the Automated Information System Security Officer to control sensitive utilities by implementing the protected program list and the special access rules feature of Computer Associates, Inc., Access Control Facility 2 security software.

Management Comments. The DISA concurred, stating that the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation

Standards," published in December 1994, explains how to secure sensitive utilities for each security control product. These standards were distributed to each Defense megacenter for implementation.

Audit Response. Management comments did not fully respond to the recommendation. In publishing the new standards, DISA WESTHEM established excellent written criteria for each Defense megacenter to follow in securing sensitive utilities. However, management's comments did not give actions completed or planned and related completion dates for implementing the DISA WESTHEM standards at DIPC-Cleveland. Our audit showed that weaknesses existed in the controls over sensitive utilities at DIPC-Cleveland. Additional comments are requested from DISA on Recommendation B.4.

B.5. We recommend that the Chief Information Officer, Defense Information Systems Agency, approve the request from the Security Officer at the Defense Information Systems Agency, Western Hemisphere, to waive the C2 requirement for autoerase and erase-on-delete at all Defense megacenters.

Management Comments. The DISA partially concurred with the recommendation because management was exploring alternatives to waiving the C2 requirements for autoerase and erase-on-delete. The DISA WESTHEM security office will provide its action plan to DISA by June 30, 1995.

Audit Response. We applaud management's efforts to fully implement the C2 security requirements of DoD Directive 5200.28. DISA should provide additional comments describing planned actions, including alternatives, and should give estimated completion dates.

Management Comments Required

Management is requested to comment on the items indicated with an X in Table 3.

Table 3. Management Comments Required on Finding B.

Recommendation Number	Organization	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issues
B.4.	DISA		X	X	None
B.5.	DISA	X	X	X	None

Finding C. Management Controls

The DMC-Columbus, DLA-DSDC, and DISA WESTHEM had made significant progress in strengthening management controls. However, those organizations still needed to correct 8 of 16 control weaknesses identified in prior audits.

o The DMC-Columbus did not perform required recertification reviews of its computer systems.

o The DLA-DSDC had not developed or implemented formal procedures for controlling changes to the operating system.

o The DISA WESTHEM had not fully developed the recommended procedures related to controlling contractors who needed system access at the Defense megacenters, automated data processing (ADP) equipment contracts, and abnormal endings (ABENDS) to computer operations.

Organizational realignments and higher priorities affecting DMC-Columbus and DISA WESTHEM caused delays in meeting the requirements of prior recommendations. DLA-DSDC did not have adequate personnel resources with subject-matter expertise available to develop procedures for controlling changes to operating systems. The Director, DISA WESTHEM, relied on individual computer centers to develop quality assurance programs for the oversight of ADP equipment contracts and ABENDS; however, adequate corrective action had not been taken at the sites we reviewed. Unless strict management controls are implemented, application and operating system integrity may be compromised.

Required Controls and Summary of Results

Required Management Controls. To enhance the security of operating systems, management controls should include sensitivity ratings and background investigations for system programmers, management of their programming functions, a change control system, and off-site maintenance of operating system software. Strict management controls are needed to ensure that program maintenance responsibilities are properly assigned, that programmer positions have the proper sensitivity designations, that change control procedures are consistent and properly applied, and that a backup of the operating system software is stored off-site.

Summary of Audit Results. Prior audits by the AFAA and the IG, DoD, identified computer security problems at DLA-DSDC and the three DISA WESTHEM organizations that occurred because of inadequate management controls (Appendixes C and D). Some of these management control weaknesses were material in nature, but had since been corrected.

This followup audit determined that DISA WESTHEM, DLA-DSDC, DMC-Columbus, and DMC-Denver had adequately implemented 8 of the 16 prior audit recommendations made to improve controls over system programmers and other

general controls. DMC-Denver had adequately implemented all of the prior recommendations. However, additional corrective actions were required by DISA WESTHEM organizations and DLA-DSDC to adequately implement eight recommendations related to controls over contractor oversight, recertification reviews, quality assurance programs, and change control procedures. Though still in process, the corrective action planned on one of those eight recommendations was considered adequate. Details of our findings are presented below and in Appendix D.

Recertification Review

The DMC-Columbus had not performed the recertification reviews of the organization's computer systems required by Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," December 1985. Periodic recertification reviews are an important means of ensuring that adequate security measures are in place on computer systems. This was especially true within DISA WESTHEM because computer operations at the legacy sites were migrating to the Defense megacenters. This condition had existed since 1987 and was last reported in IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994. A similar finding was reported in IG, DoD, Report No. 89-058, "Management of Access Controls to Computers at the Defense Logistics Agency," March 14, 1989. The Office of Management and Budget guidance states, "Agencies shall conduct periodic audits or reviews of sensitive applications and recertify the adequacy of security safeguards. Audits or reviews and recertifications shall be performed at least every three years." DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988, requires the analysis and selection of appropriate, cost-effective security measures to achieve and maintain a minimum level of protection.

Management acknowledged the requirement; however, the recertification review was not performed because the priority assigned was not high enough due to system migrations and organization realignments that were taking place. Since these significant changes affected the security posture of the automated information systems at DMC-Columbus, an interim authority to operate for an unspecified period of time was issued by the appointed Designated Approving Authority, the Director, Defense Information Services Organization (now DISA WESTHEM). The interim authority to operate is not a waiver of the requirement for recertification; however, DISA Instruction 630-230-19, "Security Requirements for Automated Information Systems (AIS)," August 1991, states that an interim authority to operate can be granted for a fixed period of time if the Designated Approving Authority is willing to accept all risks. While continuing the recertification process, the interim authority to operate permits the activity to meet its operational mission requirements while improving its AIS security posture.

Unless the required recertification review is performed and accepted, management is not assured that the level of risk has been adequately defined or reduced to an acceptable level for operational requirements.

Change Control Procedures

Formal, written procedures controlling changes to the Multiple Virtual Storage operating system had not been developed or implemented by DLA-DSDC, as previously recommended. As the only central design activity for DLA, the DLA-DSDC Office of Computer Systems Support is responsible for establishing and maintaining an ADP operating environment that supports DLA-DSDC and its fee-for-service customers.

Corrective action on this recommendation was initially delayed due to the unavailability of resources with subject-matter expertise appropriate for the project. However, the Commander, DLA-DSDC, recognized the immediate need to improve the change control procedures for operating system maintenance and elevated the priority placed on the project. As a result, the "DLA-DSDC Configuration Management Release Procedure" document is currently being prepared.

Since any software change can have dramatic and unexpected effects, changes must be properly defined, planned, coordinated, tested, and implemented. Improper control of operating system changes could allow the introduction of unauthorized or inaccurate computer programs that could compromise the integrity of the operating system.

Contractor Oversight and Control

DISA WESTHEM had not finalized guidance for control and oversight of contractor personnel requiring system access at the Defense megacenters. A DISA WESTHEM Policy Letter 95-4, "Security Guidance for DISA WESTHEM Automated Information System (AIS) Contracts," on security issues for AIS contractors, was being prepared. However, corrective action will not be complete until the guidelines are finalized and implemented at the DISA WESTHEM Defense megacenters. The delay was attributed to continued realignments at DISA WESTHEM.

To protect programs and data from improper changes, direct contractor access to the operating system and system software must be restricted and fully documented.

Quality Assurance Programs

Abnormal Endings to Computer Operations. The Commander, DISA WESTHEM, had not established an in-house quality assurance program to track, analyze, and prevent ABENDS due to repetitive causes. Rather than establishing a DISA WESTHEM procedure, the Commander, DISA WESTHEM, relied on the computer centers to implement the recommendation at their respective sites. Some corrective actions were taken at the individual computer centers. However, establishing and implementing a DISA WESTHEM procedure would help ensure that all Defense megacenters followed the required control procedures.

Without effective controls over ABENDS, DISA WESTHEM will continue to incur unnecessary system downtime, response time will be increased, and production schedules will be missed.

Automated Data Processing Equipment Maintenance. The Commander, DISA WESTHEM, had not established an in-house quality assurance program over the maintenance performed under ADP equipment contracts. This was recommended to make sure that preventive and remedial maintenance services were:

- o scheduled and approved in advance by DISA WESTHEM managers,
- o adequately documented when provided,
- o verified to contract terms before payment, and
- o certified as received only when there was evidence that the services were actually received.

Instead of issuing a DISA WESTHEM procedure, the Commander, DISA WESTHEM, relied on the computer centers to implement the recommendation. Some corrective action was taken by those computer centers. However, establishing and implementing a DISA WESTHEM procedure would ensure that all Defense megacenters followed the required control procedures. If vendor maintenance services are not adequately or effectively monitored, the Government can incur unnecessary costs.

Recommendations, Management Comments, and Audit Response

C.1. We recommend that the Commander, Defense Information Systems Agency, Western Hemisphere:

a. Direct the Director, Defense Information Systems Agency, Defense Megacenter, Columbus, Ohio, to complete by July 1995 the recertification review of the organization's computer systems, as required by the Office of Management and Budget Circular No. A-130.

b. Finalize the Defense Information Systems Agency, Western Hemisphere, Policy Letter 95-4, "Security Guidance for DISA WESTHEM Automated Information System (AIS) Contracts."

c. Establish an in-house quality assurance program to track and analyze the causes of abnormal endings to computer operations and prevent abnormal endings due to repetitive causes.

d. Establish an in-house quality assurance program over the maintenance performed under automated data processing equipment contracts. The procedure should require:

(1) Contracting personnel to schedule and approve preventive maintenance in advance. Both suggested and approved schedules should be documented in the contract files by the contracting personnel.

(2) Computer operators at the Defense Information Systems Agency, Western Hemisphere, Defense megacenters to maintain adequate documentation on actual preventive and remedial services performed.

(3) Contracting personnel to verify, before authorizing payments to vendors, that the billings by vendors (including appropriate credits) for preventive and remedial maintenance are prepared in accordance with contract terms.

(4) Managers at the Defense Information Systems Agency, Western Hemisphere, to certify that they received preventive maintenance or remedial maintenance services based on evidence that the services were received.

Management Comments. The DISA concurred with Recommendations C.1.a. and C.1.c. stating that the recertification review at DMC-Columbus will be completed by July 1995, and an in-house procedure for controlling ABENDS through quarterly analyses is being prepared and should be completed by October 1996.

Management partially concurred with Recommendation C.1.b. to finalize policy guidance on security for AIS contracts. As an alternative, the guidance in the policy letter will be incorporated into security procedures by August 1995.

DISA concurred with Recommendation C.1.d., stating that corrective actions were implemented on February 17, 1995, in response to findings reported in IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994. Management stated, "All DMCs have the corrective action and are to be implementing the procedures to establish an in-house quality assurance program over the maintenance performed under ADPE contracts. This corrective action will be included in the comprehensive internal management control program (IMCP) package DISA WESTHEM is developing for all assessable units. Estimated completion date of the DISA WESTHEM IMCP, which will incorporate the quality assurance program, is November 1995."

Audit Response. Management comments adequately responded to all but two recommendations. Management did not identify the specific security procedures that would, as an alternative to Recommendation C.1.b., be revised to incorporate security guidance on AIS contracts.

Management comments on Recommendation C.1.d., related to contract maintenance on ADP equipment, did not clearly describe the corrective actions taken or planned and give completion dates. Management's reference to the Defense megacenters' implementation of a procedure for the quality assurance program did not clearly explain what that procedure required or what organizational level issued the procedure. We are concerned because the absence of a procedure applicable to all DISA WESTHEM

organizations may result in adequate controls not being implemented at all Defense megacenters. Adequate corrective actions had not been taken when management previously relied on individual organizations to implement this recommendation. Additional comments are requested from DISA on Recommendation C.1.b. and d.

C.2. We recommend that the Commander, Defense Logistics Agency, Systems Design Center, finalize procedures for change management:

a. To control the processing of all changes to the Multiple Virtual Storage operating system at the Defense Logistics Agency, Systems Design Center, and

b. To control the export of these changes to their customers.

Management Comments. The Defense Logistics Agency did not respond to the draft of this report in time for the comments to be included in this final report. The comments we received will apply to the final report unless we receive an additional response.

Management Comments Required

Management is requested to comment on the items indicated with an X in Table 4.

Table 4. Management Comments Required on Finding C.

Recommendation Number	Organization	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issues
C.1.b., d.	DISA		X	X	None

This page was left out of orignial document

Part II - Additional Information

Appendix A. Scope and Methodology

Scope and Methodology

Methodology. We examined operating system features that can affect the integrity of operating system and security software. Those operating system features were the authorized program facility; supervisor calls; the time share option; the program properties table; the job entry subsystem 2; and sensitive utilities. We also examined the implementation of the CA-TOP SECRET, CA-ACF2, and RACF security software. The other general controls examined included controls over:

- o sensitive programmer positions,
- o changes to operating system software and user passwords,
- o physical security, and
- o the efficiency of computer operations.

Scope Limitations. As detailed in Appendix D, we did not evaluate the corrective actions taken in response to 24 recommendations made in IG, DoD, Reports No. 93-002 and No. 94-065 to the MCCTA, to DIPC-Indianapolis, and to DIPC-Kansas City. The work load of those three organizations was migrating to DMC-Denver and DMC-St. Louis during the audit. Therefore, we plan a separate followup audit at the two Defense megacenters after the work load migrations are completed.

Computer-Processed Data Used. To achieve the audit objectives, we relied on computer-processed data in the operating system libraries and the security software of each organization. We used Computer Associates, Inc., EXAMINE (CA-EXAMINE) auditing software to extract data directly from computer memory and operating system libraries. The CA-EXAMINE software program audits Multiple Virtual Storage operating systems. We used automated and manual techniques to analyze system data. For example, to test security rules and features, we used the audit features of three security software packages: CA-TOP SECRET, CA-ACF2, and RACF. To test operating system features, we used the same terminals that are normally used to gain access to system resources. All system testing and use of audit software were done in a controlled environment with management's approval. Based on those tests and assessments, we concluded that the data were sufficiently reliable to be used in meeting the audit objectives.

Organizations Visited, Time Period, and Standards. We performed audit work at DFAS FSA Denver; Headquarters, DISA WESTHEM; DIPC-Cleveland; DLA-DSDC; DMC-Columbus; and DMC-Denver. The audit at DMC-Columbus included followup on recommendations made to the DIPC-Dayton, whose function migrated to DMC-Columbus.

This program audit was performed from September 12, 1994, through January 23, 1995, except for limited analyses of post-audit corrective actions. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD, and accordingly included such tests of management controls as were considered necessary. During the audit, we visited or contacted the organizations shown in Appendix F.

Management Control Program

DoD Directive 50010.38, "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. We reviewed the adequacy of management controls over sensitive features of the operating system and security software and other general controls at DLA-DSDC and three DISA WESTHEM organizations: DIPC-Cleveland, DMC-Columbus, and DMC-Denver. We evaluated the implementation of the DoD management control program (the Program) at DLA-DSDC. However, we did not review the Program's implementation at the three DISA WESTHEM organizations because an ongoing audit determined that DISA WESTHEM had improperly defined their assessable units in FY 1994.* The 16 Defense megacenters were treated as a single assessable unit (computer operations) during FY 1994. Doing so was not reasonable because these Defense megacenters represented the majority of the mission and resources of DISA WESTHEM. To correct this problem, DISA WESTHEM designated each Defense megacenter as an assessable unit during FY 1995.

Adequacy of Management Controls. The followup audit at each organization evaluated management controls over the operating system and security software and other general controls. Material management control weaknesses, as defined by Office of Management and Budget Circular No. A-123 and DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, existed at DIPC-Cleveland, DLA-DSDC, DMC-Columbus, and DMC-Denver in their general controls over supervisor calls. Inadequate controls over these sensitive features of the operating system made it possible for knowledgeable users to improperly access, modify, or destroy sensitive computer data and programs without detection. Implementing Recommendations A.1.b.(1), A.1.b.(2), A.3.a., A.3.b., A.4.a., A.4.b., and A.4.c. will correct the material weakness in controls over supervisor calls on the operating system. See Part I (Finding A) of this report for details. As shown in Appendix E, strengthened management controls and other nonmonetary benefits will be realized from

*The DISA WESTHEM management control program was being reviewed under IG, DoD, Project No. 4RE-2005.01, "Internal Management Control Program, Defense Information Systems Agency, Western Hemisphere."

implementing the recommendations. A copy of the report will be provided to the senior official responsible for management controls in the Defense Information Systems Agency and the Defense Logistics Agency.

Reporting Process. Though not significant, the audit determined that opportunities existed for improving the reporting process for the management control program at DISA WESTHEM and DLA-DSDC. Neither organization reported to its headquarters all of the material weaknesses that existed. Specifically, DISA WESTHEM did not report material management control weaknesses identified in two IG, DoD, reports:

o A material weakness in the controls over passwords at DMC-Columbus was identified in IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994.

o Material weaknesses in the controls over operating system and security software and other management controls at DIPC-Kansas City (then the Defense Information Systems Organization, Information Processing Center, Kansas City) were identified in IG, DoD, Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994.

Likewise, DLA-DSDC did not report material weaknesses identified in the controls over operating system and security software by IG, DoD, Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993.

DoD Directive 5010.38 requires Defense agencies and other DoD Components to submit an Annual Statement of Assurance on management controls. Intended for Congress, the statement should explain how the management controls were evaluated. It should disclose all material weaknesses in the reporting year, including those corrected in the reporting year and those carried forward from prior years. The material management control weaknesses identified by the IG, DoD, were not reported by DISA WESTHEM because management decided that reporting requirements were met in FY 1993 when similar weaknesses were reported at other DISA WESTHEM organizations. At DLA-DSDC, the material weaknesses were not reported because the responsible manager thought the weaknesses could be corrected before the end of the reporting period and was not aware that those weaknesses should still be reported. Because all material weaknesses were not reported by DISA WESTHEM and DLA-DSDC, their headquarters were not given opportunities to determine whether those weaknesses should have been included in the reports submitted for possible inclusion in the annual report submitted to Congress by the Secretary of Defense.

Prior Audits and Other Reviews

Prior IG, DoD, and AFAA audits determined that financial computer systems critical to DoD were exposed to fraud and other risks. Knowledgeable users could exploit weaknesses in the operating system and security software and other general controls to improperly access, add, modify, or destroy sensitive computer data, programs, and other resources (accidentally or intentionally) without risk of detection. The reports issued on these prior audits and the audit followup made in this and other IG, DoD, audits is discussed below.

AFAA Report, "Data Processing Center (DPC) Operations and Security at the Air Force Accounting and Finance Center (AFAFC) (Project No. 0195410)," August 5, 1991. The report identified weaknesses in the controls over operating system and security software at the finance center. We followed up on all prior recommendations made to improve the security of the computer center (now DMC-Denver) of the Air Force Accounting and Finance Center.

IG, DoD, Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992. The report identified weaknesses in the controls over the operating system and security software and in operating system maintenance at two DISA organizations. We followed up on all prior recommendations made to improve security at DIPC-Cleveland. Followup on the recommendations made to the DIPC-Indianapolis is being performed at DMC-Denver under IG, DoD, Project No. 5FD-5026, "Followup Audit of Controls Over Operating System and Security Software and General Controls of the Computer Systems Supporting the Defense Finance and Accounting Service."

IG, DoD, Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993. The report also identified weaknesses at DLA-DSDC and two DISA organizations in controls over operating system and security software and in operating system maintenance. We followed up at DLA-DSDC and DMC-Columbus on all prior audit recommendations to improve computer security.

IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994. The report identified weaknesses at three DISA organizations in controls over abnormal endings to computer operations; ADP equipment maintenance and security oversight; access to sensitive computer assets; and potential environmental hazards. Weaknesses in change control procedures at DFAS FSA Denver were also identified. Followup was performed on the prior recommendations made to improve computer security at DMC-Columbus and DMC-Denver. However, we determined that followup was no longer viable on recommendations to DIPC-Indianapolis to make structural improvements or revise operating procedures. Such recommendations were made obsolete when the DIPC-Indianapolis work load was consolidated at

DMC-Denver. Followup on recommendations made to DIPC-Pensacola (formerly DFAS FSA Pensacola) is being performed under IG, DoD, Project No. 4FG-5060, "Corrective Action on System and Software Security Deficiencies."

IG, DoD, Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994. The report identified weaknesses in the controls over operating system and security software and in operating system maintenance at two Marine Corps and two DISA organizations. Followup on the recommendations made to DIPC-Kansas City, MCCTA, and MCCTA Worldwide Support Division is being made at DMC-St. Louis under IG, DoD, Project No. 5FD-5026. Followup on recommendations made to DIPC-Pensacola (formerly DFAS FSA Pensacola) is being made under IG, DoD, Project 4FG-5060.

IG, DoD, Report No. 95-066, "Controls Over Application Software Supporting the Navy's Inventories Held for Sale (Net)," December 30, 1994. The report identified weaknesses in the controls over operating system and security software, and in the integrated data management system data base at DMC-Mechanicsburg (Pennsylvania) and the Naval Supply Systems Command, Ships Parts Control Center. We did not follow up on the recommendations made in the prior report because the report had not been issued at the time this audit was requested.

Appendix B. Glossary

Access control is a general term used to describe a number of techniques that restrict users of a computer system from gaining access to the system or each others' data, or from performing unauthorized actions. When applied to software, access control usually refers to one of the specialized software security packages, such as RACF security software.

APF is an authorized program facility. It is an IBM mechanism for protecting the integrity and security of the MVS operating system. It provides for the orderly, controlled extension of the operating system by defining special program libraries that may contain programs that are authorized to execute in the supervisor state. APF-authorized programs have the potential to bypass all security controls.

Only properly authorized programs should be allowed to perform sensitive tasks such as accessing or modifying another program's execution or data areas. A program that can perform sensitive functions outside of established APF rules can become part of the operating system, and can circumvent or disable all security mechanisms, alter audit trails, or modify any computerized data, regardless of the presence of access control software.

According to IBM's MVS security manual, APF procedures should require system programmers to use security software to control the creation of and access to APF libraries and the creation of APF programs. All APF programs should have unique names to prevent mix-ups in processing, and the file containing the names of APF libraries and volume serial numbers (disk device numbers) should reflect only valid libraries and volume serial numbers. Failure to comply with these IBM guidelines can introduce significant integrity exposures to the operating system, and can lessen management's control over system software.

Application programs are programs that are intended to serve particular business or nonbusiness needs and have specific input, processing, and output activities. For example, accounts receivable, general ledger, payroll, and personnel programs are some types of application programs.

Assembler language is the fundamental, low-level language of the IBM 370 series of computers.

Bypass label processing is a process that bypasses tape security when nonstandard tapes are being processed. It positions the tape to the specified file without checking for volume or dataset labels.

Change control system is a formal procedure for management to approve and control changes to operating system programs and to track the status of those changes.

Designated Approving Authority is responsible for reviewing and approving security safeguards for automated information systems, and for issuing accreditation statements for each system under his/her jurisdiction.

Data base is a collection of interrelated data stored together.

Disk is a data storage device that allows data to be accessed randomly or sequentially without passing through unwanted data.

Embedded passwords are passwords that are coded into a program.

Erase on Delete is a RACF security feature that overwrites file data when the file has been deleted. It is a requirement for the C2 security level.

File is a collection of related data records stored on an external storage medium, usually a disk or tape.

Job entry subsystem 2 (JES2) is one of two IBM job management routines that reads the job stream and assigns jobs to class queues (computer data or programs awaiting processing). The other job management routine is JES3. JES2 processes jobs and manages system input and output processing. JES2 parameters control how and with what restrictions jobs will be run on a computer system.

JES2 options allow console operator commands to be placed in job control language. The options are assigned by type of job class. There are 36 possible batch job classes, and two additional special classes for time-share-option logons and started tasks.

Job is a basic unit of work on an IBM computer. A job consists of one or more steps or program executions.

Job Control Language is a problem-oriented computer language used in a job that identifies the job or describes its requirements to the operating system.

Job streams are a sequence of job-control-language statements and data submitted to an operating system.

Legacy sites are the computer centers that were consolidated into DISA WESTHEM Defense megacenters.

Library is a collection of related data files or programs.

Logon ID is a method by which users sign onto a computer and are identified.

MVS is the IBM multiple virtual storage operating system.

PPT is the program properties table. It contains the names of special programs, including their codes and properties. Some MVS programs are allowed extraordinary powers and privileges not normally permitted by the operating system. A list of these programs, including their special powers and privileges, is maintained in MVS, and is known as the PPT.

Programs in the PPT can bypass security software mechanisms such as password protection, can ignore file integrity, and can assign a unique storage protection key of less than eight. All of these are potential threats to system integrity. It is important to ensure that all programs in the PPT have only the capabilities needed to function properly, and that the programs are safeguarded against unauthorized use.

Program names must be kept in a special library created and controlled by the installation, or in two IBM default libraries. The program must also be contained in an APF-authorized library. Controls are intact if users cannot get a Trojan Horse program into an APF-authorized library by using the name of a nonexistent program. However, if APF controls are weak, the risk of unauthorized entry increases.

Profile is a CA-TOP SECRET term related to security administration. Profile user IDs contain permissions and access levels to resources for multiple users; their purpose is to provide a place in the security database where common access to resources can be stored.

Sensitive utilities are computer programs that provide general support for computerized processes (that is, diagnostic programs or programs designed to create test data, or copy data from one storage device to another). The utilities become sensitive when they can bypass system security software or management controls and destroy data if not used properly.

Software is a generic term used to define all programming on a computer system, whether supplied by vendors or developed by in-house programmers. System software includes the operating system and accompanying utility programs that enable a user to control, configure, and maintain the computer system software.

Supervisor Call (SVC) is an assembler language instruction that causes a hardware interruption when executed. The operating system then passes control to the SVC to tell the operating system what service is being requested (open a file for read or write access, close a file, etc.).

SVCs are divided into two categories. One category is available to all programs, while the second is restricted to APF-authorized programs only. Validity checking is the control technique that limits the execution of sensitive, unrestricted SVCs. The first 200 SVCs are provided by IBM or other software vendors. The remaining 56 SVCs can be added by a computer center's in-house programmers to meet its unique requirements or vendor software requirements.

Trojan Horse is a program that executes under an assumed identity or name. It uses a normal program name, but performs unauthorized tasks not associated with the normal program name. For example, in a payroll system, a Trojan Horse program could be used to give employees unauthorized promotions or pay increases.

Update access is a feature of the security system that allows write access to a file.

User ID is a method by which users sign onto a computer and are identified.

Utility programs are computer programs or routines that perform general data- and system-related functions required by other application software, by the operating system, or by users. Examples include copying, sorting, and merging files.

Validity checking is an MVS integrity control. It detects and disallows invalid user operations and system requests that, if allowed, would compromise system security controls.

Appendix C. Prior Audit Reports Subject to Audit Followup

Except for the scope limitations discussed in Appendix A, the audit evaluated the corrective actions taken in response to recommendations made to DISA WESTHEM organizations and DLA-DSDC in one Air Force Audit Agency report and three IG, DoD, reports. Listed below are the four reports and the organizations where audit followup was made.

Organizations Where Audit Followup Was Made	AFAA Project No. 0195410[1]	IG, DoD, Report No. 93-002[2]	93-133[3]	94-060[4]
Defense Information Systems Agency, Western Hemisphere (DISA WESTHEM):				
Headquarters, Fort Ritchie, Maryland		X		X
Defense Megacenter (DMC)-Columbus			X	X
DMC-Denver	X			X
Defense Information Processing Center (DIPC)-Cleveland		X		
Defense Logistics Agency, Systems Design Center (DLA-DSDC)			X	

[1]AFAA Project No. 0195410, "Data Processing Center Operations and Security at the Air Force Accounting and Finance Center (AFAFC)," August 5, 1991.

[2]IG, DoD, Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992.

[3]IG, DoD, Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993.

[4]IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994.

Appendix D. Summary of Audit Results by Finding, Report, Recommendation, and Organization as of January 23, 1995

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action: Adequate[3] Closed	Adequate[3] Open	Additional Required	Audit Followup Deferred[4]	Total
Finding A. Operating Systems								
AFAA 195410	1.a.	APF	DMC-Denver	1	0	0	0	1
AFAA 195410	1.b.	APF	DMC-Denver	1	0	0	0	1
AFAA 195410	1.c.	APF	DMC-Denver	1	0	0	0	1
AFAA 195410	2.a.	Guidelines	DMC-Denver	1	0	0	0	1
AFAA 195410	2.b.	Supervisor Calls	DMC-Denver	0	0	1	0	1
AFAA 195410	3.a.	PPT	DMC-Denver	1	0	0	0	1
AFAA 195410	3.b.	PPT	DMC-Denver	1	0	0	0	1
93-002	A.1.a.	Guidelines	HQ, DISA WESTHEM	1	0	0	0	1
93-002	A.1.b.	APF	HQ, DISA WESTHEM[5]	0	1	0	0	1
93-002	A.2.a.	APF	DIPC-Cleveland	0	0	1	0	1
93-002	A.2.b.	APF	DIPC-Cleveland	0	0	1	0	1
93-002	A.2.c.	APF	DIPC-Cleveland	1	0	0	0	1
93-002	A.2.d.	PPT	DIPC-Cleveland	1	0	0	0	1
93-002	A.2.e.	JES2	DIPC-Cleveland	1	0	0	0	1
93-002	A.3.a.	Supervisor Calls	DIPC-Cleveland[6]	0	0	1	0	1
93-133	A.1.a.	Guidelines	DLA-DSDC	1	0	0	0	1
93-133	A.1.b.(1)	APF	DLA-DSDC	1	0	0	0	1
93-133	A.1.b.(2)	APF	DLA-DSDC	1	0	0	0	1
93-133	A.1.b.(3)	Supervisor Calls	DLA-DSDC	0	0	1	0	1
93-133	A.1.b.(4)	PPT	DLA-DSDC	1	0	0	0	1
93-133	A.1.c.(1)	APF	DLA-DSDC	1	0	0	0	1
93-133	A.1.c.(2)	APF	DLA-DSDC	1	0	0	0	1
93-133	A.2.a.(1)	APF	DIPC-Dayton[7]	0	0	0	0	0
93-133	A.2.a.(2)	APF	DIPC-Dayton[7]	0	0	0	0	0
93-133	A.2.a.(3)	JES2	DIPC-Dayton[7]	0	0	0	0	0

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action: Adequate[3] Closed	Adequate[3] Open	Additional Required	Audit Followup Deferred[4]	Total
Finding A. Operating Systems (cont'd.)								
93-133	A.2.b.(1)	APF	DIPC-Dayton[7]	0	0	0	0	0
93-133	A.3.a.	Guidelines	DMC-Columbus	1	0	0	0	1
93-133	A.3.b.(1)	APF	DMC-Columbus	1	0	0	0	1
93-133	A.3.b.(2)	APF	DMC-Columbus	1	0	0	0	1
93-133	A.3.b.(3)	JES2	DMC-Columbus	1	0	0	0	1
93-133	A.3.c.(1)	APF	DMC-Columbus	1	0	0	0	1
94-065	A.2.b.(2)	APF	DIPC-Kansas City[7]	0	0	0	0	0
Subtotal, Finding A.				21	1	5	0	27
Summary by Organization, Finding A.								
DISA WESTHEM				15	1	4	0	20
DLA-SDC				6	0	1	0	7
Finding B. Security Software and Environmental Controls								
AFAA 195410	4.a.	Utilities	DMC-Denver	1	0	0	0	1
AFAA 195410	4.b.	Utilities	DMC-Denver	1	0	0	0	1
AFAA 195410	5.a.	Utilities	DMC-Denver	1	0	0	0	1
AFAA 195410	5.b.	Utilities	DMC-Denver	1	0	0	0	1
AFAA 195410	6.a.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	6.b.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	7.a.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	7.b.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	8.a.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	8.b.	Security Software	DMC-Denver	0	0	1	0	1
AFAA 195410	8.c.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	8.d.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	8.e.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	8.f.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	8.g.	Security Software	DMC-Denver	0	0	1	0	1

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action Adequate[3] Closed	Corrective Action Adequate[3] Open	Corrective Action Additional Required	Audit Followup Deferred[4]	Total
Finding B. Security Software and Environmental Controls (cont'd.)								
AFAA 195410	9.a.	Security Software	DMC-Denver	1	0	0	0	1
AFAA 195410	9.b.	Security Software	DMC-Denver	1	0	0	0	1
93-002	A.3.b.	Utilities	DIPC-Cleveland	0	0	1	0	1
93-002	B.1.	Security Software	DIPC-Cleveland	0	1	0	0	1
93-002	B.1.	Security Software	DIPC-Indianapolis[7]	0	0	0	0	0
93-002	B.2.	Security Software	DIPC-Cleveland	0	1	0	0	1
93-002	B.2.	Security Software	DIPC-Indianapolis[7]	0	0	0	0	0
93-002	C.1.	Security Software	DIPC-Indianapolis[7]	0	0	0	0	0
93-002	C.2.	Security Software	DIPC-Indianapolis[7]	0	0	0	0	0
93-133	A.1.c.(3)	Utilities	DLA-DSDC	1	0	0	0	1
93-133	A.2.b.(2)	Utilities	DIPC-Dayton[7]	0	0	0	0	0
93-133	A.3.c.(2)	Utilities	DMC-Columbus	1	0	0	0	1
93-133	B.1.a.	Security Software	DLA-DSDC	1	0	0	0	1
93-133	B.1.b.(1)	Security Software	DLA-DSDC	1	0	0	0	1
93-133	B.1.b.(2)	Security Software	DLA-DSDC	1	0	0	0	1
93-133	B.1.b.(3)	Security Software	DLA-DSDC	1	0	0	0	1
93-133	B.1.b.(4)	Security Software	DLA-DSDC	1	0	0	0	1
93-133	B.1.b.(5)	Security Software	DLA-DSDC	1	0	0	0	1
93-133	B.2.a.	Security Software	DIPC-Dayton[7]	0	0	0	0	0
93-133	B.2.b.(1)	Security Software	DIPC-Dayton[7]	0	0	0	0	0
93-133	B.2.b.(2)	Security Software	DIPC-Dayton[7]	0	0	0	0	0
93-133	B.2.b.(3)	Security Software	DIPC-Dayton[7]	0	0	0	0	0
93-133	B.2.b.(4)	Security Software	DIPC-Dayton[7]	0	0	0	0	0
93-133	B.2.b.(5)	Security Software	DIPC-Dayton[7]	0	0	0	0	0
93-133	B.2.b.(6)	Security Software	DIPC-Dayton[7]	0	0	0	0	0
93-133	B.3.a.	Security Software	DMC-Columbus	1	0	0	0	1
93-133	B.3.b.(1)	Security Software	DMC-Columbus	1	0	0	0	1
93-133	B.3.b.(2)	Security Software	DMC-Columbus[5]	0	1	0	0	1
93-133	B.3.b.(3)	Security Software	DMC-Columbus	1	0	0	0	1
93-133	B.3.b.(4)	Security Software	DMC-Columbus	1	0	0	0	1
93-133	B.3.b.(5)	Security Software	DMC-Columbus	1	0	0	0	1

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action: Adequate[3]: Closed	Adequate[3]: Open	Corrective Action: Additional Required	Audit Followup Deferred[4]	Total
Finding B. Security Software and Environmental Controls (cont'd.)								
94-060	C.1.b.	Environmental Controls	DMC-Columbus	1	0	0	0	1
94-060	D.1.	Environmental Controls	DMC-Denver[6]	1	0	0	0	1
94-060	D.2.	Environmental Controls	DIPC-Indianapolis[7]	0	0	0	0	0
Subtotal, Finding B.				30	3	3	0	36
Summary by Organization, Finding B								
DISA WESTHEM				23	3	3	0	29
DLA-SDC				7	0	0	0	7
Finding C. Other General Controls								
93-002	D.1.a.	Other	HQ, DISA WESTHEM[5]	0	1	0	0	1
93-002	D.1.b.	Change Controls	HQ, DISA WESTHEM	1	0	0	0	1
93-002	D.1.c.	System Programmer	HQ, DISA WESTHEM	1	0	0	0	1
93-002	D.2.a.	Change Controls	DIPC-Indianapolis[7]	0	0	0	0	0
93-002	D.2.b.	Other	DIPC-Indianapolis[7]	0	0	0	0	0
93-002	D.2.c.	System Programmer	DIPC-Indianapolis[7]	0	0	0	0	0
93-133	C.1.a.	Change Controls	DLA-DSDC	0	0	1	0	1
93-133	C.1.b.	System Programmer	DLA-DSDC	1	0	0	0	1
93-133	C.2.	System Programmer	DIPC-Dayton[7]	0	0	0	0	0
93-133	C.3.	System Programmer	DMC-Columbus	1	0	0	0	1
94-060	A.1.	Other	HQ, DISA WESTHEM	0	0	1	0	1
94-060	A.2.a.	Other	HQ, DISA WESTHEM	0	0	1	0	1
94-060	A.2.b.	Other	HQ, DISA WESTHEM	0	0	1	0	1
94-060	A.2.c.	Other	HQ, DISA WESTHEM	0	0	1	0	1
94-060	A.2.d.	Other	HQ, DISA WESTHEM	0	0	1	0	1
94-060	B.1.a.	Other	DMC-Columbus	0	0	1	0	1
94-060	B.1.b.	IMCP	DMC-Columbus	1	0	0	0	1
94-060	B.2.	IMCP	DIPC-Indianapolis[7]	0	0	0	0	0

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Follow-up: Corrective Action Adequate[3] Closed	Corrective Action Adequate[3] Open	Additional Required	Audit Follow-up Deferred[4]	Total
Finding C. Other General Controls (cont'd.)								
94-060	B.3.	Other	DMC-Denver	1	0	0	0	1
94-060	C.1.a.	Other	DMC-Columbus	1	0	0	0	1
94-060	C.2.	Other	DMC-Denver	1	0	0	0	1
94-065	C.3.	System Programmer	DIPC-Kansas City[7]	0	0	0	0	0
Subtotal, Finding C.				8	1	7	0	16
Summary by Organization, Finding C.								
DISA WESTHEM				7	1	6	0	14
DLA-SDC				1	0	1	0	2
Audit Follow-up Deferred								
93-002	A.2.a.	APF	DIPC-Indianapolis	0	0	0	1	1
93-002	A.2.b.	APF	DIPC-Indianapolis	0	0	0	1	1
93-002	A.2.c.	APF	DIPC-Indianapolis	0	0	0	1	1
93-002	A.2.d.	PPT	DIPC-Indianapolis	0	0	0	1	1
93-002	A.2.e.	JES2	DIPC-Indianapolis	0	0	0	1	1
93-002	A.4.a.	Supervisor Calls	DIPC-Indianapolis	0	0	0	1	1
93-002	A.4.b.	Utilities	DIPC-Indianapolis	0	0	0	1	1
93-002	C.2.	Security Software	DIPC-Indianapolis	0	0	0	1	1
94-065	A.1.a.	Guidelines	MCCTA	0	0	0	1	1
94-065	A.1.b.(1)	APF	MCCTA	0	0	0	1	1
94-065	A.1.b.(2)	APF	MCCTA	0	0	0	1	1
94-065	A.1.b.(3)	PPT	MCCTA	0	0	0	1	1
94-065	A.1.b.(4)	JES2	MCCTA	0	0	0	1	1
94-065	A.1.b.(5)	Utilities	MCCTA	0	0	0	1	1
94-065	A.2.a.	Guidelines	DIPC-Kansas City	0	0	0	1	1
94-065	A.2.b.(1)	APF	DIPC-Kansas City	0	0	0	1	1
94-065	A.2.b.(3)	Utilities	DIPC-Kansas City	0	0	0	1	1

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action Adequate[3] Closed	Corrective Action Adequate[3] Open	Corrective Action Additional Required	Audit Followup Deferred[4]	Total
Audit Followup Deferred (cont'd.)								
94-065	B.1.a.	Security Software	DIPC-Kansas City	0	0	0	1	1
94-065	B.1.b.	Security Software	DIPC-Kansas City	0	0	0	1	1
94-065	B.1.c.	Security Software	DIPC-Kansas City	0	0	0	1	1
94-065	B.2.a.	Security Software	MCCTA	0	0	0	1	1
94-065	B.2.b.	Security Software	MCCTA	0	0	0	1	1
94-065	C.1.a.	System Programmer	MCCTA	0	0	0	1	1
94-065	C.1.b.	Other	MCCTA	0	0	0	1	1
94-065	C.1.c.	Other	MCCTA	0	0	0	1	1
Subtotal, Audit Followup Deferred				0	0	0	25	25
Summary by Organization - Audit Followup Deferred:								
DISA WESTHEM				0	0	0	14	14
MCCTA				0	0	0	11	11
DLA-SDC				0	0	0	0	0
Subtotal, DISA, DLA-DSDC, and MCCTA Recommendations				59	5	15	25	104
Results of Other Audits[9]								
94-060	E.1.	Change Controls	DFAS FSA Denver	0	0	1	0	1
94-060	E.2.	Change Controls	DFAS FSA Denver	0	0	1	0	1
94-060	E.3.	Change Controls	DFAS FSA Denver	0	0	1	0	1
94-065	B.3.	Other	DIPC-Pensacola	0	0	1	0	1
94-065	C.2.a.	Change Controls	DIPC-Pensacola	0	0	1	0	1

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action: Adequate[3] Closed	Adequate[3] Open	Additional Required	Audit Followup Deferred[4]	Total
Results of Other Audits (cont'd.)[9]								
94-065	C.2.b.	System Programmer	DIPC-Pensacola	1	0	0	0	1
94-065	C.2.c.	Other	DIPC-Pensacola[10]	1	0	0	0	1
94-065	A.3.	Guidelines	DIPC-Pensacola	1	0	0	0	1
Subtotal, Results of Other Audits				8	0	0	0	8
Grand Total, All Recommendations				67	5	15	25	112
Summary by Organization, Grand Total:								
DFAS FSA Denver[9]				3	0	0	0	3
DISA WESTHEM -- DIPC-Pensacola[9]				5	0	0	0	5
DISA WESTHEM -- Other				45	5	13	14	77
DLA-SDC				14	0	2	0	16
MCCTA				0	0	0	11	11

[1]APF = Authorized Program Facility; Change Controls = Change controls over operating system software and application software; Guidelines = Operating system installation integrity guidelines; JES2 = Job Entry Subsystem 2 parameters; Environmental Controls = Tests of physical security plan, installation of water shutoff valves, and other means of safeguarding computer hardware and software; IMCP = Internal Management Control Program; Other = Other general controls over abnormal endings to computer operations, vendor access, and environmental protection; PPT = Program Property Tables; System programmer = Sensitive system programmer positions; and Utilities = Sensitive utilities.

[2]Acronyms used for each organization are defined as follows: DMC-Columbus and DMC-Denver are used for the Defense megacenters in Columbus, Ohio, and Denver, Colorado; HQ, DISA WESTHEM is used for the Headquarters, Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, Maryland; DIPC-Cleveland, DIPC-Indianapolis, and DIPC-Kansas City are used for the DISA WESTHEM Defense Information Processing Centers in those cities. DLA-SDC is used for the Defense Logistics Agency, Systems Design Center, in Columbus, Ohio; and MCCTA is used for the Marine Corps Computer and Telecommunications Activity in Quantico, Virginia.

[3]Closed recommendations represent those recommendations on which the recommended corrective actions (or suitable alternatives) have been completed. Therefore, no additional followup under DoD Directive 7650.3 by the Office of the Assistant Inspector General for Analysis and Followup was planned on closed recommendations. Open recommendations represent those recommendations where the corrective actions completed and planned are considered adequate. Followup under DoD Directive 7650.3 is required on open recommendations to verify that planned corrective actions are completed.

[4]Audit followup on 24 recommendations made to MCCTA, DIPC-Indianapolis, and DIPC-Kansas City will be accomplished under a separate audit, Project No. 5FD-5026, "Followup Audit of Controls Over Operating System and Security Software and General Controls of the Computer Systems Supporting the Defense Finance and Accounting Service." Audit followup was delayed because the work load of those three organizations was migrating to DMC-St. Louis and DMC-Denver during our audit.

[5]Although still in process, substantial corrective actions had been taken in response to this recommendation; the remaining actions planned were considered adequate.

[6]The integrity problem with this supervisor call must be fixed by DMC-Denver because that organization provided the supervisor call to DIPC-Cleveland.

[7]Audit followup was not performed on 24 recommendations that are no longer viable. Audit followup on recommendations made to the DIPC-Dayton, whose work load migrated to the DMC-Columbus, was accomplished as part of our audit at the DMC-Columbus. Other recommendations have been rendered obsolete by the ongoing DISA WESTHEM reorganization. For example, making structural improvements, revising operating procedures, and similar recommendations were no longer viable at the DIPC-Indianapolis and DIPC-Kansas City, which were scheduled to close during FY 1995. Followup on recommendations made to those two organizations was limited to recommendations to make software changes. Followup under DoD Directive 7650.3 will be closed on these 24 recommendations by OAIG-AFU.

[8]This recommendation was redirected to DFAS Denver because DMC-Denver was only a tenant organization. DMC-Denver adequately responded to this recommendation. For details, see the discussion of environmental controls in Part I (Finding B) of the report.

[9]Audit results are as of October 31, 1994. Corrective actions taken in response to the recommendations made in IG, DoD, Reports No. 94-060 and 94-065 to DFAS FSA Denver and DISA WESTHEM DIPC-Pensacola were separately evaluated in IG, DoD, Project No. 4FG-5060, "Corrective Action on System and Software Security Deficiencies." This report incorporates the results of the other audit.

[10]Adequate corrective actions were taken on this recommendation; however, IG, DoD, Project No. 4FG-5060 identified a new finding related to controls over keys to an off-site storage location.

Appendix E. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
A.1.a., A.2.a., A.2.b.	Management controls. Improves computer security at DIPC-Cleveland and other DISA WESTHEM computer centers by strengthening controls over the Authorized Program Facility.	Nonmonetary.
A.1.b.(1), A.3.a., A.3.b., A.4.a., A.4.b., A.4.c.	Management controls. Improves computer security at DLA-DSDC, DIPC-Cleveland, DMC-Columbus and DMC-Denver by eliminating material management control weaknesses in the controls over supervisor calls.	Nonmonetary.
A.1.b(2)	Management controls. Improves computer security at all DISA WESTHEM computer centers by ensuring that IBM-recommended installation integrity guidelines are implemented.	Nonmonetary.
B.1.a., B.1.b., B.3.	Management controls. Improves computer security at DFAS FSA Denver and DMC-Denver by strengthening controls over bypass label processing and one special privilege attribute (NOSUBCHK) .	Nonmonetary.
B.2.	Management controls. Improves physical security of costly computer assets at DMC-Denver by reducing risk of water damage. Nonmonetary.	Nonmonetary.

Appendix E. Summary of Potential Monetary Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
B.4.	Management controls. Improves computer security at DIPC-Cleveland by strengthening the controls over sensitive utilities.	Nonmonetary.
B.5.	Management controls. Improves the operational efficiency of all DISA WESTHEM computer centers by waiving an unnecessary C2 security requirement.	Nonmonetary.
C.1.a.	Management controls. Improves computer security at DMC-Columbus by completing required recertification reviews of computer systems.	Nonmonetary.
C.1.b., C.1.c., C.1.d.(1), C.1.d.(2), C.1.d.(3), C.1.d.(4), C.2.a., C.2.b.	Management controls. Strengthens management controls and improves efficiency of computer operations at DFAS FSAs, DISA WESTHEM computer centers, and DLA-DSDC by issuing standard procedures related to contractor access to systems, abnormal endings to computer operations, ADP equipment contracts, and changes to operating system software.	Nonmonetary.

Appendix F. Organizations Visited or Contacted

Office of the Secretary of Defense

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

Defense Agencies

Defense Finance and Accounting Service, Washington, DC
  Defense Finance and Accounting Service, Denver, CO
  Defense Finance and Accounting Service, Financial Systems Organization, Financial Systems Activity, Denver, CO
Defense Information Systems Agency
  Defense Information Systems Agency, Western Hemisphere[1], Fort Ritchie, MD
  Defense Information Systems Agency, Western Hemisphere, Denver, CO
  Defense Information Processing Center[2], Cleveland, OH
  Defense Megacenter[3], Columbus, OH
  Defense Megacenter[4], Denver, CO
Defense Logistics Agency, Alexandria, VA
  Defense Systems Design Center,[5] Columbus, OH

---

[1]The Defense Information Systems Agency, Western Hemisphere (DISA WESTHEM), was referred to in IG, DoD, Reports No. 93-002 and No. 94-060 as either the DISA Defense Information Services Organization (DISO) or the Defense Information Technology Services Organization (DITSO).

[2]In IG, DoD, Report No. 93-002, the DISA WESTHEM Defense Information Processing Center-Cleveland was referred to as the DITSO Information Processing Center-Cleveland.

[3]In IG, DoD, Reports No. 93-133 and No. 94-060, the Defense Megacenter-Columbus was referred to as either the DISO Information Processing Center-Columbus, or the DITSO Columbus Information Processing Activity.

[4]In Air Force Audit Agency Report No. 0195410 and in IG, DoD, Report No. 94-060, the Defense Megacenter-Denver was referred to as either the Air Force Accounting and Finance Center or the DISO Information Processing Center-Denver.

[5]The Defense Logistics Agency (DLA), Systems Design Center, was referred to as the DLA Systems Automation Center in IG, DoD, Report No. 93-133.

Appendix G. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Under Secretary of Defense (Comptroller/Management)
    Director, Management Improvement
  Deputy Under Secretary of Defense (Comptroller/Program/ Budget)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Assistant to the Secretary of Defense (Public Affairs)
Director, Administration and Management
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

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

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Office of the Deputy Assistant Secretary of the Air Force (Plans, Systems and Analysis), Audit Liaison and Follow-up

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
  Director, Defense Finance and Accounting Service Denver Center
  Director, Financial Systems Organization
    Director, Financial Systems Organization, Financial Systems Activity Denver

Other Defense Organizations (cont'd)

Director, Defense Information Systems Agency
  Commander, Defense Information Systems Agency, Western Hemisphere
    Director, Defense Information Systems Agency, Defense Information Processing Center-Cleveland
    Director, Defense Megacenter-Columbus
    Director, Defense Megacenter-Denver
  Comptroller, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
Director, Defense Logistics Agency
  Commander, Defense Logistics Agency, Systems Design Center
Director, National Security Agency
Inspector General, National Security Agency

Non-Defense Federal Organizations

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

Chairman and ranking minority members 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

This page was left out of orignial document

Part III - Management Comments

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

MAY 23 1995

DFAS-HQ/PA

MEMORANDUM FOR DEPUTY DIRECTOR FOR FINANCIAL MANAGEMENT,
DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service (Project No. 4FD-5068)

This responds to your memorandum of March 24, 1995, on the above subject. Specific Defense Finance and Accounting Service comments to recommendations B.2 and B.3 are attached.

If you have any questions, you may contact Dennis Schilcher at (703) 607-3935.

for Michael E. Wilson
Deputy Director
Customer Service and
Performance Assessment

Attachment

Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service
Project No. 4FD-5068

Recommendation B.2. We recommend that the Director, Defense Finance and Accounting Service, Denver Center, require the Director, Directorate of Support Services, at Defense Finance and Accounting Service, Denver Center, to install overhead shutoff valves in the computer room at the Defense Megacenter, Denver, Colorado.

DFAS Response:

Concur. The accomplishment of the total project will require an estimated 24 months to complete. Two contracting actions will be needed, one for the engineer design and one for installation of isolation valves. One reason for the extended installation time is to allow for accomplishment of work without interrupting the normal operation of building 444 and the Defense Megacenter computer operations.

It should be noted that the piping systems that are currently routed through the computer room are in good repair and physical inspections have not identified any pipe or component deterioration. Realizing that physical inspection systems are not flawless, but based upon the systems age, less than half of its economic life, the systems integrity does not appear to be at risk.

DFAS-DE received funding for this project on May 17, 1995. Contact has been made with support engineers at Peterson AFB and they believe they will be able to let the contracts for the design and installation of the water isolation valves this year.

Estimated Completion Date: March 1997

Recommendation B.3.: We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado, modify the application code to allow the removal of the NOSUBCHK special privilege attribute.

DFAS Comment:

Concur. We have reviewed and identified the IDMS programs utilizing a special security attribute of NOSUBCHK. Our programming effort to remove the utilization of this attribute has been tested and will be implemented in the production environment as of May 31, 1995.

Estimated Completion Date: May 31, 1995.

Defense Information Systems Agency Comments

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

06 JUN 1995

REPLY REFER TO: Inspector General

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Financial Management Directorate

SUBJECT: DoDIG Draft Report on the Followup Audit on Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service (Project No. 4FD-5068)

Reference: DoDIG Report, subject as above, 24 Mar 95

1. We reviewed the subject draft report and concur with the recommendations addressed to DISA. Our management comments are enclosed which discuss corrective actions to be taken on the recommendations. Where corrective action has already been taken, we identified the actions taken and provided the date of completion.

2. The point of contact is Ms. Sandra J. Leicht, Audit Liaison. If you have questions on our response, Ms. Leicht can be reached on (703) 607-6316.

FOR THE DIRECTOR:

1 Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

MANAGEMENT COMMENTS ON DRAFT REPORT ON THE FOLLOWUP AUDIT ON CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE AND OTHER GENERAL CONTROLS FOR COMPUTER SYSTEMS SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE (Project No. 4FD-5068)

1. **Recommendation A.1.a.:** Review and finalize the draft DISA WESTHEM Policy Letter 95-3, "Oversight and Control of Access to Authorized Program Facility (APF) Libraries/Files."

Response: Concur in Part. The Draft DISA WESTHEM Policy Letter 95-3 will be rescinded. In lieu of a policy statement, the requirements contained in the draft policy will be incorporated in the MVS Technical Implementation Standards (2.1.2.1. subparagraph 3) in the next release anticipated for August 1995.

2. **Recommendation A.1.b.(1).:** Provide technical assistance to solve the integrity problems caused by supervisor calls.

Response: Concur. DISA WESTHEM currently responds to the DMCs request for review of supervisor calls. For example, DMC Denver requested an analysis and review of the supervisor calls to determine what, if any, controls could be implemented to correct the problems. DISA WESTHEM sent two individuals to DMC Denver and provided recommendations for securing the supervisor calls. As DISA WESTHEM currently provides technical assistance to the DMCs which satisfies the recommendation, we recommend this action be closed.

3. **Recommendation A.1.b.(2):** Conduct and report on periodic assurance reviews on the DMCs compliance with the "Computer Operations MVS Security Technical Implementation Standards," 24 December 1994.

Response: Concur. DISA WESTHEM has conducted a Security Readiness Review (SRR) of each of the 16 DMCs and has developed a follow-up process for correcting, reporting, and tracking the status of each of the findings of the SRR process. In addition, during FY 1996, no-notice inspections for some of the DMCs are planned. Complementing this process is DISA WESTHEM's ability to provide real-time surveillance of the DMCs. As this is an ongoing effort which satisfies the recommendation, we recommend this action be closed.

4. **Recommendation A.2.a:** Direct the Chief, Technical Support, to review all authorized program facility libraries and programs and delete obsolete and undocumented programs.

Response: Concur. DISA WESTHEM reviewed all authorized program facility libraries and programs and deleted obsolete and undocumented programs in April 1995. Therefore, we recommend this action be closed.

5. **Recommendation A.2.b:** Direct the Automated Information Systems Security Officer to review access rules of all authorized program facility libraries and limit update access to APF databases to the software specialist's area of responsibility as required by DISA WESTHEM Policy Letter 95-3.

Response: Concur. In response to Recommendation A.1.a., the next release of the MVS Technical Implementation Standards will be August 1995. All DISA WESTHEM security officers will be required to review this manual.

6. **Recommendations A.4.a.b.c:** Make the appropriate changes required to eliminate the integrity exposures existing on the four SVCs; request appropriate programming assistance in resolving the problems with supervisor calls at DMC Denver and DIPC Cleveland; and export the corrected supervisor calls to the DIPC Cleveland.

Response: Concur. The DMC Denver made changes as recommended by the auditors during the past reviews. Efforts are underway to make changes by prioritizing the systems for implementation. While all SVCs are being reviewed, the required work to adequately comply with the recommendation on SVCs * , we estimate a completion date of 31 May 1996. It is important to note that in some cases we are dependent on FSA support and interagency cooperation. We have inherited back-leveled systems and are in the process of implementing changes as quickly as possible without impacting production. We will not be spending any effort on System B as we are in the process of migrating that system, with the cooperation of the customer, to another platform which will eliminate it entirely. The estimated completion date for SYB to migrate is 31 December 1995.

7. **Recommendation B.1.a:** Implement bypass label processing control that allows access to only tape files.

Response: Concur. The bypass label processing (BLP) was reviewed and corrective action was taken in April 1995 to allow access to only tape files. Therefore, we recommend this action be closed.

8. **Recommendation B.1.b:** Remove the NOSUBCHK special privilege attribute from system software that support DFAS application.

Response: Concur. The NOSUBCHK attribute was reviewed and a technical problem was found. Computer Associates changed some codes preventing the NOSUBCHK from being removed. However, Computer Associates has agreed to correct the problem. Once this has been accomplished, DISA WESTHEM will remove the NOSUBCHK attribute. Estimated completion date is December 1995.

9. **Recommendation B.4:** Direct the Automated Information Security Officer at DISA WESTHEM and DIPC-Cleveland to control sensitive utilities by implementing the protected program list

*Supervisor Call numbers deleted.

and special access rules features of the Computer Associates, Incorporated, Access Control Facility 2 security software.

Response: Concur. DISA WESTHEM published the MVS Security Technical Implementation Standards in December 1994 which was disseminated to all of the DMCs for implementation. This document identifies and describes how to secure sensitive utilities for each security control product. As new information is available, the standard will be updated. Recommend this action be closed as the recommendation is currently being implemented.

10. **Recommendation B.5:** Recommend the Chief Information Officer approve the request from the Security Officer, DISA WESTHEM, to waive the C2 requirement for autoerase and erase-on-delete at all DMCs.

Response: Concur in Part. The DISA WESTHEM security officer has not submitted the request to the CIO as they are reviewing alternative solutions to meet this requirement. The DISA WESTHEM security office has been tasked to provide their plan of action to DISA WESTHEM Headquarters by 30 June 1995.

11. **Recommendation C.1.a:** Direct DMC Columbus to complete by May 1995 the recertification review of the organization's computer systems as required by the Office of Management and Budget Circular No. A-130.

Response: Concur. The recertification review is being performed by the DISA Center for Information Systems Security (CISS). The in process review is scheduled for July 1995.

12. **Recommendation C.1.b:** Finalize the DISA WESTHEM Policy Letter 95-4, "Security Guidance for DISA WESTHEM Automated Information System (AIS) Contracts."

Response: Concur in Part. DISA WESTHEM will be establishing security procedures and the guidance set forth in the draft Policy Letter 95-4 will be incorporated in those procedures. Estimated completion date August 1995.

13. **Recommendation C.1.c:** Issue a procedure establishing an in-house quality assurance program to track and analyze the causes of abnormal endings to computer operations and prevent abnormal endings due to repetitive causes.

Response: Concur. DISA WESTHEM is cognizant of the ABENDS situation and is in the process of taking corrective action. The ABENDS to computer operations is an on-going problem and we can never expect to achieve a one hundred percent prevention of abnormal endings. It is anticipated that we will require a quarterly ABENDS analysis to look at the trends and take necessary action for those ABENDS due to repetitive causes. Estimated completion date of the in-house procedure is October 1996.

14. Recommendation C.1.d: Issue a procedure establishing an in-house quality assurance program over the maintenance performed under automatic data processing equipment contracts.

Response: Concur. DISA WESTHEM concurs with the validity of the Quality Assurance portion stated in the finding. DISA WESTHEM implemented corrective action on 17 February 1995, as a result of a similar finding under DoDIG Audit No. 94-060. All DMCs have the corrective action and are to be implementing the procedures to establish an in-house quality assurance program over the maintenance performed under ADPE contracts. This corrective action will be included in the comprehensive internal management control program (IMCP) package DISA WESTHEM is developing for all assessable units. Estimated completion date of the DISA WESTHEM IMCP which will incorporate the quality assurance program, is November 1995.

Defense Finance and Accounting Service, Financial Systems Activity Denver, Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
FINANCIAL SYSTEMS ACTIVITY
6760 EAST IRVINGTON PLACE
DENVER, COLORADO 80279-8000

DFAS-FSADE May 19, 1995

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL
(DEPARTMENT OF DEFENSE)
ATTN: DIRECTOR, FINANCE AND ACCOUNTING
DIRECTORATE

SUBJECT: Management Comments on Project No. 4FD-5068

We are forwarding our management comments regarding Findings A and B of Project No. 4FD-5068 on draft Audit Report titled Follow-up Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service.

The FSADE point of contact is Ms. Lana Cheatham, FSADE/SR, DSN 926-7961.

Malcolm G. Parks
Director, Denver FSA

Attachment:

cc: FSO/B (E. Cmar)

Defense Finance and Accounting Service, Financial Systems Activity Denver, Comments

Audit Report 4FD-5068

FSADE Management Comments on Findings A and B

Finding A, Recommendation A4b: The FSADE has specifically offered application programming assistance to the DMC-DE systems software staff to install whatever software changes they recommend that will facilitate system security and continuation of efficiency in processing. The FSADE has also discontinued further use of the supervisory call in question in any additional program development or modification.

Finding B, Recommendation B3: Concur. We have reviewed and identified the IDMS programs utilizing a special security attribute of NOSUBCHK. Our programming effort to remove the utilization of this attribute has been tested and implemented in the production environment as of May 1, 1995.

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service

B. DATE Report Downloaded From the Internet: 01/09/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 01/09/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.