OFFICE OF THE INSPECTOR GENERAL

CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE

Report No. 94-065 March 24, 1994

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) 614-6303 (DSN 224-6303) or FAX (703) 614-8542.

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) 614-1868 (DSN 224-1868) or FAX (703) 614-8542. 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 DoD Hotline at (800) 424-9098 (DSN 223-5080) or write to the DoD Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of writers and callers is fully protected.

Acronyms

APF	Authorized Program Facility
CA-ACF2	Computer Associates International, Inc., Access Control Facility 2 Security Software
CA-TOP SECRET	Computer Associates International, Inc., TOP SECRET Security Software
DCPS	Defense Civilian Pay System
DFAS	Defense Finance and Accounting Service
DISO	Defense Information Services Organization
IBM	International Business Machines Corporation
ID	Identification
IG	Inspector General
JES2	Job Entry Subsystem 2
MCCTA	Marine Corps Computer and Telecommunications Activity
MVS/XA	Multiple Virtual Storage with Extended Architecture
PPT	Program Properties Table
SMP/E	System Modification Program/Extended Architecture
SVC	Supervisor Call

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

March 24, 1994

MEMORANDUM FOR ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Audit Report on Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service (Report No. 94-065)

We are providing this final report for your review and comments. The report discusses management controls over selected features of the operating system and security software used by elements of the Defense Information Services Organization (DISO), the Defense Finance and Accounting Service (DFAS), and the U. S. Marine Corps. Comments received from the Defense Finance and Accounting Service and the Defense Information Security Agency (DISA) on behalf of DISO were considered in preparing the final report. Comments were not received from the Navy.

DoD Directive 7650.3 requires that all recommendations be promptly resolved. Therefore, we request that the Navy and DISO provide comments by May 23, 1994. See the "Response Requirements for Each Recommendation" chart at the end of each finding for the specific requirements for your comments.

The courtesies extended to our audit staff are appreciated. If you have any questions about this audit, please contact Mr. David C. Funk, Program Director, at (303) 676-7445 (DSN 926-7445), or Mr. W. Andy Cooley, Project Manager, at (303) 676-7393 (DSN 926-7393). Appendix D lists the planned distribution of this report. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, Department of Defense

Audit Report No. 94-065
(Project No. 1FD-0043.02)

March 24, 1994

AUDIT REPORT ON CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE

EXECUTIVE SUMMARY

Introduction. This is the final in a series of three audits of management controls over the operating systems and security software used by the information processing centers that support the Defense Finance and Accounting Centers (DFAS). The audit concentrated on the operating system and security software used by four organizations* to provide computer support to the DFAS Centers in Kansas City, Missouri (DFAS-Kansas City), and Denver, Colorado (DFAS-Denver). Those two DFAS Centers make about $22.6 billion in annual payments on more than 390,000 payroll accounts. The four organizations audited were the Defense Information Services Organization (DISO) Information Processing Center in Kansas City, Missouri (DISO-Kansas City); the DFAS Financial Systems Activity in Pensacola, Florida (DFAS-Pensacola); and the Marine Corps Computer and Telecommunications Activity (MCCTA) and its Worldwide Support Division, both in Quantico, Virginia.

Objective. Our objective was to determine whether management controls over selected features of the operating system and security software used on the production and test systems were adequate to safeguard the integrity of DFAS data. To accomplish this objective, we evaluated nine operating system features and management controls to determine whether unauthorized functions could be performed. We also reviewed the implementation of security software to determine whether controls prevented unauthorized personnel from gaining access to the systems, and authorized users from accessing unauthorized programs and data.

Audit Results. All four organizations had deficiencies in the implementation and control of operating system and security software. Any knowledgeable user could improperly access, add, modify, or destroy pay and accounting data, and enter erroneous data (accidentally or intentionally) without leaving an audit trail. Because of their sensitive nature, only general terms are used to discuss the deficiencies summarized below and in Part II of the report. The audit did not identify any unauthorized access to pay and accounting data.

o Management needed to improve controls over four of the nine operating system features reviewed at MCCTA and MCCTA-Worldwide Support Division. Improved controls were also needed on three of the nine features reviewed at DISO-Kansas City and DFAS-Pensacola. Application programs and data such as pay and accounting records could be added, modified, or deleted without detection, and the

---

* Several activities visited during the audit were subsequently renamed because of the ongoing DoD consolidation effort. All the activities visited are referred to in this report by their new names. See Appendix C for details of the reorganizations.

integrity of systems processing about $22.6 billion annually in disbursements was not fully assured (Finding A).

o At MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City, security features of Computer Associates International, Inc. (CA), CA-TOP SECRET software were not correctly implemented. Therefore, authorized system users could perform unauthorized tasks. Except in two areas, DFAS-Pensacola correctly installed CA-Access Control Facility 2 security software (Finding B).

o At all four organizations, controls over the maintenance of the operating systems needed improvement. Inadequate controls existed at one organization over changes made to the operating system. None of the organizations consistently designated sensitive system programmer positions as critical-sensitive or always obtained the required background investigations for those positions. Three organizations did not store backups of critical operating system software at off-site locations. As a result, there was increased risk to the integrity of the operating systems and the continuity of computer operations (Finding C).

Internal Controls. We identified material internal control weaknesses as defined by Office of Management and Budget Circular A-123 and DoD Directive 5010.38. Controls were not adequate to prevent numerous deficiencies in operating system and security software. A knowledgeable user could access, modify, or destroy sensitive computer data, programs, and other resources without leaving an audit trail. Critical operating system backup files were not adequately protected from damage or destruction, which could adversely affect the continuity of computer operations in the event of disaster. All recommendations in this report, if fully implemented, will correct the weaknesses. Additional details are provided in Part I, Internal Controls, and Part II, Findings A, B, and C, of this report.

Potential Benefits of Audit. This audit contains no potential monetary benefits, but recommends corrective actions for material internal control weaknesses at the four organizations. See Appendix B for a summary of the benefits resulting from this audit.

Summary of Recommendations, Management Comments, and Audit Response. We recommended that DFAS, DISO, and MCCTA strengthen controls over the use of operating systems and security software and comply with established security requirements. DFAS and DISO concurred with the findings and recommendations, except in one instance. Because of the need to respond when the production system goes down during off-peak hours, DISO did not fully concur with limiting the number of users who are allowed to change control options. Comments were not received from the Navy for the recommendations made to MCCTA. Comments on this final report are requested from the Navy and DISO by May 23, 1994. A discussion of the responsiveness of management comments is in Part II of the report, and the complete text of the comments is in Part IV.

Table of Contents

Executive Summary i

Part I - Introduction 1

Background 2
Objectives 3
Scope and Methodology 4
Internal Controls 4
Prior Audits and Other Reviews 5

Part II - Findings and Recommendations 7

Finding A. Operating System Controls 8
Finding B. Implementation of Security Software 15
Finding C. Management Controls Over MVS Maintenance 20

Part III - Additional Information 25

Appendix A. Glossary 26
Appendix B. Summary of Potential Benefits Resulting from Audit 30
Appendix C. Organizations Visited or Contacted 32
Appendix D. Report Distribution 33

Part IV - Management Comments 35

Defense Finance and Accounting Service 36
Defense Information Services Agency 43

This report was prepared by the Financial Management Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Part I - Introduction

Background

This is the final audit in a series of three audits of management controls over the operating systems and security software used by the information processing centers that support the Defense Finance and Accounting Service (DFAS). We previously reported on two audits of information processing centers of the Defense Information Services Organization (DISO) and other organizations that provide computer support to DFAS. In this audit, we concentrated on the DISO, DFAS, and Marine Corps activities* supporting DFAS-Kansas City; the Defense Civilian Pay System used by DFAS-Denver; and the Standard Accounting, Budgeting and Reporting System used by DFAS-Kansas City.

Marine Corps Systems. The Marine Corps Computer and Telecommunications Activity (MCCTA)-Worldwide Support Division at Quantico, Virginia, builds the Multiple Virtual Storage with Extended Architecture (MVS/XA) operating system used on two IBM 3090-400 computers at DISO-Kansas City. Each month, DFAS-Kansas City disburses about $1.7 billion on 342,000 pay accounts (active duty, retiree, and reserve).

MCCTA-Worldwide Support Division also developed the MVS/XA operating system used on an Amdahl 5995-1400 computer at Quantico, Virginia, and operates one partition (see Appendix A, "Glossary") on that computer. Two other partitions on that computer are operated by MCCTA and the Marine Corps Computer Science School, both at Quantico, Virginia. We reviewed only the MVS/XA systems used by MCCTA-Worldwide Support Division and MCCTA. MCCTA-Worldwide Support Division uses its partition to test standardized applications and third-party software, and to build and customize operating systems for six locations. MCCTA uses its partition to run the Standard Accounting, Budgeting and Reporting System, which processes about 1.5 million transactions per month.

DFAS Computers. The DFAS Financial Systems Activity at Pensacola, Florida (DFAS-Pensacola), operates one IBM 4381 computer at the Naval Air Station, Pensacola, and maintains an MVS/XA partition on an Amdahl 5890 computer at the DISO information processing center in Denver, Colorado (DISO-Denver). DFAS-Pensacola uses the IBM computer to develop and test the Defense Civilian Pay System (DCPS). The production DCPS for DFAS-Denver Center is run on the Amdahl computer. DCPS processes about 48,000 accounts and pays out $179.0 million per month.

MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola process only unclassified (sensitive) data. Government civilian and military personnel provide the programming support required to

* Several activities visited during the audit were subsequently renamed because of the ongoing DoD consolidation effort. All of the activities are referred to in this report by their new names. See Appendix C for details of the reorganizations.

maintain the operating system and security software. As discussed below, to assure the integrity of DFAS data, adequate management controls must be maintained over the operating system and security software installed on computer systems.

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 (i.e., scheduling jobs, loading programs, allocating computer memory, managing files, and controlling input/output operations). Operating systems also isolate and protect individual user programs. MCCTA, DISO-Denver, DISO-Kansas City, and DFAS-Pensacola all use the MVS/XA operating system software to control the execution of computer programs.

When the various 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. Commercial security software packages control authorized users; this feature is known as access control. These packages are optional, but are needed to safeguard system integrity.

Access Controls. Access controls allow only authorized employees to use computer resources, and allow those individuals to use only the resources required to perform their jobs. Computer resources include files, programs, tapes, database definitions, libraries, readers, and processing capabilities. All four organizations covered by our audit used security software developed by Computer Associates International, Inc. (CA), to control access to their computer systems. MCCTA and DISO-Kansas City used the CA-TOP SECRET package, while DFAS-Pensacola used CA-Access Control Facility 2 (CA-ACF2). When properly installed and administered, commercial security software packages, such as CA-TOP SECRET and CA-ACF2, protect a variety of resources and MVS/XA subsystems.

Other Terms. Other technical terms used in this report are defined in the Glossary (Appendix A).

Objectives

The overall objective of this audit was to determine whether management controls over selected features of the operating system and security software used at MCCTA, DISO-Kansas City, and DFAS-Pensacola were adequate to safeguard data integrity. To accomplish this objective, we evaluated nine operating system features and management controls to determine whether unauthorized functions could be performed. We also reviewed the implementation of security software to determine whether controls prevented unauthorized personnel from gaining access to the systems, and authorized users from accessing unauthorized programs and data.

Scope and Methodology

We performed audit work at MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola (including the DCPS partition at DISO-Denver). We evaluated the management controls and nine operating system features that can affect the integrity of operating system and security software. The nine operating system features examined were the authorized program facility (APF); supervisor calls (SVCs); time share option; system modification program; system management facility; program properties table (PPT); job entry subsystem 2 (JES2); exits; and sensitive utilities. We also examined the implementation of the CA-TOP SECRET and CA-ACF2 security software.

Computer-Processed Data Used. To achieve the audit objectives, we relied extensively on computer-processed data in the operating system libraries and security software of each activity. We used CA-EXAMINE auditing software to extract data directly from computer memory and operating system libraries. CA-EXAMINE is a software program that audits MVS/XA operating systems. We used automated and manual techniques to analyze system data. For example, we used the audit features of the CA-TOP SECRET and CA-ACF2 security software packages to test security rules and features. 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 was 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.

Time Period, Locations, and Standards. This program audit was performed from December 1992 through September 1993. 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 internal controls as were considered necessary. At the four locations, we reviewed operating system data covering the period December 1992 through September 1993. During the audit, we visited or contacted the organizations shown in Appendix C.

Internal Controls

At each of the four organizations, we evaluated the general controls related to the operating systems, security, change controls, and personnel. We identified material internal control weaknesses as defined by Office of Management and Budget Circular No. A-123 and DoD Directive 5010.38. At all four organizations, weaknesses in operating system controls and improperly implemented security software exposed major computer applications and data to unauthorized or fraudulent changes. Nonexistent procedures for controlling operating system changes, failure to perform the required background investigations for sensitive system programmer positions, and inadequate

protection of critical system backups threatened the integrity of the computer systems and continuity of computer operations at one or more organizations. These internal control weaknesses are considered material because they affect the integrity of computer applications used to process about $22.6 billion in annual payroll disbursements. All recommendations in this report, if implemented, will correct these weaknesses. Additional details are provided in Part II, Findings A, B, and C, of this report.

We evaluated each organization's implementation of DoD Directive 5010.38, "Internal Management Control Program." Except at DFAS-Pensacola, none of the internal control programs identified the specific operating system and security software features examined during our audit. Because of the advanced technology used, we would not expect these controls features to be addressed by the typical internal control program.

Prior Audits and Other Reviews

Five prior audit reports have been issued in this area. The first was a report from the President's Council on Integrity and Efficiency (PCIE), "Review of Internal Controls in Federal Computer Systems," October 12, 1988. The PCIE report identified serious internal control deficiencies in operating system and security software at 10 non-DoD computer centers.

Inspector General (IG), DoD, Reports. "Management of Access Controls to Computers at the Defense Logistics Agency," Report No. 89-058, was issued on March 14, 1989. The audit showed that automated access controls to mainframe computers were not effectively implemented and managed, and sensitive utilities were not effectively controlled. "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," Report No. 93-002, was issued on October 2, 1992. The audit showed that the DISO Information Processing Centers at Cleveland, Ohio, and Indianapolis, Indiana, had serious problems with operating system and security software controls. "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," Report No. 93-133, was issued on June 30, 1993. The audit showed that the DISO Information Processing Centers, Columbus and Dayton, Ohio, and the Defense Logistics Agency Systems Automation Center, Columbus, Ohio, had serious problems with operating system and security software controls. The reports recommended improvements and additions to security and software controls. Management agreed to implement the recommendations.

Air Force Audit Report. The Air Force Audit Agency (AFAR), issued "Data Processing Center Operations and Security at the Air Force Accounting and Finance Center (AFAFC)," Project No. 0195410, on August 5, 1991. The AFAR report concluded that the management of selected operating system and security software features at AFAFC (now DISO-Denver) was inadequate, and that controls over data integrity and security needed to be improved.

We identified similar deficiencies at MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola, although not to the same degree as in the previous audits. No audits of the operating system had been conducted previously at these locations.

Part II - Findings and Recommendations

Finding A. Operating System Controls

Operating system controls needed to be improved on four of the nine operating system features reviewed at MCCTA and MCCTA-Worldwide Support Division. Improved controls were also needed at DISO-Kansas City and DFAS-Pensacola in three of the nine operating system control areas. Specifically, authorized program facility libraries and programs were not adequately monitored and controlled; programmers at DFAS-Pensacola had installed non-IBM supervisor calls that compromised system integrity; program names in the program properties table were not adequately controlled at MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City; job entry subsystem 2 parameters did not control user submission of operator commands at MCCTA and MCCTA-Worldwide Support Division; and controls over sensitive utility programs were not adequate. These conditions existed because the installation integrity guidelines recommended by IBM, which would have documented the controls over the MVS/XA operating system, had not been provided to operating personnel. As a result, application programs and data, such as pay records, could be added, modified, or deleted without detection, and the integrity of systems that process about $22.6 billion annually in payroll disbursements was not assured.

Data Integrity

Authorized Program Facility. Authorized program facility (APF) libraries and programs were not adequately monitored. This occurred because management lacked clear, written APF control procedures, like those specified in the installation integrity guidelines recommended by IBM. Such guidelines are being prepared by the Director, DISO, in response to recommendations made in our Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992. Without 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. Of the 369 APF libraries and 7,722 APF-authorized programs at MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City, we found 65 obsolete or undocumented libraries, which included 751 obsolete or undocumented programs. In addition, five APF libraries were nonexistent, and eight libraries were not defined to the volumes on the MCCTA-Worldwide Support Division system. This allowed users to assign their own libraries to the APF list, making them authorized. DFAS-Pensacola maintained and adequately secured all 118 of its APF libraries on both systems.

Time-Share-Option APF Commands. Of the 185 command entries in the APF time-share-option tables at MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola, 32 commands (programs) were obsolete, nonexistent, or not documented. During the audit, DFAS-Pensacola's nine undocumented commands, as well as the six undocumented time-share-option commands on the MCCTA-Worldwide Support Division system, were deleted from the APF-authorized time-share-option tables.

Controls Over Supervisor Calls. On the DFAS-Pensacola Financial Systems Activity system and at DISO-Denver (DCPS partition), DFAS-Pensacola programmers had installed non-IBM supervisor calls (SVCs) that compromised system integrity. On the DFAS-Pensacola system, three user/vendor SVCs (see Appendix A, "Glossary") did not provide adequate controls, and three SVCs on the DCPS partition at DISO-Denver were inadequate. This occurred because information systems personnel at DFAS-Pensacola had not developed an installation integrity policy, as recommended by IBM, for reviewing SVCs added by users and vendors. With the user/vendor-added SVCs, any knowledgeable user could bypass normal controls on the operating system and security software, and could add, modify, or delete system data at will. However, during the audit, DFAS-Pensacola reinstalled these SVCs with the vendor-documented procedures, which corrected the problem. We tested the SVCs and found them adequate to protect the integrity of the two systems maintained by DFAS-Pensacola.

IBM SVCs. At MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola, including the DCPS partition at DISO-Denver, we reviewed 83 of 660 IBM-numbered SVCs on 6 systems. We contacted vendors concerning 24 IBM SVCs (83 SVCs at all locations). Vendors' software had modified, replaced, or front-ended these SVCs (front-ending means that vendor SVCs would be called up before IBM SVCs). Based on the vendors' statements and our audit tests, none of these 83 SVCs compromised system integrity.

User/Vendor SVCs. At MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola, including the DCPS partition at DISO-Denver, we reviewed 67 user/vendor-installed SVCs. A total of six SVCs (three at each of two locations) maintained by DFAS-Pensacola did not have adequate validity checking and presented significant exposures to system integrity. We tested these SVCs and were able to bypass MVS/XA controls. DFAS-Pensacola programmers observed some of our tests and agreed with our assessment. For the remaining 61 SVCs, the SVC code and vendor documentation did not show any additional risks to system integrity. During the audit, DFAS-Pensacola corrected the exposures on its central design activity system and the DCPS partition at DISO-Denver. We tested the SVCs and found them adequate to protect the respective systems.

Program Properties Table. Program names in the program properties table (PPT) were not adequately controlled. This occurred because program names were loaded in the PPT according to IBM guidelines or by local sources, but the corresponding software was not loaded or subsequently was not appropriately deleted. As a result, Trojan Horse programs (see Appendix A, "Glossary")

could be substituted for missing PPT programs, allowing users to access data controlled by another job stored anywhere in the operating system, or bypassing security software controls altogether.

PPT Controls. Program names must be kept in a special library controlled by the information processing center or in two default libraries provided by IBM. The programs must also be in an APF-authorized library. If a user cannot get a "Trojan Horse" program into an APF library by using the name of a nonexistent program, the controls are intact. However, unless these libraries are properly maintained, the risk of unauthorized entry will remain. The numbers below for MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City refer to the nonexistent programs resident on each of the defined MVS systems. These programs may have multiple sensitive system capabilities; consequently, each program may contain more than one potential integrity weakness.

PPTs at MCCTA and MCCTA-Worldwide Support Division. For the 33 programs listed on the PPT with sensitive system capabilities, 9 programs did not exist. Three of the nine nonexistent programs could bypass file integrity (two users could access a file simultaneously), three could bypass file security (security software controls), and nine had system keys (see Appendix A, "Glossary"). We also identified one erroneous program entry that should be deleted from the PPT. These conditions existed on both systems.

PPT at DISO-Kansas City. Of the 74 total programs listed on the PPT of the 2 MVS/XA operating systems, 20 programs with sensitive system capabilities did not exist. Of the 20 nonexistent programs, 6 programs could bypass file integrity, 6 could bypass file security, and 20 had system keys. On each of the two DISO-Kansas City systems, we also identified two erroneous program entries to the PPT that should be deleted.

PPT at DFAS-Pensacola. Of the 61 programs listed on the PPT of the central design activity system and the DCPS partition at DISO-Denver, all programs with sensitive system capabilities were correctly installed.

Job Entry Subsystem 2 Parameters. On the MCCTA and MCCTA-Worldwide Support Division systems, job entry subsystem 2 (JES2) parameters did not completely control user submission of operator commands through job control language. This was an oversight, since the security software and initiator controls were used to control some of the jobs. As a result, separation of duties between programmers and operators was not clear. Some users could function as operators by submitting operator commands to deny service or shut the systems down. At DISO-Kansas City and DFAS-Pensacola, JES2 parameters and various exits effectively controlled the user submission of operator commands through job-control-language job streams (see Appendix A, "Glossary"). The internal readers (a means of transferring jobs to JES) on all systems controlled the submission of operator command groups.

JES2 Controls. JES2 parameters control the disposition of operator commands submitted in job control language. These parameters can allow no operator commands to be submitted, or can display the command and query the

operator by issuing a "Write to Operator with Reply." The write-to-operator-with-reply control asks the operator to verify whether the command should be executed. If the operator replies "Yes," the command is permitted. If the operator replies "No," the system ignores the command. The write-to-operator-with-reply control may not be effective without clear written guidance, since operators respond to hundreds of messages on each shift. In addition, exits and security software can be used to control the user submission of operator commands through JES2.

MCCTA and MCCTA-Worldwide Support Division. All 38 job input categories could submit all operator commands on each system. Thirty-six job input categories on each system were coded to provide write-to-operator-with-reply control over the submission of operator commands; however, control procedures were not documented. Although some compensating controls were provided by the CA-TOP SECRET security exit and initiator controls, six job input categories on the MCCTA system could submit operator commands.

Sensitive Utility Programs. Sensitive utility programs were not adequately controlled at DISO-Kansas City, DFAS-Pensacola, MCCTA-Worldwide Support Division, and to a lesser extent, at MCCTA. The information systems security officer had not evaluated vendor utilities for potential risks; therefore, programs were available to all system users at DISO-Kansas City and DFAS-Pensacola. Knowledgeable users could execute these utilities to destroy data on tape files, bypass security, or make unauthorized changes to programs or data to which they had access.

Controlling Utilities. Sensitive utility programs must be adequately controlled. Since users can add, delete, or modify records without modifying and running the programs normally used to maintain the files, sensitive utilities can alter data independently of normal safeguards. These utilities can also damage or destroy production programs and data files.

DISO-Kansas City. CA-TOP SECRET security software did not restrict the use of sensitive utilities. Two sensitive IBM utilities and one sensitive vendor utility required additional controls. The sensitive commands in the TMON/MVS utility (see Appendix A, "Glossary") were adequately controlled.

DFAS-Pensacola. Initially, CA-ACF2 security software did not control all sensitive utilities. Two IBM sensitive utilities and one sensitive vendor utility required additional controls. However, during the audit, DFAS-Pensacola systems personnel used the CA-ACF2 security software to restrict the use of all sensitive utilities.

MCCTA and MCCTA-Worldwide Support Division. Sensitive utilities were adequately controlled at MCCTA, with two exceptions. On one sensitive vendor utility at MCCTA, 115 user identifications (IDs) were attached. The initialization parameters on another vendor utility at MCCTA

were not set to fully activate the security features. At MCCTA-Worldwide Support Division, two IBM sensitive utilities and one vendor utility were not adequately controlled.

Summary

System programmers at MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola were not adequately monitoring APF libraries and programs. Programmers at DFAS-Pensacola had installed non-IBM SVCs on their systems, which compromised system integrity; however, the integrity exposures were corrected during our audit. At MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City, program names in the PPT were not adequately controlled. At MCCTA and MCCTA-Worldwide Support Division, JES2 parameters did not completely limit user submission of operator commands. Finally, at DISO-Kansas City, DFAS-Pensacola, MCCTA, and MCCTA-Worldwide Support Division, sensitive utility programs were not fully controlled. Collectively, these conditions weakened the integrity of MCCTA, DISO, and DFAS systems that process about $22.6 billion annually in disbursements.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Marine Corps Computer and Telecommunications Activity, Quantico, Virginia:

a. Develop the IBM-recommended installation integrity guidelines for the Marine Corps data processing installations. At a minimum, the guidelines should include specific requirements for administering the authorized program facility in accordance with IBM guidelines; formal procedures for reviewing supervisor calls to prevent compromises to operating system integrity; written procedures for initial and ongoing reviews of the program properties table; guidelines for evaluating job entry subsystem 2 parameters; and procedures for evaluating and controlling sensitive utilities.

b. Require the Chief, Marine Corps Computer and Telecommunications Activity, Worldwide Support Division, to:

(1) Formally review all current authorized program facility libraries, programs, and time-share-option commands on the production and test systems, and delete obsolete and undocumented programs.

(2) Periodically review the authorized program facility list on the production and test systems, and verify that it is kept up-to-date.

(3) Review all programs in the program properties table on the production and test systems and on systems at the serviced sites, and remove or control programs that no longer require special capabilities.

(4) Review job entry subsystem 2 parameters and associated security software controls on the production and test systems to verify that user-submitted operator commands are properly controlled.

(5) Define sensitive utilities to the Computer Associates, Inc., TOP SECRET security software as restricted programs; allow access only to personnel who have a clearly defined need; correctly install vendor utilities; and strictly control any one-time use of these utilities.

Management Comments. We did not receive comments from MCCTA.

Audit Response. MCCTA is requested to comment on the finding and recommendations by May 23, 1994. See the "Response Requirements for Each Recommendation" chart below for the specific requirements for your comments.

2. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Kansas City, Missouri:

a. Fully implement the IBM-recommended installation integrity guidelines currently being developed by the Director, Defense Information Services Organization.

b. Direct the Chief, Systems Programming, to:

(1) Formally review all current authorized program facility libraries, programs, and time-share-option commands on the production and test systems, and delete obsolete and undocumented programs.

(2) Periodically review the authorized program facility list on the production and test systems and verify that it is kept up-to-date.

(3) Define sensitive utilities to the Computer Associates, Inc., TOP SECRET security software as restricted programs; allow access only to personnel who have a clearly defined need; correctly install vendor utilities; and strictly control any one-time use of these utilities.

Management Comments. DISA, responding for the Director, DISA, fully concurred with the finding and recommendations and stated that corrective actions were either completed or ongoing.

3. We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, fully implement the IBM-recommended installation integrity guidelines currently being developed by the Director, Defense Information Services Organization. In

implementing those guidelines, particular emphasis should be placed on evaluating the integrity and security of time share options, authorized program facility commands, vendor supervisor calls, and sensitive utilities.

Management Comments. DFAS fully concurred with the finding and recommendations and stated that all operating system control deficiencies were corrected during the audit.

Response Requirements for Each Recommendation

Responses to the final report are required from the addressees shown for the items indicated with "X" in the chart below.

		Response Should Cover:			
Number	Addressee	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issues[1]
1.a.	MCCTA[2]	X	X	X	M, IC
1.b.	MCCTA	X	X	X	M, IC

[1]M = material weaknesses; IC = internal control.
[2]MCCTA = Marine Corps Computer and Telecommunications Activity.

Finding B. Implementation of Security Software

MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City had not properly implemented selected features of CA-TOP SECRET security software. DFAS-Pensacola had not fully implemented needed CA-ACF2 controls on all its systems. Specifically, the AUTOERASE security feature was not activated at MCCTA and DISO-Kansas City, and the tape security bypass control was not installed on the MCCTA-Worldwide Support Division test system and both DFAS-Pensacola systems. At MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City, special attributes (security bypass capabilities) were not limited to those applications that needed them. Finally, started task access at MCCTA-Worldwide Support Division and DFAS-Pensacola was not limited to the files needed to run the applications. At MCCTA-Worldwide Support Division, this occurred because security personnel had misinterpreted vendor guidance. Personnel at DFAS-Pensacola were not aware of security implications; therefore, access to specific started tasks was not identified. Improper use or setup of the CA-TOP SECRET security software features could allow knowledgeable users to perform unauthorized tasks (e.g., to access files without the authority to do so).

Background

CA-TOP SECRET and CA-ACF2 security software offers a variety of control options and features to enhance system security. When initially delivered, all software control options are set at default values provided by the vendor. As a computer center plans for its specific security needs, an administrative structure is developed. As part of the administrative structure, the control options and features of the security software should be set for the level of security needed. The level of protection offered depends on how well the options and features of CA-TOP SECRET and CA-ACF2 are administered.

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988, required that all AISs that process sensitive unclassified information requiring controlled access protection were to have C2 security classifications by 1992. For C2 controlled access protection, DoD Standard 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria (C3I)," December 1985, requires that all datasets be protected, that residual information be erased from on-line disk devices, and that jobs entered through JES2 be checked for a valid user ID and password.

AUTOERASE Option

The AUTOERASE security software option had not been activated at either MCCTA or DISO-Kansas City because they had problems with implementation and activating the option slowed computer performance. However, they did not request the waiver required by DoD Directive 5200.28. Consequently, residual data on disk devices may not have been fully erased, which would allow unauthorized users to view sensitive data. MCCTA-Worldwide Support Division and DFAS-Pensacola (CA-ACF2 site) activated the AUTOERASE feature of their security packages. During the audit, MCCTA activated the AUTOERASE option.

Tape Security Bypass

MCCTA-Worldwide Support Division and DFAS-Pensacola had inadequately secured CA-1 tape management processing by failing to install the Expiration Date (EXPDT)=98000 process (the CA-TOP SECRET and CA-ACF2 feature that restricts the bypassing of checks on the tape management system). The EXPDT=98000 job-control-language substatement tells MVS that the requested tape is not in the CA-1 tape management system (which controls tape processing), and that MVS should process the tape as requested. The interface control of EXPDT=98000 processing does not prevent coding this substatement in job control language, but controls its use as a security bypass. The control ensures that when both the volume and file name are in the tape management system, the EXPDT=98000 substatement is ignored, and normal security checking is accomplished. Although CA-TOP SECRET, version 4.3, lacked documentation for the EXPDT=98000 substatement, this control was clearly documented in version 4.2 and should have been installed. At DFAS-Pensacola, systems personnel were not aware that this control was available. During the audit, security personnel at both locations corrected the problem.

Special Attributes

The use of special attributes should be reevaluated. At MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City, the use of CONSOLE, NODSNCHK, NOVOLCHK, NORESCHK, and NOSUBCHK were not adequately controlled. The CONSOLE attribute allows CA-TOP SECRET control options to be changed, which would allow any ACID (accessor identification) with this attribute to change the CA-TOP SECRET environment. NODSNCHK and NOVOLCHK attributes bypass all security checking at the dataset or volume level, respectively. NORESCHK allows the use of any terminal, program, certain applications, or user resources protected by CA-TOP SECRET. NOSUBCHK allows jobs to be submitted with any user ID. Since

these attributes bypass some form of security checking, their use requires prudent assignment. During the audit, MCCTA-Worldwide Support Division reevaluated these special attributes and reduced them to a reasonable level.

DISO-Kansas City. Over 50 user IDs had the CONSOLE attribute or were attached to a profile with this capability. Thirty-two user IDs were in the Customer Service Branch, and four were in the Hardware Systems Branch. One of the user IDs in the Hardware Systems Branch belonged to a non-Government field engineer. The other user IDs were in the Security Branch and the System Programming Branch. Since the CONSOLE attribute allows users to change control options, this attribute requires tight control.

MCCTA. The use of the NODSNCHK, NOVOLCHK, NORESCHK, and NOSUBCHK attributes should be reevaluated. One hundred user IDs were assigned to NODSNCHK, 105 to NOVOLCHK, 118 to NORESCHK, and 79 to NOSUBCHK. Most of these user IDs were assigned to started tasks. This occurred because Information Systems Security Office branch personnel misunderstood the application bypass requirements. As a result, the potential for bypassing security controls was increased.

MCCTA-Worldwide Support Division. The use of the NODSNCHK, NOVOLCHK, NORESCHK, and CONSOLE attributes needed to be re-evaluated. Fifty-one user IDs were assigned to NODSNCHK, 75 to NOVOLCHK, 57 to NORESCHK, and 81 to CONSOLE. Most of these user IDs were assigned to started tasks. Generally, the CONSOLE attribute was assigned to system programmers who worked shifts at the Marine Corps Operations Center. Although security bypasses are needed for certain software, the indiscriminate use of these attributes increases the risk of bypassing security. During the audit, the information systems security officer reevaluated these special attributes and reduced them to reasonable levels.

Started Task Access

Access granted to started task IDs at MCCTA-Worldwide Support Division and DFAS-Pensacola was not adequately controlled. Generally, started tasks were correctly defined to CA-TOP SECRET at MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City.

MCCTA-Worldwide Support Division. MCCTA-Worldwide Support Division allowed "*." file access to most started tasks. Using the asterisk wildcard (see Appendix A, "Glossary") in this manner allows access to all files at the installation. Normally, started tasks need only the ability to execute long-running system software or applications. With this excessive access, the operator could change certain system libraries and compromise the integrity of the system.

DFAS-Pensacola. Started tasks should be controlled by limiting access for APF-protected datasets. There were 35 started tasks on the central design

activity system and 27 on the DISO-Denver system (DCPS-only partition); only one of these started tasks was defined to CA-ACF2 security software. This occurred because security personnel gave the tasks unlimited access in order to avoid interruptions in system operations. As a result, modifications to the system could result, and integrity of the systems was not assured.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Kansas City, Missouri:

a. Require the designated approving authority to formally evaluate the adverse impact of using the AUTOERASE option on systems at that location.

b. Activate the AUTOERASE option on systems at the Defense Information Services Organization, Information Processing Center, Kansas City, Missouri, or obtain a waiver of the requirement if appropriate. If a waiver is appropriate, formally document other safeguards that achieve the required level of system security.

c. Require the Information Systems Security Officer to review the need for assigning the CONSOLE attribute to a large number of systems personnel. Its use should be limited to the minimum number of personnel in order to prevent changes to the Computer Associates International, Inc., TOP SECRET control options.

Management Comments. DISO concurred with the finding and recommendation, except in one respect. Because of the need to respond when the production system is down, DISO did not fully agree to further limit the number of systems personnel with the CONSOLE attribute. DISO stated that the CONSOLE attribute was required to issue mainframe Console Operator Commands, which START/STOP all system started tasks to include TSS. DISO stated that systems personnel require this authority to respond to system outages during nonprime hours. See Part IV for the full text of management's comments.

Audit Response. We agree that the CONSOLE attribute is needed to START/STOP TSS (CA-TOP SECRET), but it is not required to START/STOP other system started tasks. DISO should be able to further reduce the number of production scheduling personnel with the CONSOLE attribute. Based on this clarification, we request that DISO reconsider its position and provide comments on the recommendation by May 23, 1994. See the "Response Requirements for Each Recommendation" chart below for the specific requirements for your comments.

2. We recommend that the Chief, Marine Corps Computer and Telecommunications Activity, Worldwide Support Division, require the Information Systems Security Officer to:

a. Review the use of special attributes on the Marine Corps Computer and Telecommunications Activity's production system, and limit their use to where it is clearly needed.

b. Limit the started task access on the test system to the files needed to run the applications.

Management Comments. MCCTA-Worldwide Support Division did not provide comments on the finding or recommendation.

Audit Response. We request that MCCTA-Worldwide Support Division provide comments on the finding and recommendation by May 23, 1994. See the "Response Requirements for Each Recommendation" chart below for the specific requirements for your comments.

3. We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, direct the Information Systems Security Officer to identify, on both systems, all started tasks to the Computer Associates International, Inc., Access Control Facility 2 security software, and grant appropriate access to each started task.

Management Comments. DFAS fully concurred with the finding and recommendations and stated that corrective actions were implemented.

Response Requirements for Each Recommendation

Responses to the final report are required from the addressees shown for the items indicated with "X" in the chart below.

		Response Should Cover:			
Number	Addressee	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issues[1]
1.c.	DISO[2]	X	X	X	M, IC
2.a.	MCCTA[3]	X	X	X	M, IC
2.b.	MCCTA	X	X	X	M, IC

[1]M = material weaknesses; IC = internal control.
[2]DISO = Defense Information Services Organization Information Processing Center, Kansas City, Missouri.
[3]MCCTA = Marine Corps Computer and Telecommunications Activity.

Finding C. Management Controls Over MVS Maintenance

Management controls over MVS maintenance at all four organizations needed improvement. Specifically, inadequate controls existed over changes to the operating system at DFAS-Pensacola. Sensitive system programmer positions at all four organizations were not consistently designated as critical-sensitive positions, and the required background investigations for those positions were not always obtained. Backups of critical operating system software at three organizations were not stored off-site. Inadequate change controls at DFAS-Pensacola existed because standard change control procedures had not been prepared. At the two Marine Corps organizations, the requirements were not met for monitoring the sensitivity ratings of position descriptions and for requesting or conducting background investigations. At the DISO and DFAS organizations, management did not request background investigations because the system programmer positions had not been appropriately rated critical-sensitive. Backups of critical operating system files were not stored off-site at MCCTA because the impact of changing the way files were named was not adequately addressed. Management of MCCTA-Worldwide Support Division did not see the need to back up computer systems that operated in a test environment. DFAS-Pensacola had not requested off-site storage as required by their operational support agreement. As a result, the integrity of the MVS operating systems and the continuity of computer operations were threatened.

Background

Management controls for the operating system should include selection of 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.

MVS Change Control Procedures

Inadequate controls existed over changes made to the operating system at DFAS-Pensacola. DFAS-Pensacola had not published standard change control procedures specifying the process for approving, documenting, and

implementing changes to the operating system. Since standard procedures did not exist, there was no assurance that the changes made were properly authorized, documented, or implemented. Improper control of operating system changes can allow the introduction of unauthorized or inaccurate computer programs that could compromise an operating system's integrity. Since any software change can have dramatic and unexpected effects, changes must be properly defined, planned, coordinated, tested, and implemented. DFAS-Pensacola had selected a system information management utility that was intended to provide a central, structured environment for change management. To ensure that MVS integrity is maintained, the utility should be linked to formal procedures that require strict controls over changes to the operating system software.

Designation of Programmer Positions

System programmer designations at MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola were not appropriate. Military billets for technical support positions at MCCTA, MCCTA-Worldwide Support Division, and DISO-Kansas City had Military Occupational Specialty (MOS) codes for Occupational Field 40, Data Systems. Background investigations were not required for the Data Systems MOS; therefore, they had not been conducted for all military personnel in technical positions at these locations. However, background investigations should have been performed, since these positions were considered critical-sensitive.

Position descriptions for personnel in the technical support areas at MCCTA and MCCTA-Worldwide Support Division, with one exception, supported critical-sensitive ratings. However, background investigations had not been conducted for all personnel. Specifically, eight civilian positions were rated critical-sensitive, and one position was rated noncritical-sensitive. Employees in three positions had not had background investigations. Sensitivity ratings and background investigation requirements were emphasized, but the requirements were not being monitored to ensure that position descriptions were written to support critical-sensitive ratings, and that background investigations were requested or updated when appropriate.

Designated technical support positions for civilians at DISO-Kansas City and DFAS-Pensacola were not appropriately rated critical-sensitive; therefore, the required background investigations were not obtained. At DISO-Kansas City, 11 civilian positions were rated either noncritical-sensitive or nonsensitive. At DFAS-Pensacola, all 13 civilian positions were rated noncritical-sensitive. Since classified information is not processed on the operating systems at DISO-Kansas City or DFAS-Pensacola, management determined that the higher critical-sensitive rating was unnecessary. The positions at both locations were for computer system programmers, computer specialists, and supervisory computer specialists. Since personnel in these positions have considerable access and are responsible for the operating system's installation and maintenance, the higher designation is needed as a control.

System programmers represent the most critical security exposures in data processing center operations. Their personal integrity is the most effective control. DoD Regulation 5200.2-R, "DoD Personnel Security Program, C3I," January 1987, requires that all DoD military and civilian personnel who work on unclassified automated information systems should have one of three position sensitivity designations in accordance with Appendix K, with investigations conducted as required for the sensitivity level. Appendix K requires, in part, that positions of all employees who ". . . can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage . . ." should be designated critical-sensitive, and that these employees should have background investigations. Without this designation, management has less assurance that programmers are trustworthy.

Off-Site Storage of System Backups

Backups of critical MVS operating system files at MCCTA, MCCTA-Worldwide Support Division, and DFAS-Pensacola were not stored off-site. MCCTA used a tape management system to automatically schedule the rotation of operating system tapes for off-site storage. Backup tapes were being made for all 11 volumes containing the key MVS operating system files; however, 3 of those 11 volumes were not shipped to the off-site location. However, there was a change in requirements for file naming. Because the overall impact of that change was not fully determined, the three volumes were not identified by the MCCTA tape management system as requiring off-site storage.

The MVS operating system files at MCCTA-Worldwide Support Division were periodically backed up; however, the backup tapes were stored in an on-site tape library, not off-site. Because MCCTA-Worldwide Support Division's computer system operated in a test environment, management had not determined that off-site storage of operating system backup tapes was required. Backups were also made of the operating system files at DFAS-Pensacola, but they were not being rotated to off-site storage. In its support agreement, DFAS-Pensacola did not formally request that the Naval Computer and Telecommunications Station at Pensacola, Florida, store system backups at an off-site location.

When computer assets are damaged or destroyed by fire or other disasters, computer processing can continue with minimal disruption of normal business operations by reloading critical system backups. If system backups are not stored off-site, the backups may be destroyed, thus unnecessarily disrupting business operations.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Marine Corps Computer and Telecommunications Activity:

a. Require that all sensitive system programmer positions be designated critical-sensitive and that background investigations be obtained for personnel assigned to those positions.

b. Periodically verify the accuracy of the tape management system's inventory list to guarantee that all key Multiple Virtual Storage libraries are backed up and stored off-site.

c. Direct the Chief, Marine Corps Computer and Telecommunications Activity-Worldwide Support Division, to periodically back up and store at an off-site location all key Multiple Virtual Storage libraries for the test system.

Management Comments. We did not receive comments from MCCTA.

Audit Response. MCCTA is requested to comment on the finding and recommendation by May 23, 1994. See the "Response Requirements for Each Recommendation" chart below for the specific requirements for your comments.

2. We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Pensacola:

a. Require the Director, Technology Support Activity, to establish formal change management procedures to control the processing of all changes to the Multiple Virtual Storage operating system.

b. Require that all sensitive system programmer positions be designated critical-sensitive and that background investigations be obtained for personnel assigned to those positions.

c. Request that the Naval Computer and Telecommunications Station, Pensacola, Florida, store backups of critical Multiple Virtual Storage operating system files at an off-site location.

Management Comments. DISA, responding for the Director, DISO, fully concurred with the recommendation and stated that corrective actions would be completed by July 31, 1994.

3. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Kansas City, require that all sensitive system programmer positions be designated critical-sensitive and that background investigations be obtained for personnel assigned to those positions.

Management Comments. DFAS fully concurred with the finding and recommendation and stated that corrective actions would be completed by April 30, 1994.

Response Requirements for Each Recommendation

Responses to the final report are required from the addressees shown for the items indicated with "X" in the chart below.

		Response Should Cover:			
Number	Addressee	Concur/ Nonconcur	Proposed Action	Completion Date	Related Issues[1]
1.a.	MCCTA[2]	X	X	X	M, IC
1.b.	MCCTA	X	X	X	M, IC
1.c.	MCCTA	X	X	X	M, IC

[1]M = material weaknesses; IC = internal control.
[2]MCCTA = Marine Corps Computer and Telecommunications Activity.

Part III - Additional Information

Appendix A. 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 other users' data, or from performing unauthorized actions. When applied to software, access control usually refers to a specialized software security package such as CA-TOP SECRET or CA-ACF2.

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 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. When a program can perform sensitive functions outside of established APF rules, it 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. Accounts receivable, general ledger, payroll, and personnel programs are some types of application programs.

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

Designated approving authorities are responsible for reviewing and approving security safeguards for automated information systems, and for issuing accreditation statements for each automated information system under their jurisdiction.

Database is a collection of interrelated data that are stored together.

Default values are parameters that take effect if they are not overridden by the data processing center. Vendors normally provide default values in their various computer applications.

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

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

Front-ending is the method by which vendor products and installations use "need access capability" within an operating system where no other program is available. For example, the SVC table entry calls up the vendor program before the normal SVC entry.

Internal reader is a means of transferring jobs to JES. If unrestricted, it also allows users to submit operator commands. Operator commands are authorized by command group; the groups include JES, MVS/XA, Input/Output (I/O), and display commands.

JES stands for job entry subsystem. JES is IBM's job management routine that reads the job stream and assigns jobs to class queues (computer data or programs awaiting processing). It processes jobs and manages system input and output processing. JES parameters control how and with what restrictions jobs will be run on a computer system. The two types of JESs available for an MVS/XA operating system are JES2 and JES3. MCCTA, MCCTA-Worldwide Support Division, DISO-Kansas City, and DFAS-Pensacola use JES2.

JES 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 2 additional 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.

Library is a collection of related data files or programs.

MVS/XA is the IBM multiple virtual storage operating system with extended architecture.

Partitions are logical divisions of a mainframe computer. Each partition is an independent system and has its own operating system.

PPT is the program properties table. It contains the names of special programs, including their codes and properties. Some MVS/XA programs are allowed special privileges not normally permitted by the operating system. A list of these programs, including their special privileges, is maintained in MVS/XA, 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 (system key). All of these are potential threats to system integrity.

It is important 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 either in a special library created and controlled by the installation, or in two IBM default libraries. The programs 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.

Read access is a security feature that allows a user only to read, execute, or copy a file.

Sensitive utilities are computer programs that provide general support for computerized processes (e.g., 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 the system's security software or internal 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.

Started task is an operating system job or application program initiated from an operator console.

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.

System key is a hardware storage protection feature of the MVS/XA operating system. The hardware provides 15 different keys. In MVS, keys 0-7 are reserved for system use. A system key can affect the integrity of the operating system.

TMON/MVS is a utility program developed by Landmark Corporation. It has sensitive functions that need to be properly controlled to prevent serious integrity exposures to the operating system.

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, the operating system, or users. Examples include copying, sorting, and merging files.

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

Wildcards are used to perform the same task for a group of computer files without repeating the same command for each filename in the group. The asterisk (*) wildcard acts as a substitute for a name or extension and can represent a whole word or group of characters.

Appendix B. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
A.1.a.	Internal control. Implements IBM installation integrity guidance, to include APF administration policy; SVC integrity evaluation; PPT controls; evaluation of JES2 parameters; and sensitive utility controls.	Nonmonetary.
A.1.b.	Internal control. Implements APF administration guidelines. Cleans up APF files. Cleans up PPT by removing unneeded programs, and deactivates privileges that are not needed. Reviews JES2 parameters and sensitive utility controls.	Nonmonetary.
A.2.a., A.2.b.	Internal control. Implements IBM integrity controls at DISO-Kansas City. Develops procedures on how to review APF file access. Implements sensitive utility controls at DISO-Kansas City. Makes use of CA-TOP SECRET to control sensitive utilities.	Nonmonetary.
A.3.	Internal control. Implements APF administration guidelines. Implements time-share-option APF command and SVC reviews at DFAS-Pensacola. Implements reviews of new utilities.	Nonmonetary.

Appendix B. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
B.1.a., B.1.b.	Internal control. Determines how use of the AUTOERASE feature will affect resources. Determines the risk of not using AUTOERASE; allows substitute controls to be documented. Activates AUTOERASE control if a waiver is not appropriate.	Nonmonetary.
B.1.c.	Internal control. Controls the use of the CONSOLE attribute.	Nonmonetary.
B.2.a., B.2.b.	Internal control. Allows security bypass attributes to be used only where needed. Limits started task access to the specific files that need to be run. Reduces the risk of unauthorized access.	Nonmonetary.
B.3.	Internal control. Limits started task access to the specific files that need to be run. Reduces the risk of unauthorized access.	Nonmonetary.
C.1.b., C.1.c., C.2.a., C.2.c.	Internal control. Provides for improved control over MVS system maintenance. At MCCTA, provides for sending of backup files to off-site locations.	Nonmonetary.
C.1.a., C.2.b., C.3.	Internal control. Provides for the designation of sensitive system programmer positions as critical-sensitive, and for conducting background investigations on personnel in these positions.	Nonmonetary.

Appendix C. Organizations Visited or Contacted

Department of the Navy

Marine Corps Computer and Telecommunications Activity, Quantico, VA
  Marine Corps Computer and Telecommunications Activity, Worldwide Support Division,[1] Quantico, VA

Defense Agencies

Headquarters, Defense Finance and Accounting Service, Washington, DC
  Defense Finance and Accounting Service, Kansas City Center, Kansas City, MO
  Defense Finance and Accounting Service, Financial Systems Activity,[2] Pensacola, FL
Headquarters, Defense Information Services Organization,[3] Denver, CO
  Defense Information Services Organization, Information Processing Center, Kansas City, MO

---

[1] The Marine Corps Computer and Telecommunications Activity, Worldwide Support Division, was formerly known as the Multifunctional Central Design Activity of the Defense Information Technology Services Organization. It is now a subordinate element of the Marine Corps Computer and Telecommunications Activity.

[2] Until August 8, 1993, the Defense Finance and Accounting Service, Financial Systems Activity, Pensacola, Florida, was known as the Defense Information Services Organization, Central Design Activity, Pensacola, Florida.

[3] The Defense Information Services Organization and its information processing centers were known as the Defense Information Technology Services Organization and its local information processing activities until they were reorganized effective September 7, 1993.

Appendix D. Report Distribution

Office of the Secretary of Defense

Comptroller of the Department of Defense
Assistant Secretary of Defense for Command, Control, Communications and Intelligence
Deputy Assistant Secretary of Defense for Information Systems

Defense Organizations

Commandant, U. S. Marine Corps
  Director, Marine Corps Computer and Telecommunications Activity
Director, Defense Finance and Accounting Service
  Director, Defense Finance and Accounting Service, Denver Center
  Director, Defense Finance and Accounting Service, Kansas City
Director, Defense Information Systems Agency
  Director, Defense Information Services Organization
    Director, Defense Information Services Organization, Information Processing Center, Denver, CO

Non-Defense Federal Organizations

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

Chairman and Ranking Minority Member of each of the following Congressional Committees and Subcommittees:

- Senate Committee on Appropriations
- Senate Subcommittee on Defense, Committee on Appropriations
- Senate Committee on Armed Services
- Senate Committee on Governmental Affairs
- House Committee on Appropriations
- House Subcommittee on Defense, Committee on Appropriations
- House Committee on Armed Services
- House Committee on Government Operations
- House Subcommittee on Legislation and National Security, Committee on Government Operations

Part IV - Management Comments

Defense Finance and Accounting Service

DEFENSE FINANCE AND ACCOUNTING SERVICE

WASHINGTON DC 20376-5001

FEB 5 1994

(Information Management)

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SERVICES ORGANIZATION
ATTN: MS. CYNTHIA K. ANTHOFER

SUBJECT: Draft Audit Report on Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service (Project No. F-0043.02)

Your memorandum, January 7,1994, subject as above, requested comments on each of the three findings from the report.

After reviewing the DoD, Inspector General (DoD(IG)) draft report and specifically the three findings and recommendations, the following are DFAS's comments and recommendations:

- In your memorandum, and throughout the draft IG report, there are references to the Defense Information Services Organization (DISO), Information Processing Activity (IPA) at Pensacola. For clarification, DMRD 918 transferred the DFAS Central Dsaign Activity (CDA) at Pensacola, which was not an IPA, to the Defense Information Systems Agency. The CDA at Pensacola became part of the Defense Information Technology Services Organization (DITSO), which was subsequently absorbed by DISO on July 26, 1993. On June 28, 1993, ASD(C3I) realigned certain Defense Components and, in compliance, the CDA at Pensacola was returned to the operational control of DFAS on August 8, 1993. Since that time, it has been called the Financial Systems Activity (FSA)-Pensacola.

- Page 2, paragraph 4 of the IG report addresses the use of the computers at Pensacola and Denver for the development and test of Defense Civilian Pay System (DCPS) and DCPS production. The actual development and testing of DCPS is handled only at FSA-Pensacola the actual production of DCPS is run on the MVS/XA partition at the DISO in Denver.

DFAS agrees with all of the findings and that all recommendations for corrective action should be implemented by the Security Officer from the appropriate organizations. Also attached are the comments FSA-PE, which you have already received and with which we concur, and additional control information provided by DFAS Center at Kansas City.

Enclosure 2

After further review of other recent DoD(IG) reports, it was found that the same findings and recommendations have surfaced at other Defense Information Services Organization (DISO), Information Processing Centers. The subject report stated that DoD Directive 5200.28 "Security Requirements for Automated Information Systems (AISs)," March 1988, requires all AISs processing sensitive, unclassified information have C2 security classification by 1992. DFAS agrees with that statement and it is our position that all of DFAS' data be provided the appropriate level of protection at all times.

If you have any questions, please contact Harry Johnson on commercial (703) 607-0747 or DSN 327-07471.

W. E. Daeschner
Deputy Director

Attachments

DEFENSE FINANCE AND ACCOUNTING SERVICE
KANSAS CITY CENTER
KANSAS CITY, MISSOURI 64197-0001

DFAS-KC/DI

FEB 0 2 1994

MEMORANDUM FOR DEPUTY DIRECTOR FOR INFORMATION MANAGEMENT, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: DoD(IG) Draft Report "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service" dated December 6, 1993 (Project No. 1FD-0043.02)

We have reviewed the findings of the subject report and concur with the recommendations for corrective action. The conditions detailed establish an unexceptable level of risk to our data integrity. However, there are process and procedural controls in place at this Center which provide our managers a level of assurance that data/systems integrity is being maintained (examples attached). The audit's "objective was to determine whether their management controls over selected features...to ensure the integrity of the Defense Finance and Accounting Service data." We can only assume that the readers accept the limited nature of the audit.

If you have any questions or concerns, my point of contact is Mr. J. W. Snyder. He may be reached at (816) 926-7141 or DSN 465-7141.

Gregory P. Bitz
Director

Attachment

OPTIONAL FORM 99 (7-90) NOTE changed wording from 1/21 DRAFT.

FAX TRANSMITTAL # of pages ▶ 2

To Harry Johnson	From Alice S. Arielly
Dept./Agency DFAS-HQ / SL	Phone # DFAS-KC/DI 816-926-7142
Fax # 703-607-2806	Fax # 816-926-1675

NSN 7540-01-317-7368 5099-101 GENERAL SERVICES ADMINISTRATION

ORIGINAL TO FOLLOW BY MAIL

Attachment

CURRENT CONTROLS

- Social Security validation process exists; the SSNs of new accessions are extracted monthly and are provided by magnetic tape to the Social Security Administration (SSA) who, in turn, provides us a magnetic tape (quarterly) of incorrect SSNs.
- Electronic signatures (ELSIGs) are used to control access to the On-Line Diary System (OLDS) for preparing and certifying transactions -- two (2) ELSIGs are currently required to submit a transaction into the production processing cycle.
- Monthly output reports are produced to provide information to help identify any fraudulent/erroneous payments.
- Up-front edits validate data entry; prevent erroneous input and may terminate pay and allowances.
- Control limitations are placed on money amounts.
- Error reports are monitored for timely correction/ revalidation.
- Audit trails exist for processed transactions.
- Monthly testing is done of a controlled population; entitlements, deductions, and disbursements are reviewed.
- Monthly Management Reports are reviewed.
- System Change Requests are documented and approved at two (2) levels of management.
- A payroll reconciliation process ensures payments are properly and accurately recorded.
- Electronic Fund Transfer (EFT) payments are validated prior to tape submission.
- Block control totals are used for the Reserve payroll process.

DEFENSE FINANCE AND ACCOUNTING SERVICE
FINANCIAL SYSTEMS ACTIVITY
280 RABY AVENUE
PENSACOLA, FLORIDA 32509-5128

1

January 24, 1994

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS ORGANIZATION
ATTN: RESOURCE MANAGEMENT

SUBJECT: Audit Report on Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service (Project No. 1FD-0043.02)

This memorandum is the Defense Finance and Accounting Service (DFAS), Financial Systems Activity - Pensacola response to the draft audit report of December 6, 1993.

The Defense Information Services Organization (DISO) Central Design Activity - Pensacola addressee referenced in the draft audit report is now the DFAS Financial Systems Activity - Pensacola (DFAS-FSAPS). This response combines comments for both the DFAS-FSAPS system located at the Naval Computer and Telecommunication Station (NCTS) Pensacola and the DCPS production system partition at DISO-Denver.

Attachment 1 addresses each finding and recommendation with FSAPS concurrence, comments, and planned actions.

My point of contact is Ron Shaeffer, DSN 922-2990 or Commercial (904) 452-2990, extension 329.

A. B. Johnson
Director

Attachment

Copy to:
FSO Denver (Dick Gustafson)

FINDINGS, RECOMMENDATIONS, AND PLANNED ACTION

Finding A. Operating System Controls

Recommendation 3: We recommend that the Director, Defense Information Services Organization, Central Design Activity, Pensacola, Florida, fully implement the IBM-recommended installation integrity guidelines currently being developed by the Director, Defense Information Services Organization. In implementing those guidelines, particular emphasis should be placed on evaluating the integrity and security of time share options, authorized program facility commands, vendor supervisor calls, and sensitive utilities.

Planned Action: Concur. All Operating System Control deficiencies for systems under the cognizance of the Defense Finance and Accounting Service, Financial Systems Activity - Pensacola (DFAS-FSAPE), as noted in the draft audit report were corrected during the course of the audit. The remaining recommendation for DFAS-FSAPE implementation of DISO guidelines, which are in the development stage, will be aggressively pursued when the guidelines are promulgated.

Finding B. Implementation of Security Software

Recommendation 5. We recommend that the Director, Defense Information Services Organization, Central Design Activity, Pensacola, Florida, direct the Information Systems Security Officer to identify, on both systems, all started tasks to the Computer Associates International, Inc., Access Control Facility 2 security software, and grant appropriate access to each started task.

Planned Action: Concur. Action complete. The following controls over started tasks have been implemented on both systems controlled by DFAS-FSAPE to correct the stated deficiency.

1. The ACF2 global STC feature was turned on (ACF2 default is OFF) and appropriate started task LID's were established to implement validation of data set access for all started tasks.

2. Access to controlled libraries is closely monitored and the number of personnel with the ability to effect changes to the controlled libraries is limited to the eight personnel assigned to the DFAS-FSAPE systems shop.

Finding C. Management Controls over MVS Maintenance

Recommendation 2.a. Require the Director, Technology Support Activity, to establish formal change management procedures to control the processing of all changes to the Multiple Virtual Storage operating system.

Planned Action: Concur. The ultimate goal is to incorporate the formal executive software configuration management standards which are being developed in conjunction with the site consolidation and standardization effort. However, since selection and incorporation of standard products and procedures for executive software configuration management is still a future event, interim procedures are being developed locally for configuration management of the executive software suites for the DFAS-FSAPE and DCPS production systems. Implementation of fully functional configuration management processes, mechanized through the CA-NETMAN software product, is being vigorously pursued by DFAS-FSAPE. To date, DFAS-FSAPE has procured and installed the CA-NETMAN product and identified all currently installed executive software products as components of the CA-NETMAN database to establish a baseline for inventory tracking and change management. Additional customization of the product and the development of applicable procedures is required to achieve a fully functional, user friendly environment for change management. The customization and development of local procedures is expected to be completed in approximately 180 days.

Recommendation 2.b. Require that all sensitive system programmer positions be designated critical-sensitive and that background investigations be obtained for personnel assigned to those positions.

Planned Action: Concur. The sensitive positions have been identified and actions initiated to effect the position description changes required to designate those positions as critical-sensitive. Estimated completion of position description changes and background investigations is 180 days.

Recommendation 2.c. Request that the Naval Computer and Telecommunications Station at Pensacola, Florida, store backups of critical MVS operating system files at an off-site location.

Planned Action: Concur. Since the audit, an Automated Cartridge System (ACS) silo has been installed and all backup tape operations have been switched from 9-track reels to cartridge in the ACS cartridge system. Action is being taken to develop procedures for identifying and ejecting the appropriate cartridges for routing to offsite storage and to effect the necessary changes to the level of service agreement between DFAS-FSAPE and NCTS Pensacola to implement offsite storage. Estimated completion of required actions is 180 days.

Defense Information Systems Agency

Final Report Reference

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

AGA

16 FEB 1994

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

SUBJECT: Audit Report on Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service (Project No. 1FD-0043.02)

Reference: DoDIG Memo, subject as above, 6 Dec 93

1. As requested by the reference, we have reviewed the subject draft audit report and are providing comments to recommendations addressed to the Director, Defense Information Services Organization (DISO), Information Processing Center (IPC), Kansas City (enclosure 1). Page 44

2. The audit report makes reference to the Central Design Activity (CDA) in Pensacola as an activity under our DISO. In fact, the CDA is a Defense Finance and Accounting Service (DFAS) element. Operational control of the CDA was returned to DFAS on 8 August 1993 per guidance from the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to realign Defense Components.

3. However, in order to expedite comments on the draft report, we requested the support of DFAS to review and provide comments on the Pensacola-CDA (renamed the Financial Systems Activity (FSA)). Their comments are provided at enclosure 2. Page 36

4. If you have questions on our response, contact Ms. Sandra Leicht, Audit Liaison, on (703) 692-5326 (DSN 222) for assistance.

2 Enclosures a/s

RICHARD T. RACE
Inspector General

DEFENSE INFORMATION SYSTEMS AGENCY (DISA)
MANAGEMENT COMMENTS ON
CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE
SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE
(PROJECT NO. 1FD-0043.02)

1. **FINDING A:** Operating System Controls

a. **Recommendation 2.a:** Fully implement the IBM-recommended installation integrity guidelines currently being developed by the Director, Defense Information Services Organization.

Planned Action: Concur. Work continues on the development of the IBM-recommended installation integrity guidelines. Once the guidelines are complete, we will ensure full implementation. Estimated completion date is 30 April 1994.

b. **Recommendation 2.b.(1):** Formally review all current authorized program facility libraries, programs, and time-share-option commands on the production and test systems, and delete obsolete and undocumented programs.

Planned Action: Concur. The following names will be removed from the SYS1.PARMLIB member named IKJTSO00: ABRSPF, COMPRESS, EMCICS17, MCS, OMEGAMON, OMSPFAU. The same named load library and member is used by both mainframes (re: test and production environments). Estimated completion date is 1 March 1994.

c. **Recommendation 2.b.(2):** Periodically review the authorized program facility list on the production and test systems and ensure that it is kept up-to-date.

Planned Action: Concur. We will conduct annual reviews as outlined in the recommendation. Initial review date will occur commencing 1 January 1995.

d. **Recommendation 2.b.(3):** Define sensitive utilities to the Computer Associates, Inc., TOP SECRET security as restricted programs; allow access only to personnel who have a clearly defined need; correctly install vendor utilities; and strictly control any one-time use of these utilities.

Planned Action: Concur. The following modules will be protected from general access by TOP SECRET: IEHINITT and ICKDSF. Access via the "ALL" record for the dataset name "FDRABR" will be revised to reflect only needed access. Again, the same named load library is utilized by both mainframes. Estimated completion date is 1 March 1994.

Enclosure 1

2. **FINDING B:** Implementation of Security Software

a. **Recommendation 1.a:** Require the designated approving authority to formally evaluate the adverse impact of using the AUTOERASE option on systems at that location.

Planned Action: Concur. We believe it would be prudent to conduct extensive analysis and testing before implementation of this option on our extremely active DASD configuration. Estimated completion date is 30 April 1994.

b. **Recommendation 1.b:** Activate the AUTOERASE option on systems at the Defense Information Services Organization, Information Processing Center - Kansas City, Missouri, or obtain a waiver of the requirement if appropriate. If a waiver is appropriate, formally document other safeguards that achieve the required level of system security.

Planned Action: Concur. See Planned Action and Estimated completion date for Recommendation 1.a.

c. **Recommendation 1.c:** Require the Information Systems Security Officer to review the need for assigning the CONSOLE attribute to a large number of systems personnel. Its use should be limited to the minimum number of personnel in order to prevent changes to the Computer Associates International, Inc., TOP SECRET control options.

Planned Action: Concur In Part. The CONSOLE authority is required to issue mainframe Console Operator Commands which START/STOP all system started tasks to include TSS. Regrettably, it also causes this concern by allowing the Facility Matrix Tables (FMT) to be modified by the same user. Our systems personnel require this authority in order to respond to production system outages during nonprime hours. The method of production operation and production scheduling within our Customer Services Branch does not currently lend itself to further restriction of this authority due to shift changes of personnel and fluctuating production schedules which may not coincide with shift assignments. We will restrict the user IDs within the Hardware Systems Branch to those occasions when needed. Estimated completion date is 1 March 1994.

3. **FINDING C:** Management Controls Over MVS Maintenance

Recommendation 3: Require that all sensitive system programmer positions be designated critical-sensitive and that all background investigations be obtained for personnel assigned to those positions.

Planned Action: Concur. Our proposed schedule for completing this recommendation will be identified by 30 April 1994.

Audit Team Members

Terry L. McKinney	Acting Director, Financial Management Directorate
David C. Funk	Audit Program Director
W. Andy Cooley	Audit Project Manager
Stephen A. Delap	Audit Project Manager
John A. Dedio	Senior Auditor
Frances Cain	Auditor
Thomas Hare	Auditor
Susanne B. Allen	Editor
Rosemary McCarthy	Administrative Support