Audit Report

OFFICE OF THE INSPECTOR GENERAL

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

Report No. 93-133 June 30, 1993

Department of Defense

Acronyms

AIS	Automated Information System
APF	Authorized Program Facility
DAA	Designated Approving Authority
DBMS	Defense Business Management System
DESC	Defense Logistics Agency Electronics Supply Center
DFAS	Defense Finance and Accounting Service
DITSO	Defense Information Technology Services Organization
DLA	Defense Logistics Agency
DPI	Data Processing Installation
DSAC	Defense Logistics Agency Systems Automation Center
GS	General Schedule
IBM	International Business Machines Corporation
IPA	Information Processing Activity
JCL	Job Control Language
JES2	Job Entry Subsystem 2
MOCAS	Mechanization of Contract Administration Services
MVS/XA	Multiple Virtual Storage with Extended Architecture
NAS	National Advanced Systems
PPT	Program Properties Table
RACF	Resource Access Control Facility
SMF	System Management Facility
SMP	System Modification Program
SMP/E	System Modification Program/Extended Architecture
SVC	Supervisor Call
TSO	Time Share Option
WTOR	Write to Operator with Reply

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

June 30, 1993

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION TECHNOLOGY SERVICES ORGANIZATION
COMMANDER, DEFENSE LOGISTICS AGENCY, SYSTEMS AUTOMATION CENTER
DIRECTOR, DEFENSE INFORMATION TECHNOLOGY SERVICES ORGANIZATION, DAYTON INFORMATION PROCESSING ACTIVITY
DIRECTOR, DEFENSE INFORMATION TECHNOLOGY SERVICES ORGANIZATION, COLUMBUS INFORMATION PROCESSING ACTIVITY

SUBJECT: Audit Report on Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service (Report No. 93-133)

We are providing this final report for your information and use. Comments on a draft of this report were considered in preparing the final report.

We determined that the Defense Logistics Agency Systems Automation Center, Columbus, Ohio; the Defense Information Technology Services Organization (DITSO), Dayton Information Processing Activity, Dayton, Ohio (formerly the Defense Logistics Agency Electronics Supply Center's data center); and the DITSO Columbus Information Processing Activity, Columbus, Ohio, had serious problems with operating system and security software controls. Any knowledgeable user could access, modify, or destroy sensitive DFAS computer data, programs, and other resources without leaving an audit trail.

Your comments on the draft of this report met the requirements of DoD Directive 7650.3. Since there are no unresolved issues, no further comments are required.

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. William A. Cooley, Project Manager, at (303) 676-7393 (DSN 926-7393).

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Audit Report No. 93-133 **June 30, 1993**
Project No. 1FD-0043.01

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

EXECUTIVE SUMMARY

Introduction. The operating system is a major component of any computer system. It is an integrated collection of computer programs, service routines, and supervising procedures that direct the sequence and processing of computer applications, and isolate and protect individual programs from one another. Security software provides access controls that restrict the use of computer resources to authorized individuals and limit those individuals to the computer resources required to perform their jobs. The audit concentrated on Defense Logistics Agency (DLA) and Defense Information Technology Services Organization (DITSO) information processing facilities supporting the Defense Finance and Accounting Service (DFAS) Center, Columbus, Ohio (DITSO-Columbus). DITSO-Columbus makes $67 billion in annual payments to more than 528,000 payroll and contract accounts.

Objective. Our objective was to determine whether management controls over selected features of the operating system and security software used at the DLA Systems Automation Center (DSAC), the DITSO-Dayton Information Processing Activity (IPA) (formerly the DLA Electronics Supply Center [DESC] data center), and the DITSO-Columbus IPA were adequate to ensure the integrity of DFAS-Columbus 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. We found that DSAC, DITSO-Dayton, and DITSO-Columbus had serious 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.

o Management needed to improve its controls over five of the nine operating system features we reviewed at DITSO-Dayton and DITSO-Columbus, and four of the nine we reviewed at DSAC. Application programs and data such as pay and accounting records could be added, modified, or deleted without detection, and the integrity of systems that process $67 billion annually in disbursements was not fully assured (Finding A).

o At DSAC, DITSO-Dayton, and DITSO-Columbus, security features of the Resource Access Control Facility (RACF) software had not been fully implemented. Therefore, authorized system users could perform unauthorized tasks (Finding B).

o At DSAC and DITSO-Dayton, management needed to improve change controls over operating systems. At all three locations, system programmer positions needed to be upgraded to critical-sensitive (Finding C).

Internal Controls. Neither DSAC, DITSO-Dayton, nor DITSO-Columbus had prepared the installation integrity guidelines recommended by International Business Machines Corporation (IBM), and controls over operating system features were undocumented and were not fully effective (Finding A). Security software controls were not effectively implemented (Finding B), and management controls over operating system maintenance and designation of system programmer positions needed improvement (Finding C). Since DITSO-Dayton and DITSO-Columbus process about $67 billion each year in disbursements, we consider this lack of documented control procedures to be a material internal control weakness as defined by Public Law 97-255, OMB Circular A-123, and DoD Directive 5010.38. See Part II of this report for additional details.

Potential Benefits of Audit. This audit disclosed serious deficiencies in the integrity and security of computer systems. Although no potential monetary benefits were identified, the audit heightened management's awareness of this highly technical general control area, and we recommended specific actions to eliminate these deficiencies and ensure data integrity. Appendix B summarizes the benefits resulting from the audit.

Summary of Recommendations. The recommendations in this report are directed to the Commander, DSAC; the Director, DITSO-Dayton; and the Director, DITSO-Columbus. We recommended additional regulatory compliance, enhanced internal controls, formal change control procedures, and additional training for security personnel.

Management Comments. The Director, Defense Information Technology Services Organization, concurred with the findings and recommendations in the draft report. The Director, DITSO, also concurred with the internal control weaknesses highlighted in Part I.

Table of Contents

This report was prepared by the Financial Management Directorate, Office of the Inspector General for Auditing, Department of Defense. Copies of the report can be obtained from the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, (703) 614-6303 (DSN 224-6303).

Part I - Introduction

Background

The Defense Logistics Agency Systems Automation Center (DSAC) in Columbus, Ohio, develops standard systems for the Defense Logistics Agency (DLA) and the Defense Finance and Accounting Service (DFAS). DSAC also builds the Multiple Virtual Storage with Extended Architecture (MVS/XA) operating system that it exports and implements at DLA data processing installations (DPIs). DSAC provides the MVS/XA operating system for the five mainframe computers used by the Defense Information Technology Services Organization's Columbus Information Processing Activity (IPA), Columbus, Ohio (DITSO-Columbus).

The DFAS-Columbus Center provides financial and accounting services and disbursing operations for Mechanization of Contract Administration Services (MOCAS), stock funds, civilian payroll services, and general accounting, including travel and commercial contract payments. DITSO-Columbus and the DITSO-Dayton IPA (formerly the Defense Logistics Agency Electronics Supply Center (DESC) data center in Dayton, Ohio), provide information processing support so that the DFAS-Columbus Center can maintain more than 528,000 pay accounts and process a total of about $67 billion per year in payments.

The DSAC operates two IBM mainframe computers. We reviewed only the MVS/XA system that runs on one IBM 3084 mainframe computer. DSAC personnel use this computer to test standardized applications and third-party software, and to build and customize operating systems for 20 locations. DITSO-Dayton operated two Amdahl 5870 mainframe computers using the MVS/XA operating system. The Amdahl 5870 computers run the Defense Business Management System (DBMS) for DFAS, the Executive Office of the President, and the Defense Commissary Agency.

The DITSO-Columbus IPA operated five mainframe computers using the MVS/XA operating system. The five mainframe computers include four Amdahl computers (one 5880 and three 5870s) and one National Advanced Systems (NAS) 9080 mainframe computer. The five mainframe computers run DBMS and MOCAS.

Both DITSO information processing activities process unclassified sensitive data on their systems. Government programmers at DSAC, DITSO-Dayton, and DITSO-Columbus maintain the operating system and security software.

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 direct 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 separate and protect individual user programs. DSAC,

DITSO-Dayton, and DITSO-Columbus 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 ensure 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 in order to ensure system integrity.

Access Controls. Access controls allow only authorized employees to use computer resources, and to use only the resources needed to perform their jobs. Computer resources include files, programs, tapes, data base definitions, libraries, readers, and processing capabilities. DSAC, DITSO-Dayton, and DITSO-Columbus use the IBM Resource Access Control Facility (RACF) security software to provide access control. When properly installed and administered, commercial security software packages such as RACF 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 DSAC, DITSO-Dayton, and DITSO-Columbus were adequate to ensure 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

We performed audit work at DSAC, DITSO-Dayton, and DITSO-Columbus. We evaluated 11 areas that can affect the integrity of operating system and security software. These areas were the authorized program facility (APF); supervisor calls (SVCs); time share option (TSO); system modification program (SMP); system management facility (SMF); program properties table (PPT); job entry subsystem 2 (JES2); exits; sensitive utilities; the implementation of the RACF security software; and management controls.

We used CA-EXAMINE auditing software to extract data from computer memory and from 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 RACF security software package 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. Due to the security considerations of this audit, deficiencies are described in general terms.

Audit Period, Locations, and Standards. This program audit was performed from April 1992 through October 1992. 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. From April 1992 through October 1992, we reviewed operating system data at the three locations. During the audit, we contacted or visited the locations shown in Appendix C.

Internal Controls

We evaluated general controls dealing with operating systems, security, change controls, and personnel. We identified material internal control weaknesses as defined by Public Law 97-255, Office of Management and Budget Circular A-123, and DoD Directive 5010.38. Specifically, controls were not adequate to prevent serious 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. Although each location had implemented a DLA Internal Management Control Program that included FMFIA requirements, the programs did not identify specific operating system and security software controls that should be reviewed. All recommendations in this report, if fully implemented, will correct the weaknesses. We could not quantify the monetary benefits to be realized by correcting the internal control deficiencies, since the recommended preventative controls will deter undesired events. A copy of the final report will be provided to the senior officials responsible for internal controls at DSAC and DITSO.

Prior Audits and Other Reviews

Four 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. The second report, issued by the IG, DoD, was "Management of Access Controls to Computers at the

Defense Logistics Agency," Report No. 89-058, 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.

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

The fourth audit report, issued by the IG, DoD, was "Controls Over Operating System and Security Software Supporting the Defense Accounting Service," Report No. 93-002, October 2, 1992. The audit showed that the DITSO Information Processing Centers at Cleveland, Ohio, and Indianapolis, Indiana, had serious problems with operating system and security software controls.

We identified similar deficiencies at DSAC, DITSO-Dayton, and DITSO-Columbus. No audits of the operating system had been conducted previously at these locations; however, IG, DoD, Report No. 89-058 showed that sensitive utilities were not adequately controlled at DLA's DPI in Columbus, Ohio (now DITSO-Columbus). We were unable to evaluate management's corrective actions because a new security software package (RACF) had been installed after that audit. Although we found the same deficiency, DITSO-Columbus managers were learning to use the RACF security software effectively. Since the implementation of a new security software package is a large project, we did not consider this deficiency to be a repeat audit finding.

This page was left out of original document

Part II - Findings and Recommendations

Finding A. Operating System Controls

On five of the nine operating system features reviewed at DSAC, DITSO-Dayton, and DITSO-Columbus, controls needed improvement. Specifically, authorized program facility libraries and programs were not adequately monitored and controlled; programmers at DSAC had installed non-IBM supervisor calls that compromised system integrity; program names in the program properties table were not adequately controlled; job entry subsystem 2 parameters did not control user submission of operator commands at DITSO-Dayton and DITSO-Columbus; and control over sensitive utility programs was not adequate. Since DSAC, DITSO-Dayton, and DITSO-Columbus had not prepared the installation integrity guidelines recommended by IBM, controls over the MVS/XA operating system were undocumented and not fully effective. 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 $67 billion annually in disbursements was not ensured.

Data Integrity

Authorized Program Facility. Authorized program facility (APF) libraries and programs were not adequately monitored, and update access (the ability to view and change libraries and programs) to APF libraries was not properly controlled. This occurred because management lacked clear, written APF control procedures; access rules were too generous; and programmers' needs for update access to APF libraries were not periodically reviewed. Retaining obsolete programs could significantly reduce available computer storage. Users could create unauthorized programs in APF libraries; bypass access security; and add, modify, or delete sensitive pay and contract data files without detection.

APF Library Controls. Of the 315 APF libraries and 7,071 APF authorized programs at DSAC, DITSO-Dayton, and DITSO-Columbus, we found 46 obsolete or undocumented libraries; 3 nonexistent libraries; and 1,375 obsolete or undocumented programs. We also found that 25 libraries on the 8 systems were designated as APF-authorized, although vendor documentation did not require it. Users could make their own libraries authorized by assigning them to the APF list, and could accidentally or intentionally access, modify, or destroy information, programs, or other sensitive computer resources.

Access to APF-Authorized Files. Access to update APF libraries at DSAC, DITSO-Dayton, and DITSO-Columbus was not adequately controlled. At DSAC, 1600 individuals could update 1 APF library. When notified of this condition, management reduced this authorization to 12 users.

Also, up to 385 DSAC users could update 63 APF libraries. One of these libraries was in the warn mode (see Appendix A, "Glossary"). All system users could access and update the library; the only control was that their access was recorded so that managers could review it.

At DITSO-Columbus, up to 71 users could update 182 APF libraries on the 5 systems, and 4 of these APF libraries were in the warn mode. At DITSO-Dayton, up to 45 users could update 62 APF libraries on the 2 systems, and 25 of these libraries were in the warn mode. During the audit, DITSO-Dayton management put 22 of these 25 libraries into fail mode (see Appendix A, "Glossary"), thus limiting access to a smaller number of authorized users.

Ideally, no individual should have standing authority to update APF libraries or control tables that define APF libraries and programs to the operating system. Although this restriction may not always be practical at system programming activities such as DSAC, DITSO-Dayton, and DITSO-Columbus, access must be kept to the minimum needed to perform software maintenance.

Controls Over Supervisor Calls. On the DSAC, DITSO-Dayton, and DITSO-Columbus systems, DSAC programmers had installed non-IBM supervisor calls (SVCs) that compromised system integrity. On the DSAC system, 5 user/vendor SVCs did not provide adequate controls; 6 SVCs on the 2 systems at DITSO-Dayton and 12 SVCs on the 5 systems at DITSO-Columbus were also inadequate. This occurred because information systems personnel at DSAC 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.

IBM SVCs. At DSAC, DITSO-Dayton, and DITSO-Columbus, we reviewed 107 of 857 IBM-numbered SVCs on 8 systems. We contacted vendors about 7 IBM SVCs (45 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 107 SVCs compromised system integrity.

User/Vendor SVCs. At DSAC, DITSO-Dayton, and DITSO-Columbus, we reviewed 64 user-installed SVCs. SVCs (23 SVCs at all locations) did not have adequate validity checking and presented significant exposures to system integrity. Since DSAC system programmers agreed with our assessment, we did not test these SVCs further. For the remaining 41 SVCs, our review of SVC code (see Appendix A, "Glossary") and vendor documentation did not show any additional risks to system integrity. Since DSAC builds MVS and MVS/XA operating systems for all of DLA's DPIs, these five SVCs are installed in various combinations at the DPIs, weakening the systems' integrity.

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 (see Appendix A, "Glossary") programs could be substituted for missing PPT programs. Users could also access data controlled by another job stored anywhere in the operating system, bypassing security software controls altogether.

PPT Controls. Program names must be kept in a special library controlled by the DPI 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 APF controls are strengthened, the risk of unauthorized entry will remain.

The numbers below for DSAC, DITSO-Dayton, and DITSO-Columbus 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.

PPT at DSAC. We found that of the 79 programs listed on the PPT with sensitive system capabilities, 20 programs did not exist. Of these, 5 programs that could bypass file integrity (2 users could access a file simultaneously), 10 that could bypass file security (security software controls), and 7 that had system keys (see Appendix A, "Glossary") were nonexistent. We also identified four DSAC programs as obsolete.

PPT at DITSO-Dayton. Of the 143 total programs listed on the PPT of the 2 MVS/XA operating systems, 54 programs with sensitive system capabilities did not exist. Of these, 11 programs that could bypass file integrity, 27 that could bypass file security, and 20 that had system keys were nonexistent. We also identified 17 programs on each of the 2 DITSO-Dayton systems as obsolete.

PPT at DITSO-Columbus. Of the 335 programs listed on the PPT of the 5 MVS/XA operating systems, 108 programs with sensitive system capabilities did not exist. Of these, 25 programs that could bypass file integrity, 53 that could bypass file security, and 40 that had system keys were nonexistent. We also found that eight programs on each of the five systems were obsolete.

Job Entry Subsystem 2 Parameters. On two systems at DITSO-Dayton and five at DITSO-Columbus, job entry subsystem 2 (JES2) parameters did not control user submission of operator commands through job control language (JCL). Although DSAC and DITSO-Columbus controlled operator commands through the internal reader (a means of transferring jobs to JES) on their systems, DITSO-Dayton did not activate an exit, provided by DSAC, that controlled operator command submissions through the internal reader on its two systems. At DITSO-Columbus and DITSO-Dayton, management provided the same capabilities that the individual sites had before consolidation. Controls were not addressed in the decision to provide the same capabilities. 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.

JES2 controls. JES2 parameters control the disposition of operator commands submitted in JCL. 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" (WTOR). WTOR 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. WTOR may not be effective without clear written guidance, since operators respond to hundreds of messages per shift.

At DSAC, users could submit all operator commands for only two job input categories, and could submit only system commands for one category. DSAC also screened JCL submitted through the internal reader, thus effectively controlling operator- submitted commands.

At DITSO-Dayton, users could submit all operator commands on both systems for all 38 job input categories. Only one job input category on one system and eight job input categories on the second system were coded to provide WTOR control over the submission of operator commands. However, control procedures were not documented, and the internal readers on both systems allowed all operator command groups to be submitted. In addition, DITSO-Dayton did not activate the DSAC written exit that screened and controlled JCL-submitted operator commands through the internal reader.

At DITSO-Columbus, users on five systems could submit all operator commands for

38 job input categories. Although nine input categories on four systems and eight input categories on one system provided WTOR control over the submission of operator commands, the control procedures were not documented, and the internal readers on all five systems allowed all operator command groups to be submitted. However, DITSO-Columbus had activated the DSAC written exit that screened and controlled JCL-submitted operator commands through the internal reader.

Sensitive Utility Programs. Sensitive utility programs were not adequately controlled at DSAC, DITSO-Dayton, or DITSO-Columbus. Information systems officers had not evaluated vendor utilities for potential risks; therefore, 7 programs on the DSAC system, 35 programs on DITSO-Columbus systems, and 10 programs on DITSO-Dayton systems were available to all system users. 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 these programs 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 also can damage or destroy production programs and data files.

At DSAC, DITSO-Dayton, and DITSO-Columbus, RACF security software did not restrict the use of sensitive utilities. System personnel identified one obsolete program on the DSAC and DITSO-Columbus systems, and agreed to request its deletion from all systems. The CA-LOOK utility (see Appendix A, "Glossary") was adequately controlled.

Summary

System programmers at DSAC were not adequately monitoring APF libraries and programs, and access to update them was not properly limited. Programmers at DSAC had installed non-IBM SVCs on their systems, which compromised system integrity, and program names in the PPT were not adequately controlled. JES2 parameters did not properly limit user submission of operator commands, and sensitive utility programs were not fully controlled. Collectively, these conditions weaken the integrity of DSAC, DITSO-Dayton, and DITSO-Columbus systems that process about $67 billion annually in disbursements.

Recommendations

1. We recommend that the Commander, Defense Logistics Agency Systems Automation Center:

a. Develop the IBM-recommended installation integrity guidelines for the Defense Logistics Agency Systems Automation Center and the Defense Logistics Agency data processing installations. At a minimum, the guidelines should include specific requirements for administration of the authorized program facility in accordance with the 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 Director, Office of Computer Systems Support, and the Director, Office of Information Systems, to:

(1) Formally review all current authorized program facility libraries and programs, and delete obsolete and undocumented programs.

(2) Periodically review the authorized program facility list and ensure that it is kept up-to-date.

(3) Develop and implement adequate validity checking for user/vendor supervisor calls.

(4) Review all programs that are in the program properties table on the Defense Logistics Agency Systems Automation Center's operating system and that are on the operating systems at the serviced sites, and remove or control programs that no longer require special capabilities.

c. Direct the Chief, Office of Command and Automated Data Processing Security, to:

(1) Develop and implement specific guidance for periodic reviews of controls over access to authorized program facility libraries.

(2) Require that access rules be reviewed for all authorized program facility libraries to ensure that update access is limited to the minimum number of system programmers required to maintain those libraries.

(3) Define sensitive utilities to the Resource Access Control Facility security software as restricted programs; allow access only to personnel who have a clearly defined need; and strictly control any one-time use of these utilities.

2. We recommend that the Director, Defense Information Technology Services, Dayton Information Processing Activity:

a. Require the Chief, Computer Management Division, to:

(1) Formally review all current authorized program facility libraries and programs, and delete obsolete and undocumented programs.

(2) Periodically review the authorized program facility list and ensure that it is kept up-to-date.

(3) Require that job entry subsystem 2 parameters be reviewed, and that user-submitted operator commands be properly controlled.

b. Direct the Information Systems Security Officer to:

(1) Require that access rules be reviewed for all authorized program facility libraries to ensure that update access is limited to the minimum number of system programmers required to maintain these libraries.

(2) Define sensitive utilities to the Resource Access Control Facility security software as restricted programs; allow access only to personnel who have a clearly defined need; and strictly control any one-time use of these utilities.

3. We recommend that the Director, Defense Information Technology Services Organization, Columbus Information Processing Activity, Columbus, Ohio:

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

b. Direct the Chief, Technical Support, to:

(1) Formally review all current authorized program facility libraries and programs, and delete obsolete and undocumented programs.

(2) Periodically review the authorized program facility list and ensure that it is kept up-to-date.

(3) Require that job entry subsystem 2 parameters be reviewed, and that user-submitted operator commands be properly controlled.

c. Direct the Chief, Automated Data Processing Security, to:

(1) Require that access rules be reviewed for all authorized program facility libraries to ensure that update access is limited to the minimum number of system programmers required to maintain these libraries.

(2) Define sensitive utilities to the Resource Access Control Facility security software as restricted programs; allow access only to personnel who have a clearly defined need; and strictly control any one-time use of these utilities.

Management Comments

DITSO concurred with all recommendations in Finding A and will monitor corrective actions until they are complete. See Part IV for the full text of management's comments.

Audit Response

On recommendation 2.b.(2), DITSO-Dayton did not receive our memorandum dated March 26, 1993 that identified the sensitive utilities. We sent a second copy of the memorandum, and we confirmed that DITSO-Dayton had received it.

Finding B. Implementation of RACF Security Software

DSAC, DITSO-Dayton, and DITSO-Columbus had not properly implemented the features of Resource Access Control Facility (RACF) security software. Specifically, attributes (special capabilities) were not limited to users who were responsible for administering RACF; read access and update access to the system and to RACF datasets were not limited to the system programmers who were responsible for maintenance; security options of the tape management system were not installed; access to started procedures was not limited; passwords were not properly controlled; and the command to deactivate the RACF database was not controlled. In addition, protect-all processing, erase on delete, JES2 Logon ID (see Appendix A, "Glossary") and security options for password checking were not installed at DSAC, DITSO-Dayton, or DITSO-Columbus. These conditions occurred because security personnel were not adequately trained in RACF security administration and were not fully aware of DoD security requirements. Improper use or setup of the RACF security software features could allow knowledgeable users to perform unauthorized tasks (e.g., to access files without the authority to do so).

Background

RACF is an IBM software package for access control security. RACF protects data through options that:

- o identify and verify users entering the system,
- o restrict access to protected resources,
- o limit the capabilities of authorized users who have access to protected resources, and
- o log and report on security-related issues.

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

Attributes

At DITSO-Dayton and DITSO-Columbus, attributes were not limited to users responsible for administering RACF. Two system programmers at DITSO-Dayton had access to the special attribute that allows full control of all RACF profiles in the data base. Because security personnel were not adequately trained, they assigned these duties to system programmers. Therefore, the required separation of duties between operating personnel and security personnel was not maintained.

On 2 DITSO-Dayton systems, up to 49 users had access to the operations attribute that allows users to perform any RACF maintenance function (e.g., to copy, catalog, or delete RACF-protected resources). At each of the 5 DITSO-Columbus systems, over 123 individual system users had access to the operations attribute. For 51 of these 123 system users, access was obsolete and needed to be removed; for the remaining 72 users, further review was needed in order to determine specific needs for access.

Access to System and RACF Datasets

Access to system and RACF datasets was not properly limited. On the DSAC, DITSO-Dayton, and DITSO-Columbus systems, all users could read system and RACF datasets. These datasets allowed them to view system parameters and passwords that could aid a knowledgeable user in entering a system. In addition, 51 users at DSAC, 25 at DITSO-Dayton, and 43 at DITSO-Columbus could also update the RACF datasets. These users could gain unauthorized access and make changes to RACF datasets.

Tape Security

By not controlling Expiration Date (EXPDT)=98000 processing (the RACF feature that controls the bypassing of checks on the tape management system), DSAC, DITSO-Dayton, and DITSO-Columbus had not adequately secured tape processing. EXPDT=98000 is a JCL substatement that tells MVS that a tape is not in the CA-1 tape management system, and MVS should process the tape as requested. Although all systems use the CA-1 tape management system to control tape processing, the IPAs use different versions of the product. A RACF command or an exit must be installed to prevent EXPDT=98000 from bypassing the tape management system checks. The command ensures that when both the volume and the file name are in the tape management system, the EXPDT=98000 substatement is ignored, and normal security checking is performed.

Started Procedures

At DSAC, access to started procedures (operating system jobs or application programs initiated from an operator console) was not properly limited. When RACF was initially installed, started procedures had update access to all APF datasets in order to keep the system running. However, this level of access was no longer needed; started procedures should be limited to the datasets actually required.

Password Implementation

At DITSO-Dayton and DITSO-Columbus, password management required improvement. Instead of using the RACF password option that enforces password rules, management relied on system users to control password lengths and characteristics. RACF provides an automated means of enforcing the password rules required by DLA/DITSO, but security personnel at DITSO-Dayton and DITSO-Columbus had not activated the option. There was no assurance that password requirements were met, and there was more potential for an individual to compromise passwords.

RVARY Command

The RVARY option on RACF was not adequately controlled. By not changing the default passwords on the RVARY option, any user could submit a command to deactivate the RACF data base on the systems at DSAC, DITSO-Dayton, and DITSO-Columbus. The console operator must authorize such a request by issuing the default password; however, there was no written guidance to users or operators for issuing the passwords or the command to deactivate. Operators normally approved user requests by issuing the RVARY default password on the computer console.

Access Protection

DSAC, DITSO-Dayton, and DITSO-Columbus had not activated RACF control options needed to meet C2 security requirements. The options included protect-all processing, erase on delete, and JES2 LOGON ID and password checking. Since DITSO-Dayton and DITSO-Columbus process sensitive unclassified data, they must meet C2 security requirements. Because DSAC develops standard software for other sites, management also wanted the C2 security certification.

DoD Directive 5200.28 allows exceptions to C2 security requirements when computer operations are adversely affected. However, the designated approving authority (see Appendix A, "Glossary") must approve exceptions. Any substitute safeguards must achieve the required level of security.

Recommendations

1. We recommend that the Commander, Defense Logistics Agency Systems Automation Center:

a. Provide formal training on the administration of Resource Access Control Facility security software to appropriate personnel in the Office of Command and Automated Data Processing Security.

b. Direct the Chief, Office of Command and Automated Data Processing Security, to:

(1) Limit read access to system datasets and Resource Access Control Facility datasets, and limit update access to the Resource Access Control Facility datasets.

(2) Implement the security software and exit controls for Expiration Date=98000 at the Defense Logistics Agency Systems Automation Center; the Defense Information Technology Services Organization, Dayton Information Processing Activity; and the Defense Information Technology Services Organization, Columbus Information Processing Activity, Columbus, Ohio.

(3) Determine the required access for started procedures and define them to Resource Access Control Facility security software.

(4) Develop guidance and reset new passwords for the RVARY commands.

(5) Activate the Resource Access Control Facility options of protect-all processing, erase on delete, and job entry subsystem 2 Logon ID and password checking. If a waiver is needed, request the designated approving authority to evaluate the effects on the system, conduct a risk analysis, and document other safeguards to achieve the required level of security.

2. We recommend that the Director, Defense Information Technology Services Organization, Dayton Information Processing Activity, Dayton, Ohio:

a. Provide formal training on the administration of Resource Access Control Facility security software to appropriate personnel in the Office of Command and Automated Data Processing Security.

b. Direct the Information Systems Security Officer to:

(1) Assume responsibility for the administration of Resource Access Control Facility security software.

(2) Limit the users of the special attribute and operations attribute.

(3) Limit read access to system datasets and Resource Access Control Facility datasets, and limit update access to Resource Access Control Facility datasets.

(4) Set password options according to the Defense Logistics Agency requirements.

(5) Develop guidance for the RVARY command and reset the passwords for the RVARY commands.

(6) Activate the Resource Access Control Facility options of protect-all processing; erase on delete; and job entry subsystem 2 Logon ID and password checking. If a waiver is needed, request that the designated approving authority evaluate the effects on the system, conduct a risk analysis, and document other safeguards to achieve the required level of security.

3. We recommend that the Director, Defense Information Technology Services Organization, Columbus Information Processing Activity, Columbus, Ohio:

a. Provide additional formal training in the administration of Resource Access Control Facility security software to appropriate personnel in the Office of Command and Automated Data Processing Security.

b. Direct the Chief, Automated Data Processing Security, to:

(1) Limit the users who have the operations attribute and revoke the attribute for users who longer need it.

(2) Limit read access to system datasets and Resource Access Control Facility datasets, and limit update access to Resource Access Control Facility datasets.

(3) Set password options according to the Defense Information Technology Services Organization's requirements.

(4) Develop guidance for the RVARY command and reset passwords for the RVARY commands.

(5) Activate the Resource Access Control Facility options of protect-all processing; erase on delete; and job entry subsystem 2 Logon ID and password checking. If a waiver is needed, request that the designated approving authority evaluate the effects on the system, conduct a risk analysis, and document other safeguards to achieve the required level of security.

Management Comments

DITSO concurred with all recommendations in Finding B and will monitor corrective actions until they are complete. See Part IV for the full text of management's comments.

Finding C. Management Controls Over MVS Maintenance

Management controls over MVS maintenance at DSAC, DITSO-Dayton, and DITSO-Columbus needed improvement. Specifically, change control procedures for the operating system at DSAC were not formalized or properly documented, and sensitive system programmer positions at DSAC, DITSO-Dayton, and DITSO-Columbus were not appropriately designated as critical-sensitive. As a result, MVS integrity may be compromised.

Background

Management controls for the operating system include selection of system programmers, management of their programming functions, and change control procedures. The DSAC Office of Computer Systems Support is responsible for establishing and maintaining an ADP operating environment that supports DSAC and selected DPIs. System programmers are responsible for maintaining the operating system software and for installation and environmental testing of system software for the DPIs. Strict management controls are needed to ensure that program maintenance responsibilities are properly assigned, that programmer positions have the proper sensitivity designations, and that change control procedures are consistent and properly applied.

MVS Change Control Procedures

DSAC needed to improve its change control procedures for operating system maintenance. DSAC was responsible for the MVS change control process, but had no formal, written change control procedures. DSAC produced no documentation at critical decision points in the software change process; there was no formal approval or disapproval documentation from the system programming groups affected by the changes. Further, although personnel at the affected DPIs were notified and given clear instructions on implementing the changes, no follow-up procedures existed to assure DSAC that the DPIs properly implemented the changes. Improper control of operating system changes could allow the introduction of unauthorized or inaccurate computer programs that could compromise an operating system's integrity. As the software development site for DLA's designated DPIs (including DITSO-Dayton and DITSO-Columbus), DSAC is responsible for:

o exporting new software products for installation on the DPI's MVS systems,

- o upgrading operating system and product software,
- o site configuration changes, and
- o correcting emergency problems with MVS operating system software.

The IBM System Modification Program Extended Architecture (SMP/E) is DSAC's primary means of controlling changes to MVS software.

Since any software change can have dramatic and unexpected effects, changes must be properly defined, planned, coordinated, tested, and implemented. DSAC is preparing a "Change Management Proposal and MVS Integrity" program that outlines administrative and custodial duties for change management. To ensure that MVS integrity is maintained, the proposal should require strict control over changes to the operating system software.

Designation of Programmer Positions

System programmer designations at DSAC, DITSO-Dayton, and DITSO-Columbus were not appropriate. At DSAC, positions in systems development, operations, or acquisition are designated critical-sensitive at the General Schedule (GS) - 13 level and above. GS-12 (full performance) analyst, programmer, and operator positions were designated noncritical-sensitive, since their work is reviewed by higher-level employees whose positions are rated critical-sensitive.

At DITSO-Dayton and DITSO-Columbus, position descriptions for supervisory and GS-12 ADP positions were designated critical-sensitive. However, at DITSO-Columbus, only four of the seven GS-12 computer specialist positions in the Technology Division were designated critical-sensitive, and none of the lower-level positions at DITSO-Dayton and DITSO-Columbus was designated higher than noncritical-sensitive. Since all of these positions have considerable access capability and are responsible for system design 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. Consequently, their positions should be designated critical-sensitive in accordance with DoD Regulation 5200.2-R, "DoD Personnel Security Program, C3I," January 1987, Appendix K. This regulation 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 a background investigation. Without this designation, management has less assurance that programmers are trustworthy.

Recommendations

1. We recommend that the Commander, Defense Logistics Agency Systems Automation Center:

a. Establish formal management procedures to control the processing of all changes to the Multiple Virtual Storage operating system at the Defense Logistics Agency Systems Automation Center, and to control the export of these changes to the serviced data processing installations.

b. Require that all system programmer positions be designated critical-sensitive.

2. We recommend that the Director, Defense Information Technology Services Organization, Dayton Information Processing Activity, Dayton, Ohio, require that all system programmer positions be designated critical-sensitive.

3. We recommend that the Director, Defense Information Technology Services Organization, Columbus Information Processing Activity, Columbus, Ohio, require that all system programmer positions be designated critical-sensitive.

Management Comments

DITSO concurred with all recommendations in Finding C and will monitor corrective actions until they are complete. See Part IV for the full text of management's comments.

This page was left out of original document

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 Resource Access Control Facility (RACF).

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. A program that can perform sensitive functions outside of established APF rules can become part of the operating system, and can circumvent or disable all security mechanisms, alter audit trails, or modify any computerized data, regardless of the presence of access control software.

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

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

CA-LOOK is a utility program developed by Computer Associates International, Inc. It has sensitive functions that need to be properly controlled to prevent serious integrity exposures to the operating system.

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

Designated Approving Authority (DAA). The DAA is responsible for reviewing and approving security safeguards for automated information systems (AISs), and for issuing accreditation statements for each AIS under his or her jurisdiction.

Data Base 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.

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

Fail Mode is a security software feature that fully controls access requests. Access requests that do not conform to an existing access rule will be failed.

File is a collection of related data records stored on an external storage medium, usually 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 command 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. DSAC, DITSO-Dayton, and DITSO-Columbus use JES2.

JES options allow console operator commands to be placed in job control language (JCL). The options are assigned by type of job class. There are 36 possible batch job classes, and two 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 (JCL) is a problem-oriented computer language that identifies a job or describes its requirements to the operating system.

Library is a collection of related data files or programs.

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

MVS is the IBM multiple virtual storage operating system.

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

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 to ensure that all programs in the PPT have only the capabilities needed to function properly, and that the programs are safeguarded against unauthorized use. Program names must be maintained in a special library created and controlled by the installation, or in two IBM default libraries. The program must also be maintained 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.

Protect-all Processing is a RACF security option that secures all datasets by default.

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

RVARY Option is a RACF feature that deactivates the security data base.

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 system 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.

Spoofing is the technique of substituting a bogus file for a legitimate one.

Started Procedure is a started task. It is an operating system job or application program initiated from an operator console.

Supervisor Call (SVC). An 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 a vendor's software requirements.

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

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.

Warn Mode is a security feature that issues a warning message when a violation occurs, but still allows access to the system.

Appendix B. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
A.1.a.	Internal controls. 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 controls. Implements APF administration guidelines. Tells each center what its APF programs and files access. Evaluates SVC integrity exposures. Cleans up PPT by removing unneeded programs, and deactivates privileges that are not needed.	Nonmonetary.
A.1.c.	Internal controls. Develops procedures on how to review APF file access. Tells DSAC who has update access to APF files. Implements sensitive utility controls at DSAC. Makes use of RACF to control sensitive utilities.	Nonmonetary.

Appendix B. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
A.2.a., A.2.b.	Internal controls. Implements APF administration guidelines. Tells DITSO-Dayton what its APF programs/files are and what they do. Implements controls over user capability to execute operator commands. Implements review of APF-authorized update access. Implements sensitive utility controls. Makes use of RACF to control sensitive utilities.	Nonmonetary.
A.3.a., A.3.b.	Internal controls. Implements installation integrity guidelines developed by HQ, DITSO. Implements APF controls. Implements controls over user capability to execute operator commands.	Nonmonetary.
A.3.c.	Internal controls. Implements review of APF-authorized update access. Implements sensitive utility controls. Makes use of RACF to control sensitive utilities.	Nonmonetary.
B.1.a.	Internal controls. Provides additional training for security personnel to effectively implement and maintain RACF security software.	Nonmonetary.

Appendix B. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
B.1.b.	Internal controls. Implements controls available in RACF. Provides for better control of system resources.	Nonmonetary.
B.2.a.	Internal controls. Provides additional training for security personnel at DITSO-Dayton to effectively implement and maintain RACF security software.	Nonmonetary.
B.2.b.	Internal controls. Implements controls available in RACF. Provides for better control of system resources.	Nonmonetary.
B.3.a.	Internal controls. Provides additional training for security personnel at DITSO-Columbus to effectively implement and maintain RACF security software.	Nonmonetary.
B.3.b.	Internal controls. Implements controls available in RACF. Provides for better control of system resources.	Nonmonetary.
C.1.a.	Internal controls. Provides for improved control over MVS system maintenance.	Nonmonetary.
C.1.b., C.2., C.3.	Internal controls. Provides for system programmer positions to be designated critical-sensitive.	Nonmonetary.

Appendix C. Organizations Visited or Contacted

Defense Organizations

Headquarters, Defense Finance and Accounting Service, Washington, DC
Headquarters, Defense Information Technology Services Organization, Denver, CO
Defense Information Technology Services Organization, Columbus Information Processing Activity, Columbus, OH
Defense Information Technology Services Organization, Dayton Information Processing Activity, Dayton, OH
Defense Logistics Agency, Cameron Station, Alexandria, VA
Defense Logistics Agency, Systems Automation Center, Columbus, OH

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 Activities

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Information Technology Services Organization
Director, Defense Finance and Accounting Service, Cleveland Center, Cleveland, OH
Director, Defense Finance and Accounting Service, Indianapolis Center, Indianapolis, IN
Director, Defense Information Technology Services Organization, Cleveland Information Processing Activity, Cleveland, OH
Director, Defense Information Technology Services Organization, Indianapolis Information Processing Activity, Indianapolis, IN

Non-DoD Federal Organizations

Office of Management and Budget
U.S. General Accounting Office

Chairmen and Ranking Minority Members of the following Congressional Committees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Governmental Affairs
Senate Committee on Armed Services
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 Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
DEFENSE INFORMATION TECHNOLOGY SERVICES ORGANIZATION
6760 E. IRVINGTON PLACE
DENVER, COLORADO 80279-1000

IN REPLY REFER TO: GAR

10 MAY 1993

MEMORANDUM FOR PROGRAM DIRECTOR, FINANCIAL MANAGEMENT DIRECTORATE, INSPECTOR GENERAL DEPARTMENT OF DEFENSE

SUBJECT: Draft Audit Report on Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service (Project No. 1FD-0043.01)

1. The Defense Information Technology Services Organization (DITSO) reviewed the subject audit report and our management comments concerning your findings and recommendations are in enclosure 1. We also concur with the internal control weaknesses you highlighted in Part I of your report.

2. We will monitor the corrective actions until they are all completed. Our audit focal point is Mr. Tom Nicholas. He can be reached at DSN 926-6958 or commercial (303) 676-6958 if you have any questions.

Clyde E. Jeffcoat

CLYDE E. JEFFCOAT
Director

Enclosure a/s

Copy to:
Acting Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Acting Comptroller, Department of Defense
Director, Defense Information Services Agency
Director, Defense Logistics Agency
Acting Director, Defense Finance and Accounting Service
Director, Defense Finance and Accounting Service, Columbus Center

DEFENSE INFORMATION TECHNOLOGY SERVICES ORGANIZATION (DITSO)
MANAGEMENT COMMENTS
CONTROLS OVER OPERATING SYSTEMS AND SECURITY SOFTWARE
SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE
PROJECT NO. 1FD-0043

Finding A: Operating System Controls

Recommendation 1a: Develop the IBM-recommended installation integrity guidelines for the Defense Logistics Agency Systems Automation Center and the Defense Logistics Agency data processing installations. At a minimum, the guidelines should include specific requirements for administration of the authorized program facility in accordance with the 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.

Position: Concur.

Planned action: DSAC will develop installation integrity guidelines and distribute to the data processing installations. The date of estimated completion is 1 July 1993.

Recommendation 1b (1) Formally review all current authorized program facility libraries and programs, and delete obsolete and undocumented programs.

Position: Concur.

Planned action: We are reviewing and documenting all APF libraries and programs. The process will encompass all authorized libraries and programs on the system and at the conclusion of the initial effort all authorized libraries and programs will be documented and any obsolete libraries and programs will have been deleted. Any reference to nonexistent libraries will be deleted. We expect to have this completed by 1 June 1993. Of the individual programs cited, two(CATFIX and NIPZAP) have been corrected at DSAC. DSAC will send the corrected modules to the sites to replace the older modules.

Recommendation 1b (2) Periodically review the authorized program facility list and ensure that it is kept up-to-date.

Position: Concur.

Planned action: We plan periodic reviews of the authorized program facility list to ensure that it is kept up-to-date.

1

Recommendation 1b (3) Develop and implement adequate validity checking for user/vendor supervisor calls.

Position: Concur.

Planned action: We agree that integrity problems exist with the SVCs cited in the audit report. We are currently investigating a resolution to these exposures. We have contacted the vendor, Computer Associates, for a resolution of the problem with SVC 238. If the vendor cannot provide an immediate fix, we will disable the CAAM portion of ASM2 until the next release is generally available. We are currently determining the usage requirements for the SVCs 248, 254 and 255. These SVCs are called by utilities that are used in many production programs. It is unclear at this time if restricting the SVCs to specific programs will provide adequate protection. The analysis will be a complex effort and the resolution is not known at this time. We estimate that the analysis will be complete 1 November 1993. The final resolution to the problem will have to be determined at that time. The packaging of the SVC was considered the problem and ISOGON has removed the problem with a subsequent release of this user SVC. The new SVC was not able to run in an SP1 (pre-XA) environment which exists at DESC and therefore could not be implemented yet. The dry run for moving DESC SAMMS to DGSC took place. The actual consolidation is underway. After that, we will be free to implement the new/safer version of this SVC at all licensed locations. Estimated date of completion is 30 May 1993.

Recommendation 1b (4). Review all programs in the program properties table on the Defense Logistics Agency Systems Automation Center operating system and systems at the serviced sites, and remove or control programs that no longer require special capabilities.

Position: Concur.

Planned action: DSAC has begun to review all programs in the Program Properties Table and delete any obsolete or unnecessary programs. Further review and documentation is required. Our estimated completion date for the actions required to provide adequate control for all programs included in the Program Properties Table is 1 June 1993. Final changes, documentation, and recommendations will be provided to DITSO-Columbus and DITSO-Dayton, as well as other DSAC-supported data centers. The estimated completion date for release of the changes and incorporation by the sites is 1 July 1993.

Recommendation 1c (1) Develop and implement specific guidance for periodic reviews of controls over access to authorized program facility libraries.

Position: Concur.

Planned action: DSAC will develop and implement procedures for periodic reviews of controls over access to authorized program facility libraries and will require that the access be limited to the

minimum number of system programmers required to maintain those libraries. The estimated date of completion is 1 July 1993.

Recommendation 1c (2). Require that access rules be reviewed for all authorized program facility libraries to ensure that update access is limited to the minimum number of system programmers required to maintain those libraries.

Position: Concur.

Planned action: See 1c(1).

Recommendation 1c (3). Define sensitive utilities to the Resource Access Control Facility security software as restricted programs; allow access only to personnel who have a clearly defined need; and strictly control any one-time use of these utilities.

Position: Concur.

Planned action: We concur that the sensitive utilities need to be restricted. A minimum number of users will be permitted access. The date of estimated completion is 1 August 1993.

Recommendation 2a:

(1) Formally review all current authorized program facility libraries and programs, and delete obsolete and undocumented programs.

(2) Periodically review the authorized program facility list and ensure that it is kept up-to-date.

(3) Require that job entry system 2 parameters be reviewed and that user-submitted operator commands be properly controlled.

Position: Concur.

Planned Action: Periodic review of all APF libraries and programs and JES2 parameters and control of user-submitted operator commands began 30 March 1993 and is an ongoing process. See 2.a(1), (2), (3) above.

Recommendation 2b(1): Requires that access rules be reviewed for all authorized program facility libraries to ensure that update access is limited to the minimum number of system programmers required to maintain these libraries.

Position: Concur.

Planned Action: Review of access rules for APF libraries to limit access to a minimum number of system programmers was completed as of 30 April 1993.

3

Recommendation 2b(2): Define sensitive utilities to the Resource Access Control Facility security software as restricted programs; allow access only to personnel who have a clearly defined need; and strictly control any one-time use of these utilities.

Position: Concur.

Planned Action: Dayton IPA's review of policies related to sensitive utilities programs will commence upon the disclosure of the ten (10) utilities programs deemed sensitive by the Office of the Inspector General, DoD, to Dayton IPA personnel. This review is expected to be completed ninety (90) days subsequent to the receipt of the requested information.

Recommendation 3a: Fully implement the IBM recommended installation integrity guidelines currently being developed by Director, DITSO.

Position: Concur.

Planned Action: Full implementation of IBM recommended integrity guidelines is in progress.

Recommendation 3b(1): Formally review all current authorized program facility libraries and programs, and delete obsolete and undocumented programs.

(2) Periodically review the authorized program facility list and ensure that it is kept up-to-date.

(3) Require that job entry system 2 parameters be reviewed and that user submitted operator commands be properly controlled.

Position: Concur.

Planned Action: Periodic review of all APF libraries and programs, and JES2 parameters and control of user submitted operator commands is an ongoing process.

Recommendation 3c(1): Require that access rules be reviewed for all authorized program facility libraries to ensure that update access is limited to the minimum number of system programmers required to maintain these libraries.

Position: Concur.

Planned Action: Review of access rules for APF libraries to limit access to a minimum number of system programmers will be completed by 15 May 1993.

Recommendation 3c(2): Define sensitive utilities to the Resource Access Control Facility security software as restricted programs; allow access only to personnel who have a clearly defined need; and strictly control any one-time use of these utilities.

Position: Concur.

Planned Action: Restriction of access to sensitive utilities programs (AMASPEAP, IEHINITT, ICKDSF, ADRDSSN,IEHPROGM, DEBEXA, UTAU21, MVSDEDE and OSEDEBE) to system programmers and operations personnel. This will be completed by 30 April 1993.

Finding B: Implementation of RACF Security Software

Recommendation 1a Provide formal training on the administration of Resource Access Control Facility security software administration to appropriate personnel in the Office of Command and Automated Data Processing Security.

Position: Concur.

Planned action: DSAC has scheduled three employees in the RACF Conference to be held in June 1993.

Recommendation 1b (1) Limit read access to the system and Resource Access Control Facility datasets, and limit update access to the Resource Access Control Facility datasets.

Position: Concur.

Planned action: DSAC will work to restrict read access to system datasets and will further restrict access to the RACF database. The estimated completion date is 1 July 1993.

Recommendation 1b (2). Implement the security software and exit control for Expiration Date=98000 at the Defense Logistics Agency Systems Automation Center; the Defense Logistics Agency Electronics Supply Center; and Defense Information Processing Center, Columbus, Ohio.

Position: Concur.

Planned action: DSAC will implement RACF security for the tape management system. DSAC will communicate the instructions to the Defense Logistics Agency Electronics Supply Center and the Defense Information Processing Center. The estimated completion date for these actions is 1 July 1993.

Recommendation 1b (3). Determine the required access of started procedures and define them to Resource Access Control Facility security software.

Position: Concur.

Planned action: DSAC has begun the process of identifying the access requirements of the started procedures and will enter them into the RACF security software. The estimated completion date is 1 August 1993.

Recommendation 1b (4). Develop guidance and reset new passwords for the RVARY commands.

Position: Concur.

Planned action: DSAC is developing written procedures for the RVARY command usage, which will include resetting new passwords. The estimated completion date is 1 May 1993.

Recommendation 1b (5). Activate the Resource Access Control Facility options of protect-all processing, erase on delete, and job entry subsystem 2 Logon ID and password checking. If a waiver is needed, request the designated approving authority to evaluate the effects on the system, conduct a risk analysis, and document other safeguards to achieve the required level of security.

Position: Concur.

Planned action: DSAC will implement protect-all processing and will request a waiver for the erase on delete and job entry subsystem 2 Logonid ID and password checking. The estimated completion date is 1 July 1993.

Recommendation 2a: Provide formal training on the administration of Resource Access Control Facility security software to appropriate personnel in the Office of Command and Automated Data Processing Security.

Position: Concur.

Planned Action: Submission of request for seven days of formal training in the use of RACF software for two security personnel was submitted by 30 April 1993. The training will begin on 24 June 1993 in New Orleans.

Recommendation 2b(1): Assume responsibility for the administration of Resource Access Control Facility security software.

Position: Concur.

Planned Action: Assumption of administration of RACF security software will be completed by 15 December 1993.

Recommendation 2b(2): Limit the users of the special attribute and operations attribute.

Position: Concur.

Planned Action: Limitation of special and operations attributes, will be an ongoing process.

Recommendation 2b(3): Limit read access to the system and Resource Access Control Facility datasets, and limit update access to Resource Access Control Facility datasets.

Position: Concur.

Planned Action: Limitation of read and update access to RACF datasets began 30 March 1993 and is an ongoing process.

Recommendation 2b(4): Set password options to DLA requirements.

Position: Concur.

Planned Action: Adherence to DLA password requirements started in October 1992.

Recommendation 2b(5): Develop guidance for the RVARY command and reset the passwords for the RVARY commands.

Position: Concur.

Planned Action: Reset of RVARY passwords and development of guidance for use of RVARY commands, was completed 31 March 1993.

Recommendation 2b(6): Activate the Resource Access Control Facility options of protect-all processing, erase on delete, and job entry subsystem 2 LOGON ID and password checking. If a waiver is needed, request the designated approving authority to evaluate the effects on the system, conduct a risk analysis, and document other safeguards to achieve the required level of security.

Position: Concur.

Planned Action: Insofar as most of the files managed by Dayton IPA do not contain sensitive information (with exception of Social Security Number data), a risk analysis will be prepared and completed by 1 August 1993 to substantiate a request for waiver of certain security requirements enumerated. Specifically, the necessity of this activation of the "protect-all processing" and "erase on delete" RACF control options to meet security standards described in DoD Directive 5200.28, will be addressed in the risk analysis and subsequent waiver requests.

Recommendation 3a: Provide additional formal training in the administration of Resource Access Control Facility security software to appropriate personnel in the Office of Command and Automated Data Processing Security.

Position: Concur.

Planned Action: Submission of request for formal training in the use of RACF software for security personnel has been submitted and will be completed by 30 June 1993.

Recommendation 3b(1): Limit the users who have the operations attribute and revoke the attribute for users who no longer need it.

Position: Concur.

Planned Action: Limitation of operation attributes and revoke attributes for users no longer needing access will be completed by 15 May 1993.

Recommendation 3b(2): Limit read access to the system and Resource Access Control Facility datasets, and limit update access to Resource Access Control Facility datasets.

Position: Concur.

Planned Action: Limitation of read and update access to the RACF datasets was completed 1 April 1993.

Recommendation 3b(3): Set password options to DITSO requirements.

Position: Concur.

Planned Action: Adherence to DLA password requirements was completed 1 April 1993.

Recommendation 3b(4): Develop guidance for the RVARY command and reset passwords for the RVARY commands.

Position: Concur.

Planned Action: Reset of RVARY password and development of guidance for use of RVARY commands will be completed by 30 May 1993.

Recommendation 3b(5): Activate the Resource Access Control Facility options of protect-all processing, erase on delete, and job entry subsystem 2 LOGON ID and password checking. If a waiver is required, request the designated approving authority to evaluate the effects on the system, conduct a risk analysis, and document other safeguards to achieve the required level of security.

Position: Concur.

Planned Action: Development of risk analysis study for a request

of waiver of specific security requirements.Specifically, the necessity of the activation of "erase on delete" RACF control options to meet security standards described in DoD Directive 5200.28, Batch All RACF. This is to be completed by 31 August 1993.

Finding C: Management Controls Over MVS Maintenance

Recommendation 1a: Establish formal change management procedures to control the processing of all changes to the Multiple Virtual Storage operating system at the Defense Logistics Agency Systems Automation Center, and to control the export of these changes to the serviced data processing installations.

Position: Concur.

Planned actions: Change management procedures will be documented and implemented by management. The estimated completion date is 15 June 1993.

Recommendation 1b: Require that all system programmer positions be designated critical-sensitive.

Position: Concur.

Planned action: DSAC will review and update the necessary system programmer position designations in accordance with DOD 5200.2-R. The estimated completion date is 1 August 1993.

Recommendation 2: We recommend that the Commander, DESC, require that all system programmers positions be designated as critical-sensitive.

Position: Concur.

Planned Action: The designation of all system programmer positions as critical-sensitive has been initiated and is ongoing for all new employees. Dayton IPA is currently awaiting the responses to requests for background investigations of these personnel which have been submitted to the DESC Office of Command Security.

Recommendation 3: We recommend that the Director, Columbus IPA, require that all system programmer positions be designated critical-sensitive.

Position: Concur.

Planned Action: The designation of all system programmer positions as critical-sensitive has been initiated.

2. Be advised that since the date of the subject report, a new central processing unit (CPU) (an AMDAHL 5995/1400A), has been acquired and installed at Dayton Information Processing

Activity (IPA), formerly Defense Logistics Agency Electronics Supply Center (DESC). This CPU processes ten (10) Defense Business Management System (DBMS) applications formerly processed by three (3) separate CPUs.

3. Also be advised that since the date of the subject report a new computer facility has been completed at Columbus IPA. This new facility has an AMDAHL 5995/1400A processing seven (7) DBMS and five (5) Mechanization of Contract Administration Service (MOCAS) applications formerly processed on five (5) CPUs.

4. Please direct questions regarding planned actions for DITSO-Dayton IPA, GRCIRP, to Mr. Frank Titus, DSN 986-6938.

5. Please direct questions regarding planned actions for DITSO-Columbus IPA, GRCI, Mr. Ronald Remy, GRCIDDI, DSN 850-4341.

10

Audit Team Members

Nancy L. Hendricks	Director, Financial Management Directorate
David C. Funk	Program Director
Stephen A. Delap	Project Manager
John A. Dedio	Team Leader
Thomas G. Hare	Auditor
Frances E. Cain	Auditor
Susanne B. Allen	Editor

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service

B. DATE Report Downloaded From the Internet: 04/24/99

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

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 04/24/99**

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