78-21-9195 (2)
10

Report No.
CR-B-91-02

U.S. Department of Energy
Office of Inspector General

Release Date:
September 1991

Report on

**Selected Computer System
Controls at the Energy
Information Administration**

IG IG IG IG IG IG IG IG
IG IG IG IG IG IG IG IG
IG IG IG IG IG IG IG IG
IG IG **IG** IG IG IG IG IG

This report can be obtained from the
U.S. Department of Energy
Office of Scientific and Technical Information
P. O. Box 62
Oak Ridge, Tennessee 37831

SELECTED COMPUTER SYSTEM CONTROLS AT THE
ENERGY INFORMATION ADMINISTRATION

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY	1
PART I - APPROACH AND OVERVIEW	2
Purpose and Objectives	2
Scope and Methodology	2
Background	2
Observations and Conclusions	3
PART II - FINDINGS AND RECOMMENDATIONS	5
1. Disk Space Utilization	5
2. Data Storage on Tape	7
3. System Controls	9
4. System Software Maintenance	12
PART III - MANAGEMENT AND AUDITOR COMMENTS	15

MASTER

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL

SELECTED COMPUTER SYSTEM CONTROLS AT THE
ENERGY INFORMATION ADMINISTRATION

Audit Report Number: CR-B-91-02

SUMMARY

The purpose of our review of the Energy Information Administration's (EIA) computer system was to evaluate disk and tape information storage and the adequacy of internal controls in the operating system programs. We used a set of computer-assisted audit techniques called CAATS, developed by the U.S. Department of Transportation, Office of Inspector General, in performing the review at the EIA Forrestal Computer Facility.

Improved procedures are needed to assure more efficient use of disk space. By transferring data sets from disk to tape, deleting invalid data, releasing unused reserve space and blocking data efficiently, disk space with an estimated value of \$1.1 million a year could be recovered for current use. Also, procedures governing the maximum times for storage of information on tapes should be enforced to help ensure that data is not lost. In addition, improved internal controls are needed over granting users system-wide privileges and over authorized program library names to prevent unauthorized access to the system and possible destruction or manipulation of data.

Automated Data Processing (ADP) Services Staff officials indicated that software maintenance was not current, due to contractual difficulties with the operating contractor for the Forrestal Facility. Our review confirmed that improvements were needed to help prevent malfunctions of the operating system, which could cause performance degradations, system failures, or loss of either system or user data. Management generally concurred with the recommendations in the report.

Office of Inspector General

PART I

APPROACH AND OVERVIEW

PURPOSE AND OBJECTIVES

The purpose of our review of the Energy Information Administration's computer system was to evaluate disk and tape information storage and the adequacy of internal controls in the operating system programs. Our specific objectives were to determine whether disk and tape storage resources were being efficiently and effectively used; individuals' access to computer programs was adequately controlled; selected operating system controls were adequate and properly administered; and system software control mechanisms were properly installed and maintained.

SCOPE AND METHODOLOGY

The audit was performed at the EIA Forrestal Computer Facility in Washington, D.C., between January and December 1990. We used a set of computer-assisted audit techniques called CAATS, developed by the U.S. Department of Transportation, Office of Inspector General, in performing the review. A diagnostic software package was used to assess the level of system software maintenance.

We assessed internal controls for the operating system and security software by reviewing certain control programs, special routines, and assignment of access privileges. Reports on access rules were used in our review of the administration of computer access privileges. We also conducted interviews with key system software maintenance, operations, and computer security personnel. The firm of COMSIS Corporation participated with the Office of Inspector General in conducting this audit.

Our examination was conducted in accordance with generally accepted Government auditing standards for performance audits, which included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objectives. An exit conference was held with the Deputy Administrator, Energy Information Administration, on July 25, 1991.

BACKGROUND

The Energy Information Administration's ADP Services Staff operates and manages the Forrestal Computer Facility, which maintains unclassified and sensitive energy information. Authorized users throughout the United States may access the Facility through a telecommunications network. Budgets for this Facility were approximately \$9.9 million in Fiscal Year (FY) 1990 and \$11.0 million in FY 1991.

An independent contractor provides computer operations, systems software, and user support functions. The primary computer is an IBM 3084 mainframe

controlled by a MVS/XA 1/ operating system and ACF-2 2/ access security software. EIA collects unclassified and sensitive information on energy-related industries, some of which must be protected by law.

OBSERVATIONS AND CONCLUSIONS

EIA must ensure that it has the necessary computing capacity and capabilities to meet user needs. To ensure timely retrieval of data needed by the users, computer disk storage capacity must be effectively and efficiently managed. EIA also must maintain the integrity of system software (the computer programs) such as the operating and access security systems, which manage the processing workload and control user access to data.

We observed examples of effective controls for computer protection at the Forrestal Computer Facility. Each user account was assigned to a designated Department of Energy (DOE) project manager, and all users were required to attend a computer security briefing before being granted access. Also, system level manuals were restricted to personnel involved with installing and maintaining system software. Only DOE project managers were allowed to sign out important reference materials. Personnel in the Computer Security and Systems Software sections appeared to be properly trained and qualified. However, we noted several weaknesses in the areas of disk and tape storage, system controls, and system software maintenance that could, if not corrected, affect EIA's mission of providing timely and accurate information.

Improved procedures are needed to assure more efficient use of disk space. By transferring data sets from disk to tape, deleting invalid data, releasing unused reserve space and blocking data efficiently, disk space with an estimated value of \$1.1 million could be free for other use. Also, procedures governing the maximum times for storage of information on tapes should be enforced to help ensure that data is not lost. In addition, improved internal controls are needed over granting users system-wide privileges and over authorized program library names to prevent unauthorized access to the system and possible destruction or manipulation of data.

ADP Services Staff officials indicated during an interview that software maintenance was not current, due to workload backlogs caused by contractual difficulties. Our review confirmed that improvements were needed to help prevent malfunctions of the operating system, which could cause performance degradations, system failures, or loss of either system or user data.

1/ MVS (Multiple Virtual Storage) is an IBM virtual storage operating system that gives each user an environment defined as an address space. It provides for the isolation and protection of one user from another in a multi-programming system supporting many users concurrently.

2/ ACF-2 (Access Control Facility 2) is an access control software package which provides the ability to control access to the computer system and to data sets residing on the direct access storage and tape devices of the system.

Since our review was limited, it would not necessarily disclose all internal control deficiencies that may exist. However, the internal control deficiencies pointed out in Findings 3 and 4 should be considered in preparation of the yearend assurance memorandum on internal controls. Management generally concurred with the recommendations.

PART II

FINDINGS AND RECOMMENDATIONS

1. Disk Space Utilization

FINDING

Departmental policy requires that computer resources, such as disks used to store information, be managed effectively. Our analysis showed the need for more efficient disk space management at the Forrestal Computer Facility. Specifically, inactive data sets stored on disks were not routinely transferred to less costly tape storage and invalid data sets were not removed from disks; unused reserved disk space was not released for use; and data were not "blocked" (grouped) in a way that would use disk space most efficiently. These conditions occurred because EIA had not established mandatory procedures for assuring more efficient use of disk storage space. Increased efficiency could potentially free \$1.1 million worth of disk space a year for use by others.

RECOMMENDATIONS

We recommend that the Director, Automated Data Processing Services Staff, Energy Information Administration, adopt policy and procedures that require:

1. Transferring disk data sets to tape after a period of inactivity as specified in the *User's Guide to the Forrestal Computer Facility*, unless the data sets have special retention periods for control purposes;
2. Eliminating invalid data sets;
3. Releasing unused reserved disk space; and
4. Setting block size for at least 90 percent efficiency.

MANAGEMENT REACTION

Management disagreed with the finding, but generally concurred with the intent of the recommendations. See Part III for Management and Auditor Comments.

DETAILS OF FINDING

DOE Order 1360.1A, *Acquisition and Management of Computing Resources*, requires that computer resources, such as disk storage devices, be managed "in a manner that maximizes the effective use of those resources." Generally accepted techniques for maximizing the use of disk storage space in computer systems include transfer of inactive data sets from costly online disks to less expensive offline magnetic tapes. The *User's Guide to the Forrestal Computer Facility* discusses two other generally accepted practices. Specifically, it states that the period of time inactive data sets may stay on

disks without being archived on tape can be anywhere from 28 to 32 days. The *User's Guide* also recommends "a block size of approximately 6160." This block size will achieve at least 90 percent efficiency. These procedures were not mandatory at the Forrestal Computer Facility.

EIA had not transferred inactive data sets stored on disks to less expensive tapes. Some of the data sets had not been accessed in over 2 years. As shown below, our analysis of disk storage under transfer periods of 30, 45, 60, 90, and 180 days showed that between 18.9 and 26.4 percent of disk space could be freed for other uses.

We identified other areas in which the use of disk storage space could be improved. For example, invalid data sets, such as those created when a job is aborted, were not eliminated. As a result, disk space was wasted. Also, the "RELEASE" option was not used to free-up unused reserved space. In other instances, the 6160 blocking size was not being used to achieve 90-percent efficiency when allocating disk space.

DISK STORAGE ANALYSIS SUMMARY Recoverable Space as of March 27, 1990

Time Period	Estimated Recoverable (bytes, in billions)			Percent	Annual Costs (millions) 4/
	Transfer	Other 3/	Total		
30 days	13.5	8.5	22.0	26.4	\$1.4
45 days	7.9	9.4	17.3	20.8	\$1.1
60 days	7.5	9.5	17.0	20.3	\$1.1
90 days	6.7	9.6	16.3	19.6	\$1.1
180 days	5.8	9.9	15.7	18.9	\$1.0

Efficient disk usage was not achieved because EIA did not have mandatory policy and procedures requiring transfer and/or elimination of invalid data sets, release of unused reserved disk space, and use of efficient blocking size for data stored on disks.

We believe the 45-day transfer period represents the maximum potential recoverable disk space for the EIA computer facility. A 45-day transfer period is less restrictive than the 32-day period recommended in EIA's *User's Guide*. The amount of disk space that would be released under a 45-day transfer period would be 17.3 gigabytes (bytes in billions) at an estimated annual value of \$1.1 million.

3/ The "other" category includes inefficient blocking size, not releasing unused reserved space and eliminating invalid data sets. It excludes data sets that fall into this category but already reported in the "recoverable from transfer" category. Generation data sets were also excluded.

4/ Cost was calculated using \$.0085/track/day obtained from the EIA Cost Recovery Information System. The annual costs are based on an estimate that each track can store up to 47,476 bytes of data.

2. Data Storage on Tape

FINDING

Departmental policy requires that computer systems and computer programs supporting mission-essential functions be protected from adverse events and unnecessary processing delays. After 3 years, reel type magnetic tape used to store computer data and programs normally becomes unreliable. More than one-third of EIA data sets was stored on tapes more than 3-years old. This occurred because EIA allowed assignment of expiration dates beyond the 180-day retention period recommended by their *User's Guide to the Forrestal Computer Facility*. Data and programs stored on tapes over 3-years old could be lost or become useless due to the deterioration of tape, which can occur when tape reaches this age.

RECOMMENDATIONS

We recommend that the Director, Automated Data Processing Services Staff, Energy Information Administration:

1. Limit the maximum expiration period for tape data sets to 3 years (except for 3480 cartridge tape technology); and
2. Review tape data sets more than 3-years old for processing reliability and transfer those data sets deemed necessary to other tapes with acceptable reliability.

MANAGEMENT REACTION

Management concurred with the recommendations.

DETAILS OF FINDING

DOE Order 1360.2A requires that computer-generated data, including that stored on magnetic tape, be adequately protected. The Forrestal Computer Facility uses magnetic tape to back up data and computer programs for disaster recovery purposes. It also stores inactive data sets on tape.

EIA's *User's Guide* specifies that the retention period for data on tapes should be no more than 180 days. However, a greater retention period may be permitted if a tape transmittal form, signed by the project manager, is sent to the ADP Services Staff. Experience has shown that magnetic tapes, except for 3480 cartridge tape, begin losing reliability at 3 to 5 years.

We used information from EIA's Tape Management System to determine whether any tape data sets were at risk of becoming unreliable because they were more than 3-years old. This system contains such information as the assigned date of expiration, date of creation, tape density, and block size.

Our tape analysis included cartridge tapes. However, we estimated that at most only about 45 percent were the cartridge type. The following illustration summarizes the results of our analysis.

As shown, almost 20 percent of the data sets, or 13,747, were 3- to 5-years old and over 16 percent, or 11,500, were over 5-years old. Thus, as much as 36 percent of the total tape data sets could be unreliable.

Retention of tape data sets beyond 3 years occurred because EIA allowed users to assign expiration dates beyond that period and did not establish a specific retention period for tapes granted exception to the 180-day limit. Experience has shown that magnetic tapes begin to deteriorate when they are 3- to 5-years old. Tape deterioration can result in incorrect or lost data which could prevent EIA from providing timely, accurate energy information.

3. System Controls

FINDING

DOE Order 1360.2A requires that unclassified computer systems be adequately protected from misuse and abuse. It also requires protecting sensitive applications on unclassified computer systems from unauthorized access and improper use. Eleven individuals at the Forrestal Computer Facility were granted powerful system-wide (ACF-2) privileges that would allow virtually unlimited access to all resources normally protected by the security system software. In addition, 14 authorized program library names no longer in use had not been deleted and could, therefore, be used to bypass system controls. Also, a system program commonly known as Supervisor Call Instruction (SVC) 5/ allowed authorization checks to be bypassed. These conditions occurred because (1) EIA had not established specific criteria to ensure adequate separation of duties when granting special user privileges, and (2) it had neither established adequate procedures for controlling library names nor properly coded the SVC to prevent bypass of system authorization checks. As a result, the sensitive and critical applications supported by the EIA computer system could be vulnerable to unauthorized access, fraud, and accidental manipulation or destruction. Further, system availability could be reduced. Knowledgeable users could exploit these weaknesses to gain control of the operating system by (1) masquerading their programs as authorized, using the authorized library names no longer in use and (2) bypassing system authorization checks to execute their programs as authorized.

RECOMMENDATIONS

We recommend that the Director, Automated Data Processing Services Staff, Energy Information Administration:

1. Define a set of criteria in the policy and procedures for maintaining ACF-2 privileges that would ensure separation of duties when granting special user privileges;
2. Limit the special user privileges granted to users based on the above defined set of criteria;
3. Delete names of libraries of authorized programs (from the SYS1.PARMLIB data set) no longer in use and establish procedures to ensure that unused authorized library names are deleted; and
4. Modify the code of the SVC to disallow the particular parameter value that would bypass authorization checks and replace the embedded account code checks with an interface between the SVC and ACF-2, the security software.

5/ SVC is used to communicate with the Multiple Virtual Storage operating system.

MANAGEMENT REACTION

Management concurred with the intent of the recommendations. It partially concurred with specific Recommendations 3 and 4. See Part III for Management and Auditor Comments.

DETAILS OF FINDING

DOE Order 1360.2A requires adequate protection of computer systems from misuse and abuse. The U.S. General Accounting Office's internal control standards and the Office of Management and Budget internal control guidelines stress the importance of maintaining separation of duties. The *Technical Reference Series* published by Ernst and Whinney recommends that special system-wide user privileges, such as ACCOUNT and SECURITY, should not be granted to the same user. Further, a recently published article, *Computer Crime and Abuse*, in the *EDP Auditor Journal* stated that according to several computer crime surveys, employees with information about computer loopholes and those with special needs requiring special access privileges could be the greatest threat to computer security. Operating system integrity must be maintained by ensuring that (1) only those programs designed to modify operating system software can become authorized and (2) Supervisor Call Instructions are coded properly to ensure against unauthorized use.

Separation of Duties

We analyzed EIA user accounts that were granted special system-wide privileges. Eleven user accounts had privileges that would allow unlimited authority over the computer system. In particular, 10 user accounts were granted both ACCOUNT and SECURITY privileges. Users with ACCOUNT privileges could create or change all user account records. Those with SECURITY privileges could create or change access rules and execute restricted programs. One user account was granted unrestricted security privileges. We also noted that 2 of the 11 accounts were given the NON-CNCL privilege, which meant that these users could access any data sets without being cancelled.

The ADP Services Staff approved special system-wide privileges for user accounts without defining specific internal control criteria for ensuring separation of duties. Users of accounts with ACCOUNT and SECURITY privileges could manipulate user accounts and, at the same time, manipulate access rules to gain the capability of copying, modifying, or destroying any data set on the system. Thus, by assigning system-wide privileges to users without adequate separation of duties, EIA exposed its computer system to increased risk of unauthorized access, fraud, accidental manipulation, or destruction of data.

We also performed limited system integrity tests. The results of our tests indicated two internal control weaknesses existed that would enable knowledgeable users to bypass operating system and security software controls and gain unintended authorization. These weaknesses concerning control of libraries and use of an in-house developed Supervisor Call Instruction are discussed below.

Control of Libraries

Authorized Program Facility (APF) libraries are used to ensure orderly modification of the operating system. Programs placed in designated APF libraries become extensions of the operating system and can gain the ability to circumvent or disable any security mechanism, alter any audit trail, and/or modify any application data in the computer, regardless of the presence of access control software. EIA had not deleted 14 authorized library names no longer used. This occurred because there were no specific procedures requiring that unused names be deleted from the system. Creation of program libraries using the authorized library names no longer in use would automatically cause them to be recognized as authorized by the operating system. As a result, knowledgeable users could create libraries for malicious purposes, such as unauthorized access, and could modify and/or destroy sensitive data and disrupt the continuity of system availability.

In-house Developed Supervisor Call Instruction

Supervisor Call Instruction is a set of special machine instructions within an operating system that is used by a program to communicate with the operating system. For example, a "calling" program uses the Supervisor Call Instruction mechanism to request that the operating system perform a desired function, such as opening a data file for modification. An SVC could allow a user virtually unlimited access to the computer system. A review of Federal computer systems, performed by the President's Council on Integrity and Efficiency, showed that non-Multiple Virtual Storage vendor-provided Supervisor Call Instruction creates one of the greatest vulnerabilities for operating systems.

We identified 15 non-MVS vendor-provided SVCs and selected one that was developed in-house for detailed analysis. This SVC was written by EIA's ADP Services Staff to support inhouse developed programs. We found two control weaknesses in the SVC.

The user account that authorized access to the SVC was displayed in the code of the SVC without encryption. Thus, the 11 user accounts with system-wide privileges under ACF-2 and any user granted system-wide read-only privilege could readily determine the authorized user account code of the SVC. Authorization checks with readable user accounts undermine the intent of security software (such as ACF-2) that controls and validates user accounts and passwords in granting access privileges.

The SVC also contained a parameter that could be used to bypass all authorization checks, including the check for authorized user accounts. The SVC had not been properly coded to disallow the parameter value that would bypass authorization checks. Also, the account code checks had not created an adequate interface between the SVC and ACF-2, the security software. This interface should not only check for proper user accounts and passwords, but also keep usage records as audit trails. This deficiency could be used to circumvent operating system and security software controls.

Knowledgeable users could take advantage of both of these weaknesses to gain unauthorized control of the computer system and modify and/or destroy sensitive and critical data.

4. System Software Maintenance

FINDING

Departmental policy requires that computer systems be protected from unnecessary processing delays. Federal processing standards stress the importance of an orderly and controlled maintenance process to ensure system availability. EIA had two software maintenance problems: undocumented software changes needed to be documented, and vendor-provided corrections for system software needed to be installed. Undocumented software changes occurred because the ADP Services Staff had allowed the use of a program commonly known as SUPERZAP 6/, which does not automatically document changes. Vendor-provided corrections were not made because EIA did not install them due to workload backlogs caused by contractual difficulties. These deficiencies could cause malfunctions of the operating system or system failures. Also, supported user applications and vital reporting of energy statistics mandated by the Congress could be disrupted.

RECOMMENDATIONS

We recommend that the Director, Automated Data Processing Services Staff, Energy Information Administration:

1. Strengthen system maintenance by:
 - o enforcing the use of the vendor recommended System Maintenance Program when modifying system software to assure that changes are documented; and
 - o controlling the use of the SUPERZAP utility outside of SMP by requiring written justification and documentation of the changes made.
2. Determine which vendor-provided software corrections should be installed by:
 - o analyzing the report on unresolved operating system problems; and
 - o performing periodic analysis of system software maintenance levels.

MANAGEMENT REACTION

Management concurred with the recommendations.

6/ SUPERZAP is a system utility special purpose program.

DETAILS OF FINDING

DOE Order 1360.2A requires that unclassified computer systems and applications be protected from unnecessary processing delays. *Federal Information Processing Publication* (FIPS PUB) 106 defines software maintenance as "the performance of those activities required to keep a software system operational and responsive after it is accepted and placed into production." The realistic goal of software maintenance management is to keep the software maintenance process orderly and under control. In sophisticated and complex operating system environments, proper control in the performance of routine and special maintenance is essential to ensure continued systems reliability and availability. We examined selected practices for modifying software modules and installing vendor-provided corrections. The results are discussed below.

Use of SUPERZAP

The System Modification Program is a product recommended for use in controlling modifications to all vendor-provided system software. It provides capabilities for managing a computer installation's software inventory. When the program is used for system changes, it creates extensive records of additions and modifications in a specially controlled historical file.

The ADP Services Staff had not used the System Modification Program to perform all maintenance tasks for the operating system. We used computer assisted audit techniques to determine how many times no identification records were left when maintenance was applied to a selected library of the operating system software. These records provide a date and comment identifying the nature of the change made, thus providing an audit trail of the software change process. The analysis indicated 128 instances of system software modifications made without identification records. The modifications were made to frequently used operating system programs.

The undocumented modifications occurred because special justification was not required for using SUPERZAP. Also, there was no requirement to document changes made using SUPERZAP. In addition, management did not enforce the use of the vendor recommended System Maintenance Program when software was modified.

Management should control changes made to the system software. When unrecorded modifications are allowed, problems or errors causing system performance degradations or failures are difficult to detect and correct. This weakness could adversely affect EIA's ability to collect and analyze energy data and produce statistical reports vital to our national interest.

Maintenance Level

We used a commercially available diagnostic software package to examine unresolved software problems. The software package provided comprehensive information on unresolved software problems by severity level in various functional management areas. These severity levels were: *critical*, *impacting*, and *limited*. Problems in the *critical* level could result in substantial adverse impact on performance, security, user data, system data, measurement data or system availability. The *impacting* level would have less severe

impact. Problems in the *limited* level would be less serious, but should not be considered trivial.

The diagnostic software package identified 613 instances of unresolved operating system problems at the EIA Forrestal Computer Facility. It identified 55 *critical*, 225 *impacting*, and 333 *limited* problems. These problems were not identified or fixed because EIA had not analyzed the system maintenance level to determine which vendor-provided corrections should be installed.

The 55 problems considered *critical*, if left unresolved, could result in substantial adverse impact on performance, security, user or system data, measurement data or system availability. For instance, critical problems could cause system failures, lost system accounting or user data, and abnormal termination of system functions. Although the 225 *impacting* problems are considered less severe, some of them could cause lost user data, functional errors, and decreased availability of system resources. The *limited* problems also warrant some attention because they could result in increased response time, partial data loss, and abnormal termination of processing functions. We believe the problems identified by the diagnostic software package warrant special attention by EIA's Automated Data Processing Services Staff.

PART III

MANAGEMENT AND AUDITOR COMMENTS

On July 23, 1991, the Administrator, Energy Information Administration, provided comments on our draft report. Management comments on the four findings and the respective recommendations are summarized below with auditor responses.

1. DISK SPACE UTILIZATION

Management disagreed with the finding, but generally concurred with the intent of the recommendations. Management's general comments are followed by specific comments on each recommendation.

Management Comments. Management could not reconcile or verify the data used in the Office of Inspector General (OIG) report because the ADP Services Staff's system is constantly changing, and they did not have the machine readable copy of the data that was used.

Auditor Comments. The ADP Services Staff should have this data on their computer system and archived under account BH36991. All data used in our report was developed on EIA's computer system.

Management Comments. In the OIG's workpaper on device type Summary Statistics under the 3380 Potential Saving, the numbers in the columns do not add up. An explanation has not been presented, and a method of verifying this has not been provided.

Auditor Comments. To prepare the finding, we used an analysis that screened out double counting; this is why the figures don't add up. The workpapers to which management refers contained the program logic for the analysis, and management did have access to that data.

Management Comments. The OIG cost calculations on the value of potentially recoverable disk space made the assumption that all space is recoverable for the entire year. This assumption is misleading. Consequently, the estimate of potentially recoverable disk space is too high by orders of magnitude. Also, the ADP Services Staff believes that any computations based upon the output of a single run distorts the true facts.

Auditor Comments. Our potential cost savings were based on a one-time "snapshot" projected for one year; this is an accepted auditing practice. However, when we took another snapshot 3 months later, it produced results with slightly higher potential savings. Therefore, we believe that our projection fairly represents the potential savings.

Recommendation 1

Management concurred with the intent of our recommendation to adopt policy and procedures that require transferring disk data sets to tape after a period of inactivity.

Management Comments. The OIG analysis on potentially recoverable disk space included operating system disk packs, system work packs, system spare packs, system spool packs, and system test packs. In reviewing workpapers and excluding system volumes and system data sets on user disk packs, very little remains which is not archived on a regular basis. The ADP Services Staff cannot archive any system or program products that are listed as available in the *EIA User's Guide*. They must be available at all times, otherwise, when a user called for a system/program product, an error would occur possibly hours into running a multi-step job.

Auditor Comments. Our analysis showed that the equivalent of 12.4 disk packs (based on 637 megabytes per disk pack) had not been accessed for more than 45 days and, of that total, the equivalent of 9.1 disk packs had not been accessed in more than 180 days. This represents one out of every nine physical disk packs on the system. The ADP Services Staff has indicated that these represent system/program products, which are listed as available in the *EIA User's Guide*. Since normal business practice is to discontinue stocking items for which there is low demand, we believe that significant cost savings could result if ADP Services Staff were to archive these products or programs and publish retrieval procedures in the *EIA User's Guide*.

Management Comments. Transferring disk data sets to tape after a period of inactivity has been an ADP Services Staff practice and procedure for at least 10 years. However, in order to increase user awareness of this, ADP Services Staff will prepare disk space utilization articles for the periodic newsletter and will highlight disk space management in our user training programs.

Auditor Comments. Increasing user awareness of efficient disk storage practices would be partially responsive to our recommendations. However, rather than merely encouraging the users to comply, we recommended that this be a requirement.

Management Comments. Model Data Set Control Blocks (DSCB) for generation data sets do not take up one track. This is an error in the OIG program which should be fixed. The ADP Services Staff estimates that about 1,000 DSCB's with a size of one track were included in the OIG analysis. This also overstates the potential free disk space.

Auditor Comments. These DSCB's were deleted from our computations prior to issuance of this finding.

Management Comments. Each disk pack has a volume table of contents (VTOC) about 30 to 45 tracks long. These VTOCs are reflected as not being used when, in essence, they are. The last used indicator is normally not updated unless the VTOC is deleted and reallocated.

Auditor Comments. We agree and have made appropriate adjustments.

Recommendation 2

Management generally concurred with our recommendation to adopt policy and procedures that require eliminating invalid data sets.

Management Comments. Invalid data sets are being eliminated by the ADP Services Staff. A program is run weekly to eliminate the invalid data sets that have been allocated but not opened for 5 days or more. No explanation has been presented on what the OIG considers an invalid data set. The ADP Services Staff has not seen this to have a major impact on Disk Access Space Device resources.

Auditor Comments. Invalid data sets are those for which a name and space have been assigned, but that do not have valid data set organization parameters. We used the analysis program on two separate occasions to analyze disk usage. We found a slight increase in the number of invalid data sets and the amount of disk space occupied by these data sets. We concluded that the ADP Services Staff either did not run the program often enough or the program did not eliminate all invalid data sets. Although this may not have a major impact on disk space resources, we believe it indicates a procedural weaknesses.

Recommendation 3

Management generally disagreed with our recommendation to adopt policy and procedures that require releasing unused reserved disk space.

Management Comments. Management stated that releasing this space would create an operational problem and that the OIG analysis failed to recognize that part of the potentially recoverable disk space was ADP Services Staff data sets used to reserve large amounts of contiguous disk space for certain jobs and for emergency processing requirements. It said that disk space shortage creates an emergency, which must be resolved in a short time. The quickest and most efficient way to solve this is to have reserved disk space resources under the control of the ADP Services Staff that can be made available to the user community immediately.

Auditor Comments. Reserving large amounts of disk space (approximately 15 packs) inflates actual usage. The practice of maintaining empty data sets to reserve space for specific users can and will create the very shortages that the empty data sets are meant to avoid. Some ADP Services Staff reserved-space has not been accessed in approximately 2 years. Other techniques, such as disk reorganization or setting limits on percent of utilization, would allow management to satisfy needs for large amounts of contiguous space or for emergency processing.

Management Comments. Users are encouraged to code "RELEASE" on their job control statements that allocate disk space. The ADP Services Staff cannot automatically change these job control statements without creating problems. However, ADP Services Staff does periodically run a program against data sets that releases over-allocated space.

Auditor Comments. Accepted industry practice is to scan a job before execution to ensure the use of proper parameters for releasing unused space. It is more efficient to code the proper parameter for releasing unused space before creating the data set than to use computer resources to recover unused space after the data set is created. However, running a program after the fact to release over-allocated space would be effective if it were done often

enough. Our analysis indicated that over 10 percent of space was over-allocated, which indicates the ADP Services Staff program should probably be used more often.

Recommendation 4

Management generally disagreed with our recommendation to adopt policy and procedures that require setting block size for at least 90 percent efficiency.

Management Comments. Users are encouraged to utilize full track blocking. However, this policy is not enforceable because it could cause user's jobs to abort if the ADP Services Staff were to automatically reblock their data sets.

Auditor Comments. Another accepted industry practice is to scan a job before execution to ensure the use of proper parameters for efficient blocking size. Better blocking, combined with use of the "RELEASE" parameter, leads to more efficient utilization of resources, with a potential space recovery equivalent of about 15 disk packs.

2. DATA STORAGE ON TAPE

Management concurred with the recommendations.

Management Comments. Management will investigate transferring data from reel tapes to cartridges after it completes a project to determine which data must be retained and to ensure that the data is being maintained properly. It also will investigate the true life of cartridge tapes and will publish this information for users.

Auditor Comments. Management's planned actions are responsive and should achieve the intent of our recommendations.

3. SYSTEM CONTROLS

Management concurred with the intent of the recommendations. It partially concurred with Recommendations 3 and 4.

Recommendation 1

Management concurred with the intent of our recommendation that ADP Services Staff define a set of criteria in the policy and procedures for maintaining Access Control Facility 2 privileges that would ensure separation of duties when granting special user privileges.

Management Comments. A management decision had been made that the complete separation of duties is not feasible with their operational realities. It stated that all of the users with these security and account privileges are internal systems software personnel. The ADP Services Staff has never seen a problem with not having a complete separation of duties.

Auditor Comments. Management should review Federal requirements for separation of duties, and consider the risks of not implementing them. Our recommendation is consistent with OMB Circular A-123 on internal controls. We

believe that separation of duties is not only possible for the functions described by management, but highly desirable to maintain adequate internal controls. As stated in this report, the *Technical Reference Series* published by Ernst and Whinney recommends that special system-wide user privileges, such as ACCOUNT and SECURITY, should not be granted to the same user. Furthermore, statistics suggest that the greatest threat to computer security is employees with special access privileges that have information about computer loopholes. Because the internal systems software personnel have system-wide privileges and the knowledge about computer loopholes, they fit into this category.

Recommendation 2

Management concurred with the intent of our recommendation to limit the special user privileges granted based on defined criteria (see Recommendation 1), but disagreed with the specific implementation.

Management Comments. The ADP Services Staff has a set criteria for allocating and maintaining Access Control Facility 2 privileges in an unclassified environment. Special user privileges are assigned according to these criteria. Management believed that both ACCOUNT and SECURITY privileges were required by 10 personnel, and that this exposure is small because an independent computer security contractor monitors all activities and advises the Staff of unusual happenings immediately.

Auditor Comments. The ADP Services Staff criteria does not provide for separation of duties in compliance with Federal guidelines, such as OMB Circular A-123, OMB Circular A-130, and the Federal Managers Financial Integrity Act (FMFIA). We believe that users with both ACCOUNT and SECURITY privileges represent an internal control weakness. For example, MCI, a leading telecommunications company, has only three individuals with either privilege, and no individual with both.

Recommendation 3

Management concurred with the recommendation to delete names of libraries of authorized programs no longer in use and establish procedures to ensure that unused authorized library names are deleted.

Management Comments. The ADP Services Staff has deleted names of libraries of authorized programs that do not exist and will monitor this area more closely in the future.

Auditor Comments. Management's reply is responsive to this recommendation.

Recommendation 4

Management concurred with the recommendation to modify Supervisor Call to disallow the particular bypass of authorization checks and implement an interface between the SVC and Access Control Facility 2, the security software.

Management Comments. The ADP Services Staff has fixed the Supervisor Call that had a potential security weakness. The Staff is modifying the SVC to record usage records for audit trail purposes.

Auditor Comments. Management's reply is responsive to this recommendation.

4. SYSTEM SOFTWARE MAINTENANCE

Management concurred with the recommendations.

Management Comments. Management stated that system software management and maintenance procedures have been in place for many years, and have worked satisfactorily. However, the ADP Services Staff has reemphasized to system software personnel to use the System Modification Program procedures whenever possible and to thoroughly document all uses of the SUPERZAP utility. Software maintenance is now as current as the ADP Services Staff analysis indicates it should be. The Staff will continue to analyze unresolved operating system problems and system software maintenance levels and apply corrections and maintenance levels as needed and appropriate.

Auditor Comments. Management's response and proposed actions are responsive to our recommendations.

END

**DATE
FILMED**

12/30/91