DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Memorandum

Date JAN 30 1998

From Deputy Inspector General
for Audit Services

Subject Report on Policies and Procedures Placed in Operation and Tests of Operating Effectiveness for the Division of Computer Research and Technology, National Institutes of Health (A-17-97-00013)

To Distribution List

The Department of Health and Human Services (HHS) Division of Computer Research and Technology (DCRT) provides a variety of data processing services on a fee-for-service basis to the National Institutes of Health and other HHS agencies. The attached report presents the results of Ernst & Young's (E&Y), Certified Public Accountants, review of DCRT's policies and procedures placed in operation and tests of operating effectiveness. The E&Y conducted the examination under contract with the HHS Office of Inspector General. In our technical oversight and quality control of the examination, we found nothing to indicate that E&Y's work was inappropriate or that the report cannot be relied upon.

The objectives of the examination were to obtain reasonable assurance about whether; (1) the description of DCRT policies and procedures presents fairly, in all material respects, the aspects of DCRT's policies and procedures that may be relevant to a user organization's internal control structure, (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the descriptions, and (3) such policies and procedures had been placed in operation as of September 30, 1997.

As discussed in the attached report, E&Y determined that DCRT is not able to control monitoring and administration of computer machine room access privileges. This resulted in the policies and procedures not being suitably designed to achieve the control objective that states, "Control structure policies and procedures provide reasonable assurance that physical access to the computer center and other sensitive areas, and operations of the computer and related processing equipment is restricted to appropriately authorized individuals."

The E&Y concluded that the description of DCRT operations presents fairly, in all material respects, the relevant aspects of DCRT's policies and procedures placed in operation as of September 30, 1997. Also, E&Y concluded that the control structure policies and procedures as described, except for the matters described in the preceding paragraph, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved. Lastly, E&Y concluded that the control policies and procedures tested were operating with sufficient effectiveness, except for the matters

described in the third paragraph above, to provide reasonable, but not absolute, assurance that the control objectives specified were achieved during the specified period.

The relative effectiveness and significance of specific policies and procedures at DCRT and their effect on assessment of control risk at user organizations are dependent upon their interaction with policies and procedures present at individual user organizations. The DCRT controls were designed with the assumption that certain internal control structure policies and procedures would be implemented by user organizations. To ensure that the control structure policies and procedures included in this report are achieved, users of DCRT should implement their own control structure policies and procedures that acheive the control structure policies and procedures indentified on pages 10 and 11.

For Fiscal Year 1998 audit planning purposes, we plan to retain certified public accountants to perform a similar review covering Fiscal Year 1998 activity. We estimate that the results of the review will be available in December 1998.

Should you wish to discuss this report, please call me or have your staff contact Joseph E. Vengrin, Assistant Inspector General for Audit Operations and Financial Statement Activities, at (202) 619-1157. Please refer to the Common Identification Number A-17-97-00013 in all correspondence relating to this report.

Thomas D. Roslewicz

Attachment

National Institutes of Health

Division of Computer Research and Technology

Report on Policies and Procedures Placed in Operation and Tests of Operating Effectiveness

NATIONAL INSTITUTES OF HEALTH
DIVISION OF COMPUTER RESEARCH AND TECHNOLOGY (DCRT)

REPORT ON POLICIES AND PROCEDURES PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS FOR THE DIVISION OF COMPUTER RESEARCH AND TECHNOLOGY (DCRT)

Table of Contents

I. INDEPENDENT SERVICE AUDITOR'S REPORT 1

II. NATIONAL INSTITUTES OF HEALTH, DIVISION OF COMPUTER RESEARCH AND TECHNOLOGY

DESCRIPTION OF POLICIES AND PROCEDURES 3

Overview of Operations 3
Overview of Control Environment 4
Control Objectives and Related Policies and Procedures 10
User Control Considerations 10

III. INFORMATION PROVIDED BY ERNST & YOUNG LLP 13

Tests of Control Environment Elements 13
Control Objectives, Related Policies and Procedures, and
Tests of Operating Effectiveness 13
Access to Data Files and Programs 13
Violation Monitoring and Reporting Procedures 22
System Software Implementation and Maintenance 25
Physical Security 29

IV. OTHER INFORMATION PROVIDED BY NATIONAL INSTITUTES OF HEALTH, DIVISION OF COMPUTER RESEARCH AND TECHNOLOGY 35

ERNST & YOUNG LLP ■ 1225 Connecticut Avenue, N.W. Washington, D.C. 20036 ■ Phone: 202 327 6000

Section I -- INDEPENDENT SERVICE AUDITOR'S REPORT

National Institutes of Health
Bethesda, Maryland

We have examined the accompanying description of the Computer Center operations of the National Institutes of Health (NIH) Division of Computer Research and Technology (DCRT). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of DCRT's policies and procedures that may be relevant to a user organization's internal control structure, (2) the control structure policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if those policies and procedures were complied with satisfactorily, and, if user organizations applied the internal control structure policies and procedures contemplated in the design of DCRT's policies and procedures, and (3) such policies and procedures had been placed in operation as of September 30, 1997. The control objectives were specified by the management of DCRT. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

As discussed in the accompanying description, DCRT is not able to control monitoring and administration of computer machine room access privileges. This results in the policies and procedures not being suitably designed to achieve the control objective that states "Control structure policies and procedures provide reasonable assurance that physical access to the Computer Center and other sensitive areas, and operation of the computer and related processing equipment is restricted to appropriately authorized individuals."

In our opinion, the accompanying description of the aforementioned Computer Center operations presents fairly, in all material respects, the relevant aspects of DCRT's policies and procedures that had been placed in operation as of September 30, 1997. Also, in our opinion, the control structure policies and procedures as described, except for the matters described in the preceding paragraph, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described control structure policies and procedures were complied with satisfactorily, and if user organizations applied the internal control structure policies and procedures contemplated in the design of DCRT's policies and procedures as described in its description.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific policies and procedures, listed in our description of the tests of operating effectiveness, to obtain evidence about their effectiveness in meeting the control objectives described in our description of those tests during the period from April 1, 1997 to September 30, 1997. The specific policies and

procedures and the nature, timing, extent, and results of the tests are listed in our description of the tests of operating effectiveness. This information has been provided to user organizations of DCRT and to their auditors to be taken into consideration, along with information about the internal control structure at user organizations, when making assessments of control risk for user organizations. In our opinion, the control structure policies and procedures that were tested, as described in Section III of this report, were operating with sufficient effectiveness, except for the matter described in the second paragraph above, to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period from April 1, 1997 to September 30, 1997.

The relative effectiveness and significance of specific policies and procedures at DCRT and their effect on assessments of control risk at user organizations are dependent upon their interaction with the policies, procedures, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of the policies and procedures placed in operation at individual user organizations.

The description of the policies and procedures at DCRT is as of September 30, 1997 and the information about tests of the operating effectiveness of specified control structure policies and procedures covers the period from April 1, 1997 to September 30, 1997. Any projection of such information to the future is subject to the risk that, because of changes, the description may no longer portray the system in existence. The potential effectiveness of the specified policies and procedures at the service organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

The information included in Section IV of this report is presented by DCRT to provide additional information to user organizations and is not part of DCRT's description of policies and procedures placed in operation. The information in Section IV has not been subjected to the procedures applied in the examination of the description of policies and procedures, and accordingly, we express no opinion on it.

This report is intended solely for use by the management of DCRT, its user organizations, and the independent auditors of its user organizations.

September 30, 1997

Ernst + Young

Section II -- NATIONAL INSTITUTES OF HEALTH
DIVISION OF COMPUTER RESEARCH AND TECHNOLOGY
DESCRIPTION OF POLICIES AND PROCEDURES

OVERVIEW OF OPERATIONS

The National Institutes of Health (NIH), Division of Computer Research and Technology (DCRT) is located in Bethesda, Maryland. DCRT provides a variety of data processing services on a fee-for-service basis to the NIH and other governmental agencies. Although DCRT is not responsible for actual user applications, it does own and operate the overall computer facility and hence, is responsible for its general controls. The general control areas that are controlled by DCRT are:

- system parameter settings available within IBM's Resource Access Control Facility (RACF) which is used to provide logical access control;
- system software maintenance;
- physical access to the DCRT Computer Center; and
- back-up and contingency planning.

DCRT uses IBM's Multiple Virtual System/Enterprise System Architecture (MVS/ESA) operating system. The MVS/ESA operating system and Job Entry System 2 (JES2), incorporating the NIH-developed Shared Spool capability, present a unified system interface to the user. The MVS/ESA system offers: batch processing with capability for hundreds of concurrent jobs; library of utilities and routines; full suite of interactive systems: Time Sharing Option (TSO), Customer Information Control System (CICS), Interactive System Productivity Facility (ISPF), WYLBUR; online services such as E-mail, bulletin boards, telephone directories, account information, problem reporting, training, schedules, and class registration; access via a variety of network and telecommunication methods; language compilers (e.g., COBOL, FORTRAN, C, C++, VSBASIC, REXX, Assembler, etc.); database systems (Oracle, DB2, and IMS); disaster recovery planning; RACF security; data encryption; automatic data backup; and gateways for client/server applications.

In July 1997, another DHHS computer center (the MVS portion of the Information Technology Service formerly located on the 2nd floor of the Parklawn Building in Rockville, Maryland), was consolidated into the Computer Center located at DCRT's Building 12 Complex. The majority of the software and personnel from the Information Technology Service data center were moved and consolidated with the Computer Center resources at DCRT. The computing environment associated with the former Data Center was named the North System and the computing environment which originated from the DCRT Computer Center was named the South System. The North System also runs on MVS/ESA with JES2, TSO and CICS. The North System operates Oracle and ADABAS

database systems, DASD, tape drives, and a tape library which is separate from the South System. The North System runs on its own logical partition (LPAR) on an IBM 9672 mainframe. The South System runs on several LPARs spread across two IBM 9672 mainframes.

DCRT is currently establishing an Enterprise Open System based on a DEC Alpha 8400 running Digital UNIX. Since this system did not include production user applications during the audit period, it was not included in this review.

DCRT also has other computer systems that are used primarily for scientific applications and are not part of this review.

OVERVIEW OF CONTROL ENVIRONMENT

An organization's control environment reflects the overall attitude, awareness, and actions of management, and others concerning the importance of controls and the emphasis given to controls in the organization's policies, procedures, methods and organizational structure. The following is a description of the key policies and procedures that are generally considered to be part of the control environment.

Organizational Structure

The National Institutes of Health (employing approximately 16,000 people) consists of approximately 25 different Institutes, Centers, and Divisions (ICDs). NIH is primarily located on the Bethesda campus. In addition, portions are at Poolesville, Maryland, the Research Triangle in North Carolina, Montana, Massachusetts, and other locations.

The NIH Office of Information Resources Management (OIRM)

Within the NIH organization, the OIRM is developing an IRM program to enhance existing NIH Federal Information Processing (FIP) resources to achieve the following: meet changing user requirements; integrate information from various sources to assist decision making; and ensure the IRM program remains current with Federal IRM requirements.

The Division of Computer Research and Technology

DCRT is one of the divisions within NIH. There are approximately 400 employees in the entire DCRT division. Most of the DCRT employees are located in the Building 12 complex (Building 12, 12A, and 12B) of the NIH campus. Other staff are in Building 31, the Federal Building in Bethesda, and the Executive Plaza in Rockville, MD. There are two main organizational components: 1) Research (Office of Computational Bioscience) with approximately 25 - 30 staff , and 2) Services (Office of Computing Resources and Services) with over 300 staff. The Office of Computing Resources and Services currently consists of four branches.

The Office of Computing Resources and Services branches are described below.

Computing Facilities Branch (CFB)

The CFB operates the large-scale mainframe computer complex known as the NIH Computer Center. This includes the design, selection, implementation, and maintenance of a unified set of computing facilities composed of multiple subsystems and highly sophisticated operating system software. The CFB uses the capacity management approach, aligning available computing capacity with user requirements. An equally important aspect of the mission of the CFB is to assist persons using those facilities. The CFB provides guidance and support to current and prospective users on connectivity technologies. This includes accessing all central facilities from personal workstations, local area networks, and wide area networks.

The CFB's MVS/ESA system has been developed to support the intramural, extramural and administrative programs of NIH. The NIH Computer Center also performs processing for other government agencies.

The CFB is responsible for the development, operation, and support for all centrally owned, shared-use computing resources. The CFB plans to undertake a number of new strategic directions in the near future that will significantly benefit users.

The CFB consists of the following sections:

Systems Operations Management Section (SOMS)

SOMS manages and operates diverse computing platforms, auxiliary systems, output services, and other functions in support of the CFB; provides management and problem resolution for telecommunication services offered by CFB; selects, implements and utilizes automated operations tools to provide and improve responsive, reliable service to the customer community by CFB; and manages the installation of the computing platforms selected by the CFB, the physical plant supporting them and physical security controlling access to them.

Enterprise Systems Software Section (ESSS)

ESSS provides system services for planning, selection, evaluation, design, development, management, and support of central, general purpose, computing and storage management facilities for corporate use, particularly including the MVS/ESA operating environment; evaluates, selects, and integrates alternative computing systems technologies of potential interest to a broad cross-section of the customer community.

Enterprise Applications Support Section (EASS)

EASS seeks, evaluates, selects, documents, supports, provides instruction on, and promotes general software products and services needed for the existing MVS/ESA system user environment and for enterprise use in emerging computing environments; performs software installs, change management, and problem management for products that it supports, as well as selected others; provides a link between CFB and Computer Services Branch (CSB) for support needed by enterprise systems users; and conducts

research, systems integration, and development to apply new computing technologies to the needs of enterprise applications, to enhance current software offerings, and to maintain current knowledge of emerging computing capabilities.

Database Support Section (DBSS)

DBSS works with users and other branches within DCRT to identify promising database and information processing technologies; evaluates and provides database and information technologies that enhance access to centralized data; provides a stable software and data repository environment for enterprise-wide database and information systems; and supports and assists ICDs in implementing appropriate technologies to meet their centralized database and information processing needs.

In order to make help readily available to all users, a variety of assistance programs are in place: telephone and walk-in consulting, provided by DCRT Technical Assistance and Support (TASC); online problem reporting, through the Problem Tracking Report (PTR) mechanism; and the DCRT Training Program that includes classroom courses, short seminars, and interactive computing courses. The DCRT Technical Information Office distributes a full range of vendor-supplied and DCRT-written documentation to users. These support services are available to all registered Computer Center users.

The NIH Computer Center currently encompasses two interconnected mainframe facilities, the MVS/ESA system and the Helix Systems, as well as the Advanced Laboratory Workstation System for distributed computing. Users have an array of software tools available and the computing power to use those tools to their best advantage. Each facility offers a range of online and off-line services. The systems are linked together by high-speed telecommunications lines to facilitate the exchange of data and programs.

High Performance Scientific Computing Section (HPSCS)

HPSCS plans, manages, and supports centrally managed high performance computers for use by NIH scientists; evaluates new high performance technologies and incorporates them into production work at NIH; installs and supports scientific applications both locally and through national networks, and provides facilities for disseminating information from NIH through networks; and supports servers for and incorporates high performance systems into a distributed computing environment at NIH.

Distributed Systems Section (DSS)

DSS investigates, evaluates, and applies distributed computing technologies, such as distributed file systems, network-transparent graphics systems, distributed transaction processing, and object-based distributed systems; identifies, acquires or develops, tests, evaluates, and deploys networked, interoperable, open-architecture, distributed computing environments; contributes to the development of and applies standards to achieve and maintain software portability across differing machine architectures from a variety of vendors; and participates in the development of operating and support

procedures and user training materials and documentation for networked computing environments.

Information Systems Branch (ISB)

The ISB serves as a central NIH resource to provide advice and services to the NIH user community in the development and maintenance of computer-based information systems. The ISB provides advice and assistance to research investigators, program officials and administrators throughout NIH in planning and obtaining computer information services. The ISB also develops, maintains, and processes the NIH Administrative Database and the Clinical Center's Clinical Information Utility.

Network Systems Branch (NSB)

The NSB is responsible for the ongoing support and development of NIHnet, the wide area network that currently connects nearly 300 NIH Local Area Networks (LANs) in over 60 locations. The NSB provides leadership in developing and implementing networking and other communications technologies for the NIH campus and its outlying facilities. The NSB also maintains liaisons with networking activities within various NIH institutes as well as other Department of Health and Human Services organizations to improve the overall networking and information dissemination infrastructure.

Customer Services Branch (CSB)

The CSB is responsible for customer consulting for virtually all DCRT services via the Technical Assistance and Support Center (TASC). CSB also handles documentation and software distribution, plans and implements the DCRT Training Program, and administers DCRT accounts.

Policies and Procedures

DCRT has developed formal policies and procedures covering various financial and operational matters and all critical aspects of employment services applicable to management personnel, including: hiring, training/development, performance appraisals and terminations. In addition, all new employees are issued an employee information kit when hired that documents various procedural and administrative matters applicable to them.

The Human Resources department is responsible for the initial recruiting and evaluation of job applicants in accordance with the Federal government's affirmative action program. Once the selection process has been completed, qualified applicants are referred to the applicable operating department manager for the final hiring decision.

Performance appraisals are required for all employees of the organization by their immediate supervisor every 6 to 12 months; more frequent progress appraisals are performed for new employees. DCRT uses formal classroom instruction and on-the-job employee training programs for all departments and functions.

Backup and Contingency Planning

North and South System

The Computer Center has an un-interruptible power supply (UPS) for use on the centralized computing, data storage, and communications facilities managed by the Center. The UPS eliminates virtually all power interruptions, such as those caused by sudden surges or drops in power, or violent weather conditions.

The UPS system is designed to provide all electrical service to Building 12 - the core of the NIH Computing Center that houses the hubs and routers of the NIHnet, the enterprise servers supporting NIH, and super-computers.

Within the Computer Center there is one fire extinguisher every 50 feet, water detectors beneath the raised floor and smoke detectors on the ceiling as well as beneath the raised floor to provide adequate environmental controls. In addition to these detection devices, there are Honeywell temperature and humidity monitoring systems that monitor the first and second floors of the Computer Center.

South System

The Computer Center creates full volume backups every week of all public and critical system disks that are used for the permanent storage of data. Bi-weekly, all disks (including private disks) are backed up and stored off site. At their own discretion, user organizations may arrange more frequent backups and off-site rotations. In addition, RAID 5 technology is used for real-time, redundant backup of all disks. Incremental backups are also made daily for public disks and kept on-site.

DCRT accepts responsibility for providing an alternative (off-site) recovery resource for designated critical applications, and for developing suitable communications access to the resources. DCRT has signed an agreement with the General Services Administration and Federal Systems Integration Management that obligates Comdisco Disaster Recovery Services (CDRS) to provide hot-site and cold-site (a machine room floor) facilities and services to the NIH Computer Center. The agreement is renewed annually. DCRT primarily uses the CDRS hot-site in North Bergen, New Jersey because of its convenient location, along with a business recovery facility (for a command post) in Columbia, Maryland. The agreement obligates CDRS to provide at least one hot-site and cold-site in case of disastrous events.

The Computing Facilities Branch has a formal disaster recovery program which includes a full time Disaster Recovery Coordinator, and has developed a written disaster recovery plan. This plan provides disaster recovery facilities and services for some "critical" applications that run on the Center's MVS System. These applications, originally identified by the NIH Office of Information Resources Management (OIRM), have voluntarily joined the Computer Center's disaster recovery program. Their owners have accepted responsibility to prepare for disasters and periodically test their disaster recovery procedures. Program managers of other important applications can self-declare their applications as critical, and be included in the formal disaster recovery program.

The Computing Facilities Branch continually reviews and tests its disaster recovery plan twice a year with CDRS. DCRT successfully conducted a disaster recovery exercise on May 13, 1997. The test partially restored telecommunication links, and fully restored the MVS operating system, and major subsystems such as Information Management System (IMS), and SAS. Tests of applications were the user organizations' responsibility. DCRT invited all users of designated critical applications to participate in the exercise. DCRT provides a user assistance team during all disaster recovery (DR) tests to provide user support.

In the event of a disaster, the Damage Assessment Team will evaluate the damage to the physical assets and functional capability of the Computer Center, and report its findings to the Executive Team. The Executive Team (consisting of the Chief and Deputy Chief of the Computer Center, DR Coordinator, and three other senior managers in CFB) will then consider the findings of the Damage Assessment Team, along with other available information, and will make a decision on declaring a disaster. Only the Executive Team has the authority to declare a disaster.

The CFB Disaster Recovery Manager is responsible for orchestrating the execution of the CFB Disaster Recovery Plan. The Disaster Recovery Plan defines the leaders, contact numbers as well as pre/post-disaster duties and responsibilities for the Damage Assessment Team and Executive Team and other functional teams.

The Disaster Recovery Plan describes emergency procedures to handle disasters during or after normal business hours. Employees requesting and accepting the physical delivery of the media must be in possession of a valid First Federal IS badge issued by the appropriate level of authority.

North System

For the North System, efforts are underway to provide similar policies, procedures and facilities as the South System, including the hot site recovery capability with Comdisco.

CONTROL OBJECTIVES AND RELATED POLICIES AND PROCEDURES

DCRT's control objectives and related policies and procedures are included in Section III of this report, Information Provided by Ernst and Young LLP, to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III. Although the control objectives and related policies and procedures are included in Section III, they are, nevertheless, an integral part of the DCRT's Description of Policies and Procedures.

USER CONTROL CONSIDERATIONS

DCRT's controls were designed with the assumption that certain internal control structure policies and procedures would be implemented by user organizations. In certain situations, the application of specified internal control structure policies and procedures at user organizations is necessary to achieve certain control objectives included in this report. In such instances, the required user organization internal control structure policies and procedures are indicated under the related control objective in Section III of this report.

This section describes other internal control structure policies and procedures that should be in operation at user organizations to complement the control structure policies and procedures at DCRT. User auditors should consider whether the following policies and procedures have been placed in operation at user organizations:

Data and Access Security

For both the North and South System, user organizations are responsible for:

- reviewing and ensuring that the RACF universal access authority levels specified for their data sets prohibit unauthorized access.

For the South System, user organizations are responsible for:

- determining other types of computerized data that may need protection and for choosing and using appropriate security measures. Since the research mission of NIH requires data and information sharing, there will always by design be data that is not protected against access. Data should be protected from unauthorized access unless it is clearly intended for shared access.

- creating their own generic or discrete profiles within RACF to protect their data sets

- protecting their own tape data sets through such means as DCRT's VOLSTAT facility.

- forcing periodic password changes more frequently than 180 days if desired.

- creating and disseminating user organization policy for password parameters such as no reuse of prior passwords, minimum length of password and requirements for combination of letter and numbers within a password.

- coordinating with DCRT on the use of RACF to protect IMS resources. IMS resources such as IMS transactions are not protected by RACF.

- investigating possible access violations noted by DCRT and returning a written explanation to the DCRT Computing Facilities Branch responding to each instance. The Computing Facilities Branch staff works with the account sponsor at the user organization to determine the cause of the problem and how violations can be avoided in the future.

For the North System, user organizations are responsible for:

- assigning a RACF Coordinator to implement the organization's security policies for using RACF. The RACF Coordinator assists users in recovering from forgotten passwords and grants access to data. The Coordinator may also review and resolve unauthorized access attempts, review reports of unresolved violations, and if necessary, revoke a user's access privileges.

- ensuring that their RACF Coordinator implements the correct organization password policies. Under RACF, as implemented by DCRT for the North System, if a RACF Coordinator takes no action at all, no one in that user organization, or group, will ever have to change their password. Every eighty-five days users receive warning messages that their passwords will expire. If the messages are ignored, the existing password is renewed for another ninety days on the ninetieth day.

- creating their own generic or discrete profiles within RACF to protect their data sets.

Security Violation Monitoring

North System

North System users are not provided with the same security violation monitoring services that are provided for the South System. DCRT will contact RACF Coordinators via e-mail or telephone for certain security violations, but the responsibility for investigating violations remains with the designated RACF Coordinator for each North System Account. A RACF Coordinator must be designated by the user and the Coordinator is then responsible for investigating and monitoring system activity. There are five reports

that a RACF Coordinator can generate with minimal JCL. The reports include failed logon and data set access attempts (security violations) and data set deletions.

Physical Security of Output Boxes

Users that produce output listings containing sensitive or confidential data at the central facilities must ensure that their pick up and delivery procedures are appropriately controlled. While boxes are secured by locks which are controlled by a Box Access Code, there are occasions when groups of user organizations share an output box. It is the responsibility of the user organizations to protect their own output from those who do not have the Box Access Code.

Backup and Recovery

On the South MVS system, the Computer Center's data management service includes incremental backups of all FILE data sets, for recovery using WYLBUR's ENTER RESTORE command. These incremental backups can be used if a data set stored on a public disk is accidentally lost. However, since these backups exist as part of the central MVS facility's data pool, they cannot be used in the event of a disaster in the Center's machine room. Users are responsible for backing up their own designated private packs to tapes since DCRT's off-site backups are only available for disaster recovery.

No plans are currently in place to provide automatic backup of user data stored on tapes in the Center's Tape Library. Users are responsible for backing up their own data stored on tapes.

To ensure a secure backup system, users with critical data should periodically copy the data to tape and arrange for off site storage under conditions that meet their requirements.

Users are responsible for designating their applications as mission critical to DCRT in order to participate in disaster recovery exercises at the hot-site location.

The list of user control considerations presented above is not a comprehensive list of all internal control structure policies and procedures that should be employed by user organizations. Other internal control structure policies and procedures may be required at user organizations.

Section III -- INFORMATION PROVIDED BY ERNST & YOUNG LLP

TESTS OF CONTROL ENVIRONMENT ELEMENTS

In addition to the tests of operating effectiveness of specified control structure policies and procedures described below, our procedures included consideration and tests of the following relevant elements of DCRT's control environment:

- Organizational structure;
- Personnel policies and practices; and
- Management's control methods.

Such tests included inquiry of appropriate management, supervisory, and staff personnel; inspection of DCRT's documents and records; and observation of DCRT's activities and operations. The results of these tests were considered in planning the nature, timing, and extent of our tests of the specified control structure policies and procedures related to the control objectives described below.

CONTROL OBJECTIVES, RELATED POLICIES AND PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS

DCRT has specified its control objectives and has identified control policies and procedures designed to achieve those objectives. The objectives have been determined by the management of DCRT. For each control objective, DCRT control policies and procedures that are designed to achieve the stated control objectives are described.

Access to Data Files and Programs

Control Objective

Control structure policies and procedures provide reasonable assurance that the necessary computer environment and facilities exist for an application owner to appropriately restrict access to data files, programs, and other computer resources to properly authorized individuals.

Description of Policies and Procedures

South System

For the South System, DCRT provides for logical security through IBM's RACF product, the Keyword facility, the VOLSTAT procedure, CONNECT:Direct, and NIH encryption facilities. Also, DCRT provides appropriate documentation and training to facilitate the

effective use of these facilities. DCRT has a Computer Emergency Response Team (CERT) and distributes time critical computer security information to appropriate management and technical staff. DCRT prohibits the use of certain software features and facilities to preserve the integrity and dependability of the operating system. The following describes security provided by each of these facilities or security policies.

RACF

NIH Information Resource Management (IRM) policy requires its computer facilities to provide access control software to users for protection against unauthorized access and use of data. The Computer Center supports RACF to allow South System users to maintain data and access security.

Registration for Users

All individuals who desire to use the Computer Center services must obtain a DCRT account number. The appropriate Account Authorization forms are available from the Technical Assistance and Support Center (TASC). The account number is a four character combination used to access the system and for accounting purposes.

In addition to the account number, each user is registered with a unique user identifier (ID) (also known as "initials"). A set of initials is composed of three alphabetic characters with digits also permitted as the second or third characters. The DCRT Project Control Office assigns the user the three character initials. One user may be authorized to use one or more account numbers, and an account may have one or more authorized users.

The three-character initials are the RACF ID. The account is combined with the RACF ID to form a RACF group. For example, for a user with the initials III and the account AAAA, the RACF ID would be III and the RACF group would be AAAAIII and would be owned by III.

Preferred Sponsor Initials

Preferred sponsor initials are provided for account sponsors and alternates to authorize them to make changes to their accounts. These preferred initials are required for accessing WYLBUR's ENTER SPONSOR command to carry out sponsor functions. Preferred sponsor initials provide the proper authority for making changes to accounts as well as a means of receiving verification of account changes by electronic mail. Sponsors are required to complete an ENTER SPONSOR Authorization Form, available from TASC, to designate a set of initials as preferred sponsor initials.

The ENTER SPONSOR command permits sponsors and alternates to make online changes to their accounts, including:

- registering users;
- validating and invalidating initials;
- changing addresses;
- deactivating accounts;
- changing the sponsor or alternate for DCRT accounts; and
- resetting RACF passwords.

Preferred Deregistration Official (DO) Initials

DCRT has established a structure whereby the ultimate responsibility within an Institute, Center, Division (ICD) for the accuracy of computer access information belongs to the ICD senior manager/official designated as the Deregistration Official (DO) by the Executive Officer. DCRT also requires that an Alternate Deregistration Official be assigned.

Preferred DO initials are provided for deregistration officials and alternates to authorize them to perform online deregistration functions, including resetting RACF passwords when users leave the ICD. DOs are required to complete a DO Authorization Form, available from TASC, to designate a set of registered initials as DO initials.

Implementing Password Policy

Users must type in their user identifier and password to access the system. The password facility protects accounts against unauthorized access and changes. RACF passwords must be 4-8 characters long. Users may change their passwords at any time; however, the passwords must be changed at least once every six months. Users are prompted to supply new passwords when logging onto an online system if their current passwords have been in effect for six months.

The NIH Computer Center requires the account/initials at the beginning of every user's disk data set name. Each data set that is protected begins with an account/initials combination that has been registered as a RACF group.

Keyword Facility

During the review period, DCRT provided the keyword facility to automatically provide protection against the unauthorized scratching, renaming, or rewriting of data sets in WYLBUR and TSO. Users are required to have a three-character keyword for each account / initial used. New users are automatically assigned the first three characters of their RACF passwords as their keywords. The keyword can be changed at any time by the user through WYLBUR's SET KEYWORD command.

WYLBUR data sets cannot be SCRATCHed from a terminal by anyone who does not know the keyword, and specially designated private data sets cannot even be used. A specially designated private data set is a data set which requires a keyword to read it and

which is identified with an "@" in the high level prefix of the data set name. The keyword is associated with the account and initials, not the data sets. Therefore, the user must remember the current keyword, not the one in effect when the data set was created. Although there is a level of disk data set protection provided by keywords, full protection is available using RACF. Keyword protection is being phased out and is being superseded by RACF.

The keyword also protects the user's account and initials against unauthorized use by batch jobs. Keyword information must be included in every job that is run with another user's account and initials. WYLBUR and TSO prompt for keyword information from the user and supply it directly to the system. Jobs submitted directly to the system must include a /*KEYWORD control statement in the JCL.

Requests for forgotten keywords are submitted by the user or the account sponsor. Requests may be submitted via the Problem Tracking and Reporting (PTR) System, by fax transmission, or in a memo addressed to the Security Investigators of DCRT/ Enterprise Applications Support Section. The request must include the account and initials associated with the requested keyword. If this information is incorrect or incomplete, the request will be rejected and returned. When the correct information has been confirmed, the Security Investigators give the keyword to the account sponsor or designated alternate on the following business day.

VOLSTAT

The VOLSTAT facility is a batch program and is part of DCRT's Automatic Tape Inventory Control System. While VOLSTAT has many functional capabilities, users can invoke this facility to set security attributes for tapes. More specifically, the SET control statement has several operands related to access security for tapes as follows:

- The ACCESS operand limits access to tapes to designated accounts and owners. The keyword of each authorized user ID is also required so that VOLSTAT can validate the identity of the user when he tries to access the given tapes;

- The READ operand allows a tape owner to specify that the tape data cannot be modified, deleted, or added to (i.e., tape is read only). By itself, it will not limit who can read the tape, but it will prevent the tape from being written to; and

- The NO PUBLIC operand requires that a /*ACCESS statement be included in a batch job if the account and initials of the tape owner differ from those on the JOB statement of the job trying to access the tape. The /*ACCESS statement must include the properly authorized keyword to access the given tape.

CONNECT:Direct

CONNECT:Direct, a product that provides host-to-host file transfer, is required by the Department of the Treasury for online financial transactions with their systems. The function it provides is similar to that of the SENDFILE and RCVFILE programs

provided by DCRT for the same purpose, but it is easier to use and uses the Data Encryption Standard (DES) protection for file transfers.

CONNECT:Direct monitors the progress of the file transfer. This product receives full (level 1) support. Level 1 support is the highest level of service response provided for critical services supported by DCRT.

CONNECT:Direct must be installed at the remote site as well as at DCRT. Multiple CONNECT:Direct nodes are currently defined.

CONNECT:Direct requires coordination with another site as well as modifications to certain CONNECT:Direct configuration files. DCRT users may also establish a new CONNECT:Direct application for critical file transfers requiring stringent levels of encryption security by registering through the submission of a PTR.

Data Set Scrambler (DSSCM) and Data Set Unscrambler (DSUNSCM) Encryption Facilities

DCRT has programs that permit the user to scramble and unscramble the contents of a sequential data set. A scrambled data set will occupy the same amount of space as it did before it was scrambled.

The scrambling process is controlled by a code phrase which is chosen by the user. The phrase must be from eight to seventy-two characters long. The same code phrase must be used to unscramble a sequential data set. The code phrase is not permanently stored in the system.

Cataloged procedures have been provided that will scramble a specified data set by creating a new data set or by updating the data set in place. The scrambling procedures use a code phrase chosen by the user to create a seed (initial value) for a random number generator. During the scrambling process, a newly generated random number is used to scramble each character in a record.

DSSCM creates a scrambled output data set from an input data set. DSUNSCM creates an unscrambled output data set from a scrambled input data set.

North System

RACF

NIH Information Resource Management (IRM) policy requires its computer facilities to provide access control software to users for protection against unauthorized access and use of data. The Computer Center supports the use of IBM's Resource Access Control Facility (RACF) to allow North System users to maintain data and access security. RACF provides system and data protection for the North System by:

- Providing security capabilities to meet an organization's security goals;
- Logging and reporting attempts of unauthorized access;

- Identifying and verifying users; and
- Authorizing users to access data.

RACF Coordinator

RACF allows security to be administered at the organizational level. In coordination with DCRT, each participating organization or agency assigns a RACF Coordinator who implements that organization's security policies for using RACF. The coordinator assists users in recovering from forgotten passwords and grants access to data. The coordinator also reviews and resolves unauthorized access attempts, reports unresolved violations, and if necessary, revokes a user's access privileges.

DCRT enables each user organization's RACF Coordinator to perform the following:

- Implement the organization's password change policy;
- Recover from forgotten passwords;
- Revoke a user's access privilege;
- Grant special data access privileges;
- Implement project accounting;
- Implement project data set access; and
- Run reports.

Assignment of RACF User ID and Initial Password

RACF identifies an authorized user by an assigned user ID and then verifies the user ID with an appropriate password. Under RACF, only one person knows a specific user ID/ password combination. User IDs are assigned by DCRT and remain unchanged. DCRT assigns passwords, but a user must change the password during the first logon session. RACF controls access to sensitive data by authorizing users to access particular collections of data and restricts the level of data access (e.g., read or update). In addition to identifying users and controlling access to data, RACF records and reports unauthorized access attempts.

RACF Profiles

RACF maintains information on each group, user, and data set. This information is referred to as a profile and contains the data necessary to enforce security.

A group is either an organization or a subset of an organization. At DCRT, many organizations (e.g., SSA, FDA, and HRSA) have several groups. Groups are known by RACF by a three-character code referred to by DCRT as an agency account code. A user is known to RACF by a three character user ID code referred to by DCRT as the user's registered initials. All three character codes are unique.

RACF also maintains information on the relationships that exist between users and groups. This information is called a connect profile. User profiles are said to be "connected" to the group profile of their organization. A connect profile describes the relationship of a user to a group.

At DCRT, participating agencies of the North System must appoint a RACF Coordinator for each of their groups. The coordinator is made the "owner" of the group profile and all the user profiles connected to the group. It is this ownership over the profiles that gives a RACF Coordinator the authority to change the information contained in these profiles, and thereby regulate the level of security used by that group.

RACF Implementation of the North System at DCRT

RACF is used to control access to data sets on direct access volumes at DCRT. Users are registered in RACF by the users' registered initials. The RACF Coordinator assigns a RACF password when initials are assigned.

As an additional control, the user must reset the initial password for any new user because RACF forces this initial change after the creation of a new user ID. This is an important control so that only the user knows the password.

For the North System, RACF is required for TSO and WYLBUR use.

RACF security is applicable to a user's application when its databases and files are accessed via TSO, WYLBUR, or batch jobs. Therefore, a user's application source programs, Program Specification Blocks (PSBs), Data Base Definitions (DBDs), load modules, and JCL can all be protected from TSO, WYLBUR, or batch jobs with RACF security profiles. Discrete RACF profiles are automatically generated whenever a data set is created.

Implementing Password Policy

Users must type in their user identifiers and passwords to access the system. The password facility protects accounts against unauthorized access and changes. RACF passwords must be 5-8 characters long.

As originally designed by IBM, RACF enforces password changes at a selected interval for all users; everyone or no one changes passwords. Because each user organization is responsible for the security they chose to implement, DCRT developed an alternative method for the North System. This method permits each organization to decide on which individuals need to change passwords periodically and those who do not.

DCRT established the following method to permit a RACF Coordinator to selectively require password change. For every group that exists, a companion group was created whose name is the group name preceded by a pound sign (#). For example, for NMH, the group would be #NMH. By default, all user IDs that a RACF Coordinator connects to the #group are required to change the password at least once every ninety days. (A user is connected to the #group with the RACF CONNECT command which only a RACF Coordinator can perform.) The user will be warned as the expiration date approaches. If the user does not change the password before the expiration date, the user is forced to enter a new password at the first logon attempt on or after the expiration date.

Users can voluntarily change passwords whenever they wish, either at logon time with the JES /*PASSWORD statement in the JCL, or by using the RACF PASSWORD command. The password lifetime is re-initialized whenever a password is changed.

Granting Special Data Access Privileges

RACF provides group ownership of data sets where the lowest group authority allows individual users access to group-owned data sets. For the North System at DCRT, however, there is individual ownership of data sets to help provide additional security. Users must expressly "permit" other users to have access to their data sets.

However, selected individuals in some organizations may need special access to all agency data. In these cases, DCRT provides a method for the RACF Coordinator to specify to RACF that selected users may have access to all group data sets. Access may be granted at three levels: read only, read and update, and alter authority (read, update, and delete).

Implementing Project Accounting and Project Date Set Access

Project codes are three-character codes used by a group to identify sub-activities within an account that serve two purposes: one for accounting and the other for allowing common access to project data sets.

If project codes are used by the user organization, another process is available that grants access to data sets among project participants. This concept allows project members to access project data sets without needing the data set owner to execute a PERMIT command for each individual user and data set.

Running RACF Reports

There are five reports that a RACF Coordinator can generate with minimal JCL. The reports include failed logon and data set access attempts (security violations) and data set deletions. All that is required is a valid JOB and EXEC card using the RACFRPT procedure. The default parameters cause REPORT 1 to be processed that generates information on the events that occurred the previous day. The program determines the organization to generate information on by reviewing the contents of the JOB card. The available reports include:

- Report 1 All violations.
- Report 2 All violations and data set deletions.
- Report 3 Summary of all security events.
- Report 4 Summary of all security events with a summary by time of day.
- Report 5 All events sorted by user and time of day.

Tests of Operating Effectiveness

North and South System:

RACF

- Reviewed the RACF SETROPTS and DSMON reports to verify the global activation and availability of RACF as a security tool to control access to users' computer files, programs and other computer resources.

South System:

Keyword Facility

- Accessed WYLBUR and attempted to delete a sample of WYLBUR data sets without knowing the keyword and verified all attempts failed.

- Submitted a sample of batch jobs on both TSO and WYLBUR without knowing the keyword for the /* KEYWORD control statement and verified all batch jobs failed.

VOLSTAT

- Submitted a sample of TSO and WYLBUR batch jobs where the JCL had the account and initials on the JOB statement that were different from DCRT tapes where a CFB employee was the tape owner and verified all batch jobs failed.

CONNECT:Direct

- Reviewed a hardcopy of DCRT's production JCL that is used for the submission of CONNECT:Direct and reviewed a hardcopy log of the most recent job output as evidence of its use and functionality.

- Reviewed documentation from the vendor of CONNECT:Direct that certifies the product as meeting data encryption standards (DES)

DSSCM and DSUNSCM

- Submitted a sample of batch jobs accessing DSSCM and DSUNSCM and reviewed the scrambled version of an output data set that DSSCM produces and reviewed the unscrambled output data set that DSUNSCM produces and verified that the two programs operated as intended.

Results of Tests

North System:

The program control attribute (NOWHEN(PROGRAM)) in RACF for the North System was inactive. Similarly, the PROGRAM general resource class in RACF was inactive. These attributes controls access to program load modules and program access to data files. The status of these attributes indicate that RACF profiles developed for programs in the North System will have no effect.

No other exceptions were noted.

Violation Monitoring and Reporting Procedures

Control Objective

Control structure policies and procedures provide reasonable assurance that adequate security violation monitoring and reporting procedures exist to detect significant breaches of access security with the appropriate follow-up action.

Description of Policies and Procedures

South System

DCRT carefully monitors the RACF system security information and takes immediate action when it appears an attempt to breach security has occurred. When logging onto the system, if the user does not enter the correct RACF password for their user ID, the screen displays a security warning message, which is also recorded in the system logs. After three unsuccessful attempts, the system logs the user off and forces them to start the log-in procedure again. The following unsuccessful attempts are also recorded: failed access to a keyword-protected data set, failed access to a RACF-protected data set, or failed submission of a batch job. Use of the account/initials related to any security violation is suspended by the DCRT's security investigators after a daily review of the audit logs determines that a user has exceeded a pre-determined threshold of attempts.

Every night a batch job, LOGSCAN, is automatically run that extracts all records from the system logs that pertain to keywords and passwords being incorrectly specified. These extracted records are written into a RACF-protected data set and reviewed via the DAILY CP batch job (described below).

Every workday morning two programs are run. These programs are the XRACF CP (Command Procedure) and the DAILY CP. The XRACF CP automatically creates and submits batch jobs that remove from RACF any individual (RACFID) that has been discontinued. This facility ensures all authorities are completely removed from a RACFID before it is revalidated for use by another individual.

The DAILY CP submits a batch job that lists all incorrect attempts to specify passwords and keywords for the security investigator. On Mondays, Security Investigators run the DAILY CP for the past Friday, Saturday and Sunday. The DAILY job is printed in the Enterprise Applications Support Section (EASS) area and is retrieved immediately after completion due to the sensitivity of its contents. If "apparent" violations exist (i.e., the number of incorrect logon attempts exceed a pre-determined threshold within a one day period), the Security Investigators initiate a security investigation.

DCRT pursues all apparent security violations. To initiate investigations, the security investigators change the violator's password so that it cannot be specified or reset by the user or the account sponsor(s). Next, they contact the appropriate account sponsor or alternate by telephone and also send a confirming memorandum detailing the specific circumstances of the apparent security violation. The Security Investigators attach to the memo a list of attempts obtained from the daily listing and then create a Case Folder which contains documentation of the situation.

It is the responsibility of the account sponsor to investigate the apparent violation and to determine the cause of the problem. The DCRT staff works with the account sponsor as needed to develop steps to prevent future violations. The account sponsor must then return a written explanation of the violation to DCRT including what steps have been taken to avoid such violations in the future.

When the written explanation is received, the Security Investigators review the response. It is then presented to the security investigator's supervisor for acceptance or rejection. If the response is unsatisfactory, the Security Investigators call the sponsors to ask for further information and, if necessary, to request them to submit another reply.

After the supervisor's acceptance of the response, the Security Investigators reinstate the suspended account/initials and notify the account sponsors. All notes/conversations are recorded and the case is closed. A folder of the details of each case, along with all pertinent documentation, is then filed in a secure file cabinet.

Security cases are saved in a designated dataset. All security records, including all security investigations, are maintained for seven years. After seven years, these records are removed from the file and destroyed.

North System

DCRT has a different set of procedures for monitoring RACF activity on the North System. Two copies of a report called SSORACF are automatically submitted at the end of a batch billing job (DLHDAILY) which is processed at 10:00 pm each work day. One copy is routed to the print queue and given to DCRT security personnel the following morning. The second copy is retained in the held printed output queue and can be viewed online. This report reflects RACF violations for the previous work day up until 10:00 pm.

DCRT security personnel review the SSORACF report for the following:

- 10 or more log-on attempts with invalid passwords;
- Any instances where the user ID is revoked, and;
- 10 or more attempted log-ons after the user ID has been revoked.

In the instances above, an e-mail notification is sent to the user's RACF Coordinator or contacted by phone if the e-mail address is unavailable. E-mail notification to the user's RACF Coordinator includes the following information:

- User Initials
- User Name
- Occurrence Date
- Violation Code
- Number of Occurrences
- Time of Occurrences
- Action

Responsibility for investigating these violations rests with the designated RACF Coordinator for each North System Account.

A RACF Coordinator must be designated by the user and the coordinator is then responsible for monitoring system activity beyond the DCRT services described above. There are five reports that a RACF Coordinator can obtain with minimal JCL. The reports include failed logon and data set access attempts (security violations) and data set deletions. A JOB and EXEC card is required to use the RACFRPT procedure. The default parameters generate REPORT 1 as described below that it contains information on the events that occurred the previous day. The program determines the organization to generate information about by scanning the JOB card. The reports available include:

- Report 1 All violations.
- Report 2 All violations and data set deletions.
- Report 3 Summary of all security events.
- Report 4 Summary of all security events with a general summary by time of day.
- Report 5 All events sorted by user and time of day.

Tests of Operating Effectiveness

- Attempted to access a user application and verified that a security violation message appeared after each unsuccessful attempt and that access attempts were appropriately recorded in the security logs for subsequent reporting.

- Attempted to access a user application using incorrect RACF passwords three times and verified the system appropriately logs the user off, records the event in the security logs, and requires the user to re-initiate the terminal session.

- Reviewed a sample of memorandums issued by security investigators to Account Sponsors and verified the investigation actions were initiated timely.

- Reviewed a sample of Account Sponsors and memorandums from each Account Sponsor describing security violations and the written explanation for reinstatement.

- Attempted to access TSO using an incorrect RACF password and verified the attempt was recorded in the security log and the security investigator initiated investigative actions.

- Reviewed a sample of security violation case folders and verified violation information was documented and investigation actions were initiated timely.

- Reviewed a sample of daily reports and verified the time period covered by the report.

Results of Tests

No exceptions noted.

System Software Implementation and Maintenance

Control Objective

Control structure policies and procedures provide reasonable assurance that all implementation of and changes to system software should be authorized, adequately tested and implemented, and restricted to authorized personnel.

Description of Policies and Procedures

North and South System (unless otherwise specified)

There are three types of system software changes at DCRT:

- Installs of new software products;
- Maintenance -- includes fixes and upgrades; and
- Emergency Fixes.

Installs of New Software Products

The System Modification Program/Extended (SMP/E) is provided by IBM as an automated change control system for both IBM- and DCRT-supplied updates to the MVS/ESA operating system software. To ensure that SMP/E is used, DCRT makes every reasonable effort to ensure that all new IBM products for use by the end users be installed using SMP/E. Install plans are documented and followed by the DCRT/CFB/ESSS Section.

Access to system software is controlled via the establishment of RACF profiles over the libraries containing such software. Only authorized personnel have alter access to system software libraries that are related to their job responsibilities.

After the product has been initially RECEIVED through SMP/E along with the associated procedures (PROCs) and maintenance onto the MASTER VOLUME's SMP/E Consolidated Software Inventory (CSI), it is APPLIED (copied) via SMP/E to TARGET LIBRARIES on the MASTER VOLUME. The MASTER VOLUME is then copied to the TEST Logical Partition (LPAR)'s SYSRES VOLUME and testing is performed on the TEST LPAR.

Most non-database testing is performed by DCRT/CFB/EASS and DCRT/CFB/ESSS section. After EASS and/or ESSS is satisfied with the test results, they inform the appropriate personnel in the DCRT/CFB/ESSS/OSS (ESSS's Operating Systems Support Unit) are instructed to move the new system software to production systems DASD. Normally, this is performed via SMP/E controlled utilities.

For database products such as IMS, an additional step is involved after ESSS or EASS has performed initial system testing. The Data Base Support Section (DBSS) coordinates testing of the appropriate database software. Once DBSS is satisfied, they notify ESSS /OSS staff who then applies the appropriate software to the User Test Target Libraries (e.g., DB2 TEST, IMS TEST, etc.). The user database administrators (DBAs) at this time are notified and become involved in user testing of their databases. After they have completed their testing and are satisfied with the results, DBSS requests ESSS/OSS to move these newly tested and updated software products into the production environment (e.g., DB2 Prod, IMS Prod, etc.). This is accomplished via SMP/E by applying the appropriate software to the appropriate target libraries in the production environment.

All movement of system software from one library to another is recorded in the On-line System Change/Event Log. The logging software provides the following fields for logging:

- Software that was migrated;
- Libraries affected by the software installation;
- Personnel performing the maintenance;
- Description of the problem and resolution;
- Systems volume(s) affected; and
- CPU(s) affected.

The information in the on-line log is transmitted via electronic mail to the appropriate support groups within DCRT/CFB.

Maintenance (Fixes and Upgrades)

Problems with system software are initially reported to the Help Desk (TASC) or for IMS, directly to the IMS Support Staff of DCRT/CFB/DBSS. These problems can be reported via phone call or via the Problem Tracking (PTR) System. DCRT/CFB/ESSS

and appropriate systems staff diagnose the problem and work with the appropriate software vendor to obtain a software fix to resolve the problem.

The appropriate software vendor provides ESSS with the software fix that is received into the CSI Global Zone. Next, the software fix is applied to the appropriate Test LPAR Target Zone Libraries.

The new software is then tested on the Test LPAR. Depending on the product, testing is first performed by either DCRT/CFB/EASS or DCRT/CFB/ESSS. For database products such as IMS, an additional step is involved after ESSS has performed initial system testing. After EASS and ESSS are satisfied with the system test results, DBSS is notified and its personnel perform more detailed testing on the affected DBMS (e.g., IMS). Once DBSS is satisfied, it requests ESSS/OSS to apply the appropriate software, which was applied into the Test LPAR Target Zone Libraries, to the User Test Target Zone Libraries. The user DBAs as well as DCRT/CFB/DBSS become involved in user testing of the databases. After they have completed their testing and are satisfied with the results, they request ESSS/OSS to move the programs to production. Once again, this is accomplished via SMP/E by applying (copying) the appropriate software to the appropriate production target libraries.

DCRT's policy is to accept system modifications (SYSMODs) into the Distribution Zone Libraries only after applying the next SYSMOD version to the production target libraries. In this manner, DCRT always has a "fallback" version of a SYSMOD in the event that the current production running version of a given software in the target library has an unrecoverable failure.

All movement of system software from one library to another is recorded in the On-line System Change/Event log.

For upgrades and preventative maintenance, Program Update Tapes (PUTs) and Program Temporary Fixes (PTFs) are received from the various software vendors on a periodic basis. As a general policy, DCRT endeavors to be three levels behind the most current level to provide additional assurance that the vendor removed software bugs from the PUTs and PTFs. The installation of upgrades follows the same procedures as those for installing fixes.

Procedures for South System Only

DCRT has an extensive Test Job Stream (TJS) built from batch jobs acquired from the user community. All PUTs and PTFs are applied to the Test LPAR via SMP/E and the TJS is run against the newly upgraded software. DCRT/CFB/EASS compares the output to known results. Completion codes and report output are reviewed to determine if the output is still the same as before the application of the PUTs/PTFs maintenance.

Emergency Fixes

In general, users will contact DCRT via the PTR mechanism or via TASC for critical problems that require emergency fixes such as those resulting in data integrity problems. If personnel from DCRT/CFB/EASS or ESSS determine that there is a critical problem and an emergency fix is required, then the appropriate vendor support personnel are contacted. DCRT/CFB has on-site vendor support that can provide the necessary fix to the ESSS/OSS staff for immediate installation and testing.

SMP/E is still used to receive and apply the fix, just as with regular maintenance. All movement of emergency fix software from one library to another is recorded in the On-line System Change/Event log.

Tests of Operating Effectiveness

North and South System

- Reviewed a hardcopy listing of IBM system software that was maintained through SMP/E for a sample user organization and verified that MVS/ESA, TSO, and IMS were on this report.

- Reviewed a hardcopy of the system software installation template used by ESSS.

- Verified the existence of the on-line log that records the movement of system software by displaying the screens available for logging the system software information.

- Reviewed a sample of days and verified the existence of the PTR system by reviewing system software problem entries.

- Verified that the most recent vendor PUT or PTF for IMS were:

    - Received into the CSI Global Zone;
    - Applied into the appropriate test LPAR target libraries;
    - Applied into the appropriate user test version target libraries; and
    - Applied into the appropriate production target libraries.

- Reviewed an independent listing of the IBM Function Modification Identifiers (FMIDs) for MVS/ESA, TSO, CICS, IMS and DB2 as these are the IBM products which DCRT is maintaining via SMP/E and compared this list to the FMIDs identified on the DCRT SMP/E target libraries to verify these products are maintained by SMP/E.

- Reviewed the CSI data sets and verified those CSI data sets corresponded to MVS/ESA, TSO, CICS, IMS and DB2.

- Verified that the appropriate system programs are associated with the SMP/E target libraries.

- Verified that SMP/E's CSIs are in synchronization with the actual contents of the target libraries.

- Performed automated tests to determine if any maintenance of fixes were performed directly to programs without the use of SMP/E.

South System

- Reviewed a hard copy of the TJS batch job and verified that known results of the TJS batch file were maintained, and reviewed the results of the last TJS batch job that was actually processed.

Results of Tests

No exceptions noted.

Physical Security

Control Objective

Control structure policies and procedures provide reasonable assurance that physical access to the Computer Center and other sensitive areas, and operation of the computer and related processing equipment is restricted to appropriately authorized individuals.

Description of Policies and Procedures

CFB enforces physical security procedures to protect data located at the NIH computer center from access by unauthorized individuals. CFB adheres to the Privacy Act of 1974 (5 U.S.C. Section 552a) which requires federal agencies that collect information about individuals ensure that it is disclosed only to authorized individuals and agencies, that it is accurate, relevant, up-to-date, and complete, and that its security and integrity are protected.

Physical Access Control

The Computer Center is located on the NIH campus in Bethesda, Maryland. To meet its responsibilities (under the DHHS Automated Information Systems Security Program, the Privacy Act of 1974, and the Computer Security Act of 1987), and to protect the information systems and the data in its systems, the Computer Center restricts physical access to its Computer Centers and output handling areas.

Access to the Building 12 complex (Buildings 12, 12A, and 12B) is limited. A security guard is stationed at the main entrance of the complex, which is the west door to Building 12A (at the breezeway to Building 12B), 24 hours a day, seven days a week. Anyone entering the building must display a valid government ID, or register with the security guard, showing a current photo identification, to acquire a temporary visitor's badge.

NIH provides DCRT with a magnetically encoded Cardkey System to control access to the Computer Center, which is located in Building 12 of the NIH campus. All employees must use the cardkeys to gain access to the Computer Center. Entrances to all doors of the Computer Center and to building areas adjoining the machine room are controlled by card-activated locks which restrict access 24 hours a day, 7 days a week.

Visitors or non-NIH personnel entering Building 12A are required to sign-in and out. Access to the Computer Center (housed in Building 12) is restricted to properly authorized personnel. Anyone in this area must have an authorized identification badge. There are three types of badges: (1) regular entry badges are given to DCRT employees and selected individuals that have a recurring need to enter the restricted area; (2) temporary, self-expiring, fading access badges which permit short-term entry are provided for equipment installers, technicians, and visitors, and (3) escort required badges are used for personnel to be escorted by an authorized DCRT employee. The temporary, self-expiring, fading access badges for short-term entry turn red after they have expired.

All cardkey issuance, termination, and privilege changes are authorized by the Chief, System Operation and Management Section (SOMS) or his designee. The unassigned cardkeys are kept by the NIH campus security (i.e., Division of Public Safety), and once they are issued an access list is updated to reflect the personnel changes. Cardkeys belonging to terminated and transferred employees expire upon termination or transfer date. The individual's cardkey is retrieved during the exit interview. Policies and procedures have been established to review the access list twice a year to verify that all individuals on the list have a job related need to access the Computer Center.

The physical security of the computer center is directed by the Chief, SOMS. DCRT has administrative responsibilities for authorization of new cardkeys and deletion of keys belonging to departing individuals. The Crime Prevention Branch of Public Safety Division of NIH controls and maintains the cardkey system for the Computer Center.

The Chief, SOMS maintains a list of all individuals that DCRT has authorized to have cardkey access to the Computer Center. The list contains the cardkey number, the individual's name, the individual's organization, and a description of the reasons machine room access is required.

All requests for additional access (i.e., new individuals) must be made in writing or e-mail from a responsible manager to Chief, SOMS. These requests must include the individual's name, organization, and reason that Computer Center access is required.

The Administrative Office of each DCRT organization that includes individuals with Computer Center access is requested to notify the Chief, SOMS, whenever such an individual terminates or changes employment. This is facilitated via an Employee Termination form that includes a procedure that requires retrieval of carkeys.

At approximately mid-year, the DCRT Human Resource Office is requested to verify employment of those individuals with Computer Center access. A "check-off" list is provided to the Human Resources Offices by the Chief, SOMS, for this purpose. The Chief, SOMS, who then requests appropriate changes to the cardkey system for the

Computer Center access, investigates employment changes noted by the Human Resources Offices.

The Chief, SOMS, maintains a log of all changes in machine room access. This log includes the date that the change was requested from the NIH Crime Prevention Branch, the type of change requested (e.g., add access for an individual, remove access for an individual, change the spelling of an individual's name), the reason for the change (e.g., why access is required, or why it is being removed), the individual's name, and the individual organization.

DCRT has installed surveillance cameras with tape recording capabilities that monitor building access and the Computer Center from 17 different angles. CFB retains the information on the on-site tapes for one month.

Each tape used for surveillance lasts 72 hours so that there is no need to change tapes over the weekends. Currently, the Chief, SOMS, the secretary and the night shift supervisor are responsible for changing the tapes.

Mail Box and Output Management

Users may request that a secure box be assigned for output generated at the central facility. DCRT assigns each user a 7 digit access code to access the assigned output box. Output generated at the central facility is placed in locked boxes which can be accessed only by users knowing the "box access code" (BAC). If the output is too voluminous for the box, an overflow key is placed in the box. The overflow key has an identification number which corresponds to the number of the overflow box. For very large volumes of output, an overflow card, for pickup from the Output Distribution Services counter, is put in the box and must be submitted to receive the output.

DCRT Account Authorization forms are used to register for output boxes or a mailing box numbers for a remote location. To obtain an output box, a user checks the request items marked "box number" and BAC and identifies the person who should be given the BAC on the registration from. The Computer Center then sends the BAC to the designated person.

A user who forgets a BAC may request assistance from Output Distribution Services. After verifying that the user is registered to use the box, Output Distribution Services will open the box. The user is then given a form to complete, and the BAC is returned by mail. BACs are not sent to courier services, messengers, or anyone else who is not registered for the box.

Tape Management

To ensure the physical security of 9 track and cartridge tapes that are checked out of the Computer Center, DCRT requires that specific procedures be followed. To remove a tape from the library, a memorandum must be sent or brought to the Information Media Library requesting the purchase (permanent removal) of the tape. The memo must include the following:

- the volume serial number of the tape to be removed;
- the DCRT account and registered initials to be charged; and
- authorization by the sponsor of the account for the one-time removal and purchase charge.

The requested tape is stripped of NIH Computer Center identification and removed from the library registration and the user is notified when the tape is ready to be picked up. The deleted tape is then replaced in the library by a new tape with the same volume serial number. If the user wishes to return the deleted tape for processing at some future date, it must be handled as a special tape. The tape cannot be re-entered into the library unless it is copied to another tape identified to the library.

To remove a tape temporarily from the Information Media Library, the individual receiving the tapes must provide the following information in the Magnetic Media Log for the Production Unit staff:

- serial number of volume;
- name of person removing volume;
- government ID or driver's license of the person removing volume;
- date and time;
- signature;
- agency or company name; and
- telephone number and name of person to whom the volume is assigned and their account and initials.

This information is confirmed by a DCRT staff member who also records the tape's temporary location and scheduled return date.

DCRT's automated tape management system is also simultaneously updated with this information. If the tape is not returned to the library, any jobs that require access to the tapes are rejected by the tape management database. Periodically, DCRT performs a reconciliation between the magnetic media log, DCRT's tape management system, and the tape library.

Tests of Operating Effectiveness

- Reviewed physical security procedures for appropriateness.

- Reviewed a sample of individuals with access to the Computer Center and determined whether access was appropriate based on the individual's job

responsibilities and also verified that appropriate, written management authorization existed prior to giving each individual access to the Computer Center.

- Reviewed the total number of individuals with access to the Computer Center to ensure that there is not an excessive number.

- Reviewed who has custody/ownership/physical control over the card readers which guard the entrances to the Computer Center for propriety.

- Observed that the card key system was in operation, individuals without a Computer Center cardkey were escorted and that they were logged entering and exiting the Computer Center.

- Reviewed a sample of cardkey issuance, termination, and privilege changes performed and the audit trail for proper authorization.

- Conducted a physical inspection of the Computer Center as well as the building.

- Verified that the entire building was controlled by the cardkey system and monitored by 24 hour guard service and closed circuit TV.

- Reviewed DCRT's Magnetic Media Log for the following information: name (signature), ID badge number, driver's license number and state, company name, company phone number, and serial number of the tape and verified its presence.

- Reviewed a sample of Security Video Tape logs and verified the date and time of tape exchanges and that the tapes were properly secured.

Results of Tests

We noted the following exceptions during our review:

- The Computer Center has glass windows on two sides of the room on the ground level. The alarms and security detection facilities for the windows were not activated with an audible alarm as of September 30, 1997.

- Two of the 28 individuals sampled were not authorized for access to Computer Center.

- DCRT does not have custody, ownership, or physical control over the card key readers controlling access to the Computer Center. The NIH Safety Division/Crime Prevention Branch controls all card readers on campus. Active ongoing monitoring and immediate deletion of individuals from the Computer Center are not possible without ownership or partial ownership over the card readers which control the entrances to the Computer Center.

No other exceptions were noted.

Section IV – OTHER INFORMATION PROVIDED BY THE NATIONAL INSTITUTES OF HEALTH, DIVISION OF COMPUTER RESEARCH AND TECHNOLOGY

Year 2000

DCRT has a plan for addressing the Year 2000. DCRT has identified the operating systems and utilities that are their responsibility and Year 2000 ready, and those that must be updated in the future. DCRT has coordinated with the vendors for the current (Year 2000 ready) version of the operating systems and utilities and installed these in a functional test region. This test region allows agencies, centers, institutes, departments or divisions (ICD's) to test their applications.

The responsibility to test the applications remains with the controlling (owning) ICD. DCRT cannot mandate that each ICD test their respective applications. Additionally, an awareness campaign has been initiated and various formal communications have been distributed in NIH publications.

Federal Financial Management Improvement Act of 1996 (FFMIA)

In accordance with the Memorandum for Chief Financial Officers and Inspector Generals at CFOs Act Agencies, dated September 9, 1997, which was issued by the Office of Management and Budget and gives guidance on compliance with the FFMIA 31 U.S.C. 3512, applications being executed at DCRT are considered Federal financial management systems. Accordingly, DCRT is responsible for substantial compliance with Section 1 regarding Federal financial management systems requirements.