DEPARTMENT OF INFORMATION TECHNOLOGY

RICHMOND, VIRGINIA

SERVICE ORGANIZATION REVIEW

REPORT ON POLICIES AND PROCEDURES PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS AS OF MARCH 31, 2001

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

EXECUTIVE SUMMARY

This report reviews the Department of Information Technology's (DIT) policies and procedures placed in operation as of March 31, 2001. We conducted our review using Statement on Auditing Standards (SAS) No. 70, "Service Organizations," as amended by SAS No. 88, "Service Organizations and Reporting on Consistency," and the considerations in SAS No. 78 – Appendix B, "Amendment to Reports on the Processing of Transactions by Service Organizations," issued by the American Institute of Certified Public Accountants. We have defined the control objectives for this review from the Information Systems Audit and Control Foundation's work on Control Objectives for Information and Related Technology (COBIT). COBIT provides generally applicable and accepted standards for good practices for information technology control.

This report should provide DIT's user agencies, their internal auditors, and report users with sufficient information about DIT's internal control policies and procedures. This report assesses the operating effectiveness of policies and procedures surrounding automated transactions processed or other services provided by DIT.

This report, when combined with an understanding of the user agency's internal control policies and procedures, is intended to assist auditors in planning the user agency's audit and assessing control risk for assertions in the user agency's financial statements that may be affected by policies and procedures at DIT. We have included a discussion of user agency control considerations to facilitate this analysis. If user agencies do not have effective controls, DIT's control policies and procedures may not compensate for such weaknesses.

We found:

> DIT's policies and procedures, as reported in Section II, are suitably designed and operating effectively to provide reasonable assurance that the DIT has achieved the specified control objectives as of March 31, 2001. The reader should evaluate this information only with a concurrent assessment of the user agency's internal control.

We recommend that DIT:

- Perform reviews of firewall trusted-relationships
- Perform quarterly reviews of Data Center access
- Develop policies and procedures for maintaining security controls on the UNIX Sun E10000
- Develop policies and procedures for terminated contractors
- Implement the ACF2 password history feature in the MVS environment

TABLE OF CONTENTS

I. DEPARTMENT OF INFORMATION TECHNOLOGY DESCRIPTION OF CONTROLS

Overview Of Services Provided

The Department of Information Technology (DIT) provides state and local governments with a source for meeting their information technology needs. DIT manages the state's telecommunications contracts; provides state government with data processing services; assists state agencies and local governments with designing and purchasing information technology resources; and provides other information technology services, such as audio and video conferencing. Data processing services offered through the Data Center support MVS, UNYSIS, UNIX, and Windows NT operating environments.

Control Environment Elements

ORGANIZATION

Effective February 1, 2001, Scott Fairholm began serving as DIT's Director and oversees DIT's two directorates: Finance and Administration, and Services. The Finance and Administration Directorate organizes, manages, and provides internally the financial, human resources, information systems, technology resources, and acquisition services necessary to support the Services Directorate. The Services Directorate coordinates and supplies information technology resources to state and local governmental entities within the Commonwealth. As this directorate directly impacts user agencies, below is a description of its divisions.

During calendar year 2000, a realignment of the Services Directorate occurred to streamline its divisions. Despite these changes, senior management remained stable over the past five years. Leslie Carter continues to serve as the Deputy Director for the Services Directorate, which is composed of the following divisions:

- **Integrated Telecommunications Services** manages and coordinates the Commonwealth's local and long distance voice services, data communications, wireless services, and broadband and network equipment. The Division also maintains information on all telecommunication services requested and used by state agencies, contracts for the services with carriers throughout the Commonwealth, and collects payments from state agencies for remittance to the carriers.

- **System Software** provides database, operating, and system software support services for DIT operated computing platforms including MVS, UNISYS, UNIX, and Windows NT. In addition, the Division supports automated operations, storage management, and enterprise management for multiple operating systems.

- **Computer Operations** is responsible for the operation of the Data Center providing general utility and data management software products and services to support batch processing, on-line processing, and remote job entry in the MVS and UNYSIS mainframe environments. Further, the Division provides facility and data management support for user agency UNIX and Windows NT servers.

- **Enterprise Solutions** performs PC and network services to support local and wide area networks by assisting with the planning, implementation, and support of network and client/server environments. The Division also provides services for custom software and database development, and assistance in developing information technology and telecommunication-related procurement requests. Finally, this Division offers services to develop, maintain, and enhance custom applications and e-commerce solutions.

- **Security** is responsible for the logical and physical access to DIT's resources, including the Data Center, provides training and assistance to customer agency security officers, and manages security services available to agencies. In addition, the Division assists the Council on Technology Services in the establishment of statewide security plans, programs, and policies.

- **Acquisition Services** purchases equipment and services for the Services Directorate Divisions. The Finance and Administration Directorate performs all other procurement functions.

- **Network Internet/Intranet** provides Transfer Control Protocol/Internet Protocol (TCP/IP) network connectivity and network support services.

- **Partnership** provides customers with a point of contact to communicate their day-to-day assistance requirements and planned service delivery requirements. The Division has three branches: Customer Assistance, Communications and Publications, and Customer Service.

PERSONNEL POLICIES AND PROCEDURES

DIT has personnel policies and procedures for all DIT employees maintained on DIT's intranet. New hires must attend an orientation class that covers these policies and procedures and includes security awareness as a topic. Each employee must sign the DIT security agreement, which includes password integrity and non-disclosure of sensitive information. Employees must wear identification badges at all times and are expect to challenge anyone not wearing a badge or who is unfamiliar to them.

New employees generally receive on-the-job training upon hiring. Existing employees attend periodic technical or other training as necessitated by their job function. DIT has job descriptions for each position and follows all policies and procedures issued by the Virginia Department of Human Resource Management regarding discipline and periodic appraisal of performance.

Termination and voluntary exit procedures include exit interviews. Termination and exit notices go to the Human Resources Division who notifies the necessary divisions of an employee's exit.

RISK ASSESSMENT

Management conducts risk assessments at least every two years or as major system changes occur to determine whether measures exist to counteract threats to assets under DIT's control. To aid in this process, DIT uses a risk assessment software package called RiskWatch.

DIT's risk assessment procedures include: identifying the likelihood a threat will occur, investigating the factors that could affect the threat occurrence rate, determining the vulnerabilities of service areas to potential threats, estimating the loss potential of a service area, and developing proactive countermeasures to reduce business loss.

MONITORING

Management receives daily, weekly, and monthly reports to monitor the operational performance. These reports provide information on logical and physical access information. DIT also uses software applications to monitor operating system performance, track help desk incident tickets, and manage system backup process and offsite storage.

QUALITY ASSURANCE

Division managers maintain controls and determine when they need new controls.

COMMUNICATIONS

DIT documents and maintains operating policies and procedures covering Service Directorate functions and security activities on their intranet. Management reviews these policies and procedures at least annually and updates them when necessary to address new and changing technology. Employees receive information about security issues as needed through e-mails.

Communications with user agencies occur through multiple mediums, including phone, e-mail, and the Internet depending on the issues. DIT's website has an "alert" page providing customers up-to-date system status information, as well as a "news" page notifying customers of major trends, issues, and upcoming changes.

II. INFORMATION PROVIDED BY THE SERVICE AUDITOR, THE AUDITOR OF PUBLIC ACCOUNTS

Objectives of the Review

This report provides user agencies with information sufficient to obtain an understanding of those aspects of the Department of Information Technology's (DIT) controls over the Data Center that may affect the user agency's internal controls. This report, when combined with an understanding of the user agency's internal controls, should assist auditors in planning the user agency's audit and in assessing control risk for assertions in the user agency's financial statements that policies and procedures at DIT could affect.

Our examination was restricted to selected user agency processes administered by DIT and accordingly, did not extend to procedures in effect at the user agency's organization. The examination was conducted in accordance with the Statement on Auditing Standards (SAS) No. 70, "Service Organizations," as amended by SAS No. 88, "Service Organizations and Reporting on Consistency," and the considerations in SAS No. 78 – Appendix B, "Amendment to Reports on the Processing of Transactions by Service Organizations" of the American Institute of Certified Public Accountants.

We used the Information Systems Audit and Control Foundation's work on Control Objectives for Information and Related Technology (COBIT) to help define the control objectives for this review. COBIT was developed as a generally applicable and accepted standard for good practices for information technology control. Our examination included the inquiry of appropriate management, supervisory, and staff personnel; inspection of documents and records; and observation of activities and processes surrounding DIT's operations.

The description of control activities and control objectives is the responsibility of DIT's management. The Auditor of Public Accounts' responsibility is to express an opinion as to whether controls are operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, as specified by DIT's management, were achieved during the period covered by our report.

It is the responsibility of each interested party to evaluate this information in relation to their internal controls and assess the related control risk. User agency and DIT portions of internal control must be evaluated together. If user agencies do not have effective internal controls, DIT's controls may not compensate for such weaknesses.

Tests of the Control Environment

An organization's internal control represents the collective effect of various components in establishing, enhancing, or mitigating the effectiveness of specific controls. In addition to tests of specific controls described below, our procedures included tests of, or consideration of, the relevant components of DIT's control environment including:

- the control environment, which reflects the tone of the organization and its approach to internal control;

- the organization's risk assessment process for identifying, analyzing, and managing the risks to the achievement of its objectives;

- the control activities, which are the policies and procedures that help ensure that management directives are carried out;

- the methods for the identification and communication of information; and

- the monitoring of the quality of internal control performance over time.

Our tests of the control environment included the following procedures to the extent we considered necessary: (a) a review of DIT's organizational structure, including management controls, the segregation of functional responsibilities, policy statements, processing manuals, human resource policies; (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) a review of actions taken by DIT in response to recommendations to improve controls.

The Auditor of Public Accounts considered the control environment in determining the nature, timing, and extent of tests performed in order to obtain evidence of the operating effectiveness of the control activities in meeting specified control objectives.

Tests of Operating Effectiveness of Specific Controls

Our examination of the operating effectiveness of certain controls of DIT was restricted to the objectives and related controls determined by the Auditor of Public Accounts and included below and was not extended to procedures in effect at user agency locations or other controls that may be described in Section III, but not listed in below.

Our tests of the effectiveness of controls included such tests as we considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified objectives were achieved during the period from April 1, 2000 to March 31, 2001. In selecting particular tests of the operating effectiveness of controls, we considered: (a) the nature of the items being tested; (b) the types and competence of evidence available; (c) the nature of the objectives to be achieved; and (d) the expected efficiency and effectiveness of the test.

The procedures used to test the operating effectiveness are organized by control objective and listed below the description of controls. The results of the tests are described following the test procedures and represent testing as of March 31, 2001.

OPERATING SYSTEM CONTROLS

Control Objective 1

Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing system software and implementation of new systems

Description of Controls

DIT has established and documented standard procedures for the installation, modification, and/or removal of operating system software, which provide an adequate audit trail. The policy states common steps to follow in the installation, modification, or removal of system software. These steps are Receipt, Create Change Management Documentation, Analysis, Approval, Project Plan, Schedule/Coordination, Test Plan and Test Implementation, Back-out Plan, Production Implementation, Post Implementation Evaluation, and Closure. During emergencies, the staff abbreviate the procedures described below and complete the documentation after the emergency.

The following divisions under the Systems Software Division make changes in existing operating system software and new system software:

Divisions for the MVS Environment:

- Data Communications
- MVS Database
- MVS System Software Support

Divisions for UNISYS and UNIX Environments:

- UNISYS/UNIX Database
- UNISYS Systems Software Support

The Chief Engineer or designee coordinates the analysis of the new product, version, maintenance, or removal of the operating system software.

The Process

All changes to existing software and the implementation of new software involve the creation of a change management record in the Change Management System. Staff discuss all change request forms during the weekly Change Management Review meeting. System software changes require approval at the analysis, testing, and implementation phases.

The Chief Engineer ensures the completion of the approval process by either accepting or rejecting the system software change. The Chief Engineer may escalate approval authorization to the Project Leader level for any change that does not have unanimous approval. Where circumstances warrant, the Project Leader may escalate approval to the Division Director.

During testing of software change implementation, the Chief Engineer takes precautions to protect the production libraries/systems files from loss or destruction. The Chief Engineer must review and determine if the plan adequately and thoroughly tests the change and documents the results. The engineering staff for the affected system communicates all problems or unexpected results to the Chief Engineer.

Before production implementation, the Chief Engineer documents the back-out plan. This plan allows staff to restore the system to its former production state should the implementation of the change fail. All impacted divisions review the back-out plan and after final implementation, perform an assessment of the impact of the change, review the adequacy of the project and test plan, and provide input from lessons learned.

After successful production implementation, the Chief Engineer resolves any problems or unexpected results and is responsible for closing the project.

Tests of Operating Effectiveness

- Reviewed existing system software change procedures and evaluated whether they comply with management's specifications. Documented any change control tracking software currently in use.

- Determined whether DIT was up to date with new versions and patches for each operating environment.

- For a selection of system software changes from each operating environment, identified the initiating request. Determined if DIT personnel properly authorized, tested, documented, and approved changes and they only moved authorized programs back into production.

Test Results and Conclusion

No exceptions noted. Based on the tests of operating effectiveness, the controls are operating with sufficient effectiveness to achieve this control objective.

PHYSICAL ACCESS CONTROLS

Control Objective 2

Policies and procedures provide reasonable assurance that physical access to computer equipment, storage media, and documentation is limited to properly authorized personnel

Description of Controls

Policies and procedures for physical access involve all DIT divisions and computing envir onments. The DIT Physical Security Section of the Security Division administers and maintains the physical security program.

New and Current Employees

The Personnel Department notifies the Physical Security Section of a new employee's starting date. The hiring division generates and forwards an access authorization form to the Physical Security Officer. The hiring division manager determines the employee's access, considering his job classification/function.

The physical security officer assigns an access card, picture ID number, and the appropriate clearance codes and forwards the access form to the security manager for approval. Employees must sign to acknowledge receipt of their access card and ID badge.

The physical security officer maintains access card information on the Security Tracking System and keeps unassigned access cards in a locked file cabinet. An inactivated access card cannot open any doors until the physical security officer record the cards on the Tracking System and assigns specific access points. The access card reader at each locked door reads the access card and only unlocks it if the Tracking System acknowledges authorization for access to the locked area.

All DIT employees visibly display picture ID badges at all times and report any lost, missing, or stolen picture ID badges or access cards immediately to the Physical Security Section. If the discovery occurs after normal business hours, the employee contacts the Capital Police so they can take the proper steps to remove the card from the security system. Employees obtain a visitor's badge from the appropriate reception area or the security station if they forget their picture ID or access card.

DIT employees do not allow unescorted visitors or vendors to follow behind them when entering a door requiring the use of an access card. With the exception of those individuals using the DIT auditorium or classrooms, DIT requires that visitors have escorts at all times while in areas requiring access cards unless the visitor has an access card. Employees must report any unidentified or unauthorized person to the Capitol Police or the DIT Physical Security Section.

The Division of Capitol Police enforces access control through continuous manning of the security station and observing all video monitors. After normal business hours, a capitol police officer makes a periodic walk-through check of all DIT areas including all corridors and fire exits. Capitol Police respond immediately to panic alarms and treat every alarm as an emergency. They notify key personnel if emergencies occur and make decisions for evacuating the building.

Effective July 2000, the physical security officer will review quarterly the Data Center access for individuals who have access to, but infrequently enter the Data Center. Users are subject to having their access rights to the Data Center removed based on this review.

Terminated, Transferred, or Promoted Employees

When a supervisor learns of an employee's termination, the supervisor immediately provides the Personnel Department with a memorandum notifying them of the termination. The Personnel Department immediately notifies the Security Division who provides the supervisor with a separation checklist. The checklist serves to guide the supervisor in collecting all items related to physical access.

For those employees terminating under abnormal circumstances (i.e., firing or death), the supervisor contacts Security immediately to remove physical access to DIT premises. The supervisor attempts to collect, at a minimum, the employee's ID card, door keys, and access card.

For transferred and promoted employees, Personnel notifies Security of the change in status by providing them with a Payroll Transaction/Authorization Form. Security works with both the present and former supervisors to modify the employee's physical access to meet the needs of the new position.

User Agency Control Considerations

Physical access to terminals, routers, and other equipment located at the user agency organization, which connect to DIT, should be limited to authorized individuals and be environmentally controlled and monitored.

Tests of Operating Effectiveness

- Toured Data Center to determine the existence of physical security over critical hardware and if proper precautions exist against environmental hazards such as loss of power, fire, water damage, and heat.

- Reviewed who has authorization to enter the Data Center and for a selection of employees and contractors determined whether their access was reasonable.

- Determined whether management periodically re-evaluates access privileges for users having Data Center access privileges so that infrequent users may have their access removed. For a selection of users with access, determined their frequency of entering the Data Center.

- For a selection of terminated employees and contractors determined whether DIT removed access to it facilities in a timely manner.

Test Results and Conclusion

Three of the twenty-five employees reviewed had not accessed the Data Center during the six-month period reviewed, and two employees accessed the Data Center ten times or less during this same period. Management had not changed these individuals' access rights to the Data Center nor reviewed their access activity due to the length of the Data Center access reports. This is in direct conflict with DIT's policies and procedures and prevents the timely identification and removal of unnecessary or inappropriate access. The auditor informed management of this finding.

No other exceptions noted. Based on the tests of operating effectiveness, the controls are operating with sufficient effectiveness to achieve this control objective.

LOGICAL ACCESS CONTROLS

Control Objective 3

Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data

Description of Controls

The Security Division has responsibility for managing logical access to programs and data. Their policies and procedures cover the computing environments of MVS, UNISYS, and UNIX, and access through firewalls.

All DIT Computing Environments

DIT has established a program to ensure the confidentiality, availability, and integrity of the data DIT owns or for which it serves as custodian. The program follows the Commonwealth of Virginia Information Technology Resource Management Standard SEC2000-01. When user agencies request access to DIT systems, DIT follows the procedures below.

Logical Access to Programs

When user agencies request access, they receive access to all programs in either the MVS or UNISYS systems by default. In the MVS system, ACF2 provides security to all programs, except some specific IMS databases, and users must prepare specific rules to allow user access to programs.

In the UNISYS system, user agencies must take security measures to ensure that another user agency cannot access their data contained within a program. DIT provides three types of security for protecting user agency data in the UNISYS system: (1) Read-Write Access; (2) Access Control Records (ACR); and (3) Compartments, for protecting user agency data. DIT recommends, but cannot mandate that user agencies use these security features. If a user agency does not use one of the security options, then other UNISYS users have free access to the computer programs and data.

Logical Access to Data

MVS Computing Environment for DIT Employees and User Agencies

Each user agency (including DIT) must appoint an Agency Security Officer, who establishes, maintains, updates, and deletes access for user agency end-users. The user agency must complete a form for each individual user and the Agency Security Officer, DIT Security Officer, System Coordinator, and Direct Access Storage Device Coordinator must sign the form indicating approval. DIT's Security Division keeps a copy of the approved form and performs the following procedures after receiving the approved form:

- Verifies the Agency Security Officer signature.
- Verifies that the logon ID is seven alphanumeric characters and that the first three characters are the agency qualifier.
- Lists the logon ID's to make sure that ACF2 returns the message that the logon ID does not exist. If the logon ID does exist, the Agency Security Officer is contacted.

UNISYS Computing Environment for User Agencies

Each user agency must select a UNISYS sub-administrator and send a letter to DIT indicating the sub-administrator's name to have the appropriate security features established. DIT does not set up access for any of the user agency's employees except the sub-administrator. The individual user agency implements procedures for setting up end-user logon ID's and privileges.

UNISYS Computing Environment for DIT Employees

All DIT end-users must fill out a UNISYS logon ID request form, get the proper authorization, and submit it to the Security Division when requesting access. DIT-designated personnel receive all special requests with written justification, the signature of the end-user, and the end-user's supervisor before setting up the logon ID in accordance with the request.

UNIX Computing Environment for DIT Employees and User Agencies

The Department of Social Services (DSS) owns the E10000, which is located at and administered by DIT. End-users at DSS must fill out an internal DSS form in order to obtain access to the E10000. A database analyst at DSS contacts DIT via e-mail to request access for an end-user in accordance with the form. DSS users are given access only to those applications that they need and not blanket access to the E10000.

Other UNIX-based equipment housed at DIT on behalf of agencies do not rely on DIT logical access controls. These servers are located at DIT for physical security, environmental controls, and logistics reasons, but are administered by the owning agency.

Logical Access to Programs and Data through DIT Firewalls

The security firewall is a combination of hardware (SUN SPARC workstations) and software (CISCO PIX, Raptor Systems, Incorporated) designed to provide a security barrier by blocking external networks from accessing DIT's computer environment, which includes the MVS and UNISYS systems.

The Agency Security Officer requests access to the DIT firewall by contacting the DIT Help Desk and completing and signing a Firewall Access IBM or Firewall Access UNISYS form. The DIT Firewall Administrator establishes a user logon ID and password. This password does not expire and users do not have the capacity to change their password.

In addition to requesting access, the Agency Security Officer can request additional firewall services such as monitoring the system, changing passwords, and using TRACEROUTES that identify external traffic trying to access the network. DIT has established procedures for each of these additional services.

User Agency Control Considerations

Procedures for logical access from the user agency to resources located at DIT must be established, maintained, and monitored. This includes appropriate procedures for authorizing who can access user applications and at what level, and controlling who can modify user access.

Agencies are responsible for whom they give access, including DIT personnel. The appropriateness of agency employee access, other than DIT personnel, was not reviewed during this audit.

Tests of Operating Effectiveness

MVS Environment

- Determined whether system settings are reasonable for parameters such as password length and maximum password attempts allowed.

- For a selection of logon ids, verified that access by DIT personnel is restricted only to authorized individuals.

- For a selection of terminated DIT employees, verified that logon IDs were deleted in a timely manner.

- Evaluated for reasonableness, based on job function, those DIT employees having one or more of the following privileges: Account, Security, Audit, Consult, and Leader.

- Determined whether the rules for access to system programs were appropriate by reviewing rules for the ADABAS, IMS, and DB2 environments.

- Determined whether the ACF2 rules files were restricted to security personnel at DIT.

- Determined through inquiry and observation which security reports are run and whether they are fully utilized.

- Reviewed access and control over Control-M scheduling software to determine that user agency programs would run automatically as scheduled.

UNISYS Environment

- For a selection of Unisys Sub-Administrator request forms, determined whether they were properly completed and accompanied by a request letter from the user agency's authorized designee, before DIT granted access.

- Determined the appropriateness of those DIT personnel that have DIT SIMAN administrator sign-on, which allows for adding, deleting, or changing agencies' sub-administrator capabilities.

- For a selection of user agencies, obtained confirmation of their awareness that UNISYS access security is their responsibility.

- Determined whether access to the scheduler functions was reasonable so that user agency programs run automatically, as desired.

UNIX Environment

- Determined whether the UNIX operating system and files have been properly configured by performing the following:

  - Reviewed the /etc/passwd file to determine only one account in the /etc/passwd file has a UID of "0," a shadow password file is used with all accounts passworded or disabled, and application users are given a shell with a UNIX prompt.

  - Determined how many users know the superuser password.

  - Determined that only the owner has write permission to system files such as /Bin and /Dev.

  - Determined that the initab and crontab files reside in protected directories.

  - Determined that all trusted services are turned off in files such as /etc/host.equiv.

  - Determined that the only world writable directories are /spool/temp.

  - Determined whether vendor-supplied security patches have been applied.

  - Determined that superusers do not log on as root but instead SU (Switch User) to the root account or have a root capable account with their ID.

- Determined whether the permissions are appropriate for the application programs and data files.

- Determined through inquiry and observation which security reports are run and evaluated how often they are reviewed.

Firewalls

- Reviewed the firewall application program and determined its function within the network and what services and users it controls.

- Determined whether the UNIX operating system and files have been configured properly on the firewall by performing the following:

  - Determined whether any other applications such as compliers, application programs, or Web Services are resident on the server through review of the root directory listing.

  - Determined that only root and one admin account exist along with a shadow password file.

  - Determined that only the owner had write permission to system files such as /Bin and /Dev.

  - Determined that network services are commented out of the /etc/inetd.conf file.

  - Determined that the initab and crontab files reside in protected directories.

  - Determined that all trusted services are turned off in files such as /etc/host.equiv.

  - Determined that the only world-writable directories are /spool/temp.

  - Determined that vendor-supplied security patches have been applied.

  - Determined that superusers do not log on as root, but instead SU (Switch User) to the root account or have a root capable account with their ID.

- For a selection of users, verified they were properly authorized to access the firewall.

- Determined through inquiry and observation, what reports are generated from the firewall and evaluated how often they are reviewed.

Test Results and Conclusion

MVS Environment

The password history feature of ACF2 is not activated in the MVS environment even though the forced change of password feature is implemented. This configuration allows the same password to be reused repeatedly when a user is prompted to change his password every 30 days. This issue has been communicated to management.

No other exceptions noted.

UNISYS Environment

No exceptions noted.

UNIX Environment

There are no written policies and procedures for maintaining security controls in the UNIX environment. This issue has been communicated to management. A review of this environment based on industry recommended standards was completed. No other exceptions noted.

All Environments

DIT does not have policies and procedures addressing the prompt removal of logical access for terminated contractors. Existing polices and procedures apply to terminated DIT employees alone. This issue has been communicated to management.

Firewalls

Four agencies (Departments of Transportation, General Services, Social Services, and Health), as well as the agencies that go through these agencies' firewalls to reach DIT, are exempt from authenticating at the DIT firewall. DIT does not perform security reviews of these trusted agency firewalls to ensure adequate security (Repeat Finding). This issue has been communicated to management. DIT has developed a draft policy, dated

January 1, 2001, to address this concern; however, as of the date of fieldwork, it has not been formally implemented.

No other exceptions noted.

Based on the test of operating effectiveness, the controls are operating with sufficient effectiveness to achieve this control objective.

BACKUP CONTROLS

Control Objective 4

Policies and procedures provide reasonable assurance that backups are performed and stored off-site

Description of Controls

The Computer Operations Division performs backups of the MVS, UNISYS, and UNIX environments, including all shared disk packs. It is the user agency's responsibility to perform backups of all dedicated disk packs and to inform DIT of the data files and application programs to store offsite.

MVS, UNISYS, and UNIX Backups

DIT backs up all data files and application programs that reside on shared disk packs nightly (Sunday through Friday, except holidays) at midnight. DIT uses Control-M to automatically perform the nightly backups at midnight for all MVS operating system files, any sub-systems, and program products. There is also a weekly backup of all dedicated IMS and ADABAS database files. SAM Control provides the same automatic backup for UNISYS systems.

For UNIX systems DIT procured and is currently installing an Enterprise Backup and Recovery System that will use Veritas software and DLT7000 tape drives housed in an automated tape library. Further, DIT is reviewing technology for backing up this data to direct access storage devices.

The DIT scheduling group enters the backup, offsite storage, and retention time requests made by user agencies and in-house divisions into an automated system. DIT maintains the latest disk file backup tapes at the Data Center for on-request file restoration. As part of DIT's disaster recovery plan, the offsite storage facility retains the two previous backup tapes.

Offsite Storage

For offsite storage, DIT contracts with Argus, who sends a courier to pick up new and return old tapes. Monthly, DIT personnel go to the offsite storage location and perform an inventory of the tapes. If there is a discrepancy, DIT personnel determine its cause.

DIT uses a robotics tape library to manage the MVS tapes. The "robots" pull the tapes for offsite storage and MVS librarians scan the tapes to ensure the shipment of the correct tapes. A bar code helps DIT employees perform the same function for UNISYS and UNIX tapes.

User Agency Control Considerations

User agencies need to communicate to DIT which tapes created by user applications are critical and need to be stored offsite. This information is usually not resident on hard drives and therefore, not automatically backed up and stored offsite.

Tests of Operating Effectiveness

- Determined whether the offsite tape storage vendor, which had no test work exceptions last year, has changed or moved.
- Determined through inquiry of the Manager of Data Center, the appropriateness and completeness of the hardware support agreement for failed backup equipment.
- Determined whether adequate procedures are in place to maintain effective backup in the case of tape drive or primary medium failure through inquiry and observation of the annual disaster recovery test.

Test Results and Conclusion

No exceptions were noted. Based on the tests of operating effectiveness, the controls are operating with sufficient effectiveness to achieve this control objective.

TELECOMMUNICATION CONTROLS

Control Objective 5

Policies and procedures provide reasonable assurance that data completeness and security occurs for data transmissions/communications between DIT and its user agencies

Description of Controls

DIT provides several modes of communications such as dial-up, dedicated lines, and a telecommunications network. Our focus for this objective is the COVANET, which is used as the backbone carrier by a user agency for their private network.

The user agency contacts DIT to establish the proper connections and can use frame relay, PVC (Point Virtual Circuit), or a telephone line on the COVANET to send data. DIT contracts with various communication companies to provide telecommunication service. These companies, such as MCI, Bell Atlantic, and Sprint own and control the physical lines from the user agency to DIT. DIT takes no security responsibility for these lines.

DIT has one main router, which is used to control and direct traffic from the COVANET frame relay environment and Network Virginia. Internet traffic passes through the Network Virginia gateway router before it reaches DIT. The network security division at Virginia Polytechnic Institute is responsible for configuring the security controls on the Network Virginia gateway router. DIT's router is configured to allow traffic coming in from the Internet to only access DIT's web page and the DNS server that provides various state agency home page information.

Users that need to access the mainframe systems at DIT through COVANET and Network Virginia are included on an access list that is defined in the router table configuration. The access list is a security feature programmed into the router using Internet Protocol (IP) addresses. Only user agencies using the specified IP address can gain access through the router. Though these users are allowed to pass through the router, they also have to be authenticated through the firewall before they can access the MVS, UNISYS, and UNIX mainframe systems.

User agencies must formally request access to the DIT firewall (see further explanation at the LOGICAL ACCESS Control Objective). Upon user agency request, DIT will establish or configure routers physically located at the user agency. These requests are handled through the Help Desk where the ticket is initiated to complete the work.

User Agency Control Considerations

User agencies need to communicate to DIT the criticalness and level of sensitivity of connections from the user to DIT, so that DIT may provide controls and services as needed.

Logical and physical access to telecommunication equipment and routers residing at the user agency that link the user to DIT are the user agency's responsibility to control.

Firewalls at DIT protect the MVS, UNISYS, and UNIX systems and the DIT local area network located at the DIT data center. These firewalls do not provide security for user agency internal networks. User agencies have responsibility for the proper control of those networks.

Tests of Operating Effectiveness

- Documented the communication and network environment that connects agencies to DIT.

- Determined how DIT provides incoming and outgoing Internet services for other agencies and evaluated whether the DIT firewall protects agencies from any Internet-based threats and is secure.

- Evaluated the extent of cooperation between DIT and an agency in regards to configuring the necessary communication lines and equipment (modem, routers) and determined whether the level of cooperation provides a secure method of communications implementation.

- Reviewed the router table and determined whether: (1) source and destination IP addresses are valid, (2) filtering rules are reasonable, (3) Internet traffic originating outside of DIT is routed to a secure web page or through the firewall, (4) the router is using the two-level password option so that the router table itself is secure, and (5) a deny statement exists for packets received with a source address of an internal network address.

- For a selection of problem tickets, documented instances of line downtime and how DIT and COVANET handled such an event and determined if there are any tickets that were not resolved within a 24-hour period.

- Reviewed and evaluated the methods that agency employees use to dial in from laptops or home PCs and its security.

Test Results and Conclusion

No exceptions noted. Based on the tests of operating effectiveness the controls are operating with sufficient effectiveness to achieve this control objective.

CONFORMANCE TO SEC2000-01.1

Control Objective 6

Policies and procedures provide reasonable assurance that the Department of Information Technology conforms to SEC2000-01.1 as it relates to the following areas:

- Business Impact Analysis
- Risk Management
- Contingency Management Plan
- Security Safeguards
- Security Awareness/Training Programming

Description of Controls

DIT's Security Division promotes information security awareness; provides security technical assistance to divisions; implements and administers security programs and procedures; performs risk analyses; investigates alleged security breaches; develops, maintains, and disseminates a contingency management plan; and trains users on proper methods of securing technology resources. Until October 2000, Council on Information Management Standard 95-1 guided DIT on the minimum requirements to maintaining an information security program. In October, the Council, now the Department of Technology Planning, issued an updated standard entitled, "Information Technology Security SEC2000-01.1."

Business Impact Analysis

DIT completed a business impact analysis following CIM Standard 95-1 in April 1999, but has not updated its analysis for the new standard, since it has not added any new systems.

The business impact analysis only covers systems that affect DIT's operating areas, not user agency applications. To develop this analysis, the Security Division sent a questionnaire to each DIT Division Director and Project Leader requesting that they identify their systems containing critical or confidential information and the resulting impact if the system was not operational for a period of time. The Security Division compiled the information into the Business Impact Analysis, which the DIT Director reviewed and approved.

When DIT adds new systems, management intends to repeat the same process, incorporating the results into the existing overall business impact analysis.

Risk Assessment

Staff conduct risk assessments at least every two years or as major system changes occur to determine whether measures exist to counteract threats to assets under DIT's control. To aid in this process, DIT uses a risk assessment software package called RiskWatch.

DIT's risk assessment procedures include: identifying the likelihood a threat will occur, investigating the factors that could affect the threat occurrence rate, determining the vulnerabilities of service areas to potential threat, estimating the loss potential of a service area, and developing proactive countermeasures to reduce business loss.

Contingency Management Plan

The critical divisions at DIT have a contingency management plan, which DIT's contingency plan administrator maintains and manages centrally. Each critical division has a disaster recovery coordinator, who supports the contingency plan administrator by updating their division's portion of the plan.

The disaster recovery coordinators review their divisional action plans quarterly to determine the status of the information and identify pages that require corrections. After correcting the pages, the coordinator sends them to the contingency plan administrator. If there are no changes, the coordinator e-mails the contingency plan administrator stating that there are no changes.

DIT has a contract with SunGard to provide "hot sites" for the restoration of the MVS, UNISYS, and UNIX systems in the Data Center. Philadelphia, Pennsylvania is the hot site for the MVS and UNIX (E10000), and Warminster, Pennsylvania is the UNISYS hot site. DIT tests these hot sites regularly to verify that the system and data can be restored.

Annually, the contingency plan administrator requests from user agencies a list of critical applications processed by DIT and uses this information for capacity planning at the hot sites. The contingency plan administrator also maintains a list of current processing requirements for the alternate processing sites as a part of the divisional action plans. When the divisional action plans change, the DIT Configuration Review Committee communicates any plan changes to SunGard.

Security Awareness/Training Program

The Personnel Department and the Security Division require new employees to read DIT Directive 92-1, "System Access Control" and sign an information security access agreement. This agreement details the proper use of employee access to DIT systems. If the new employee will have Internet access, they must sign an Internet use form.

DIT does not have any formal procedures for security awareness training for existing employees. However, each year at the end of November, the Security Division sponsors a Computer Security Day. DIT places a notification in each employee's pay envelope with the training date and displays posters in the building. Closer to the security day, employees receive an e-mail as final notification. During Computer Security Day, employees attend a formal program and receive a packet of information on security awareness.

User Agency Control Considerations

User agency policies and procedures should provide reasonable assurance that they also conform to SEC2000-01.1. The development of these policies and procedures should consider DIT's relationship to the user agency and the services DIT provides.

Some agencies have begun to use DIT's data center as a site to house their various servers. With the exception of the E10000, these servers are administered by each respective agency and are not included in DIT's contingency plans. DIT, however, is willing to work with each agency to determine if DIT can provide contingency services through either SunGard or other means such as offsite-mirrored servers. Each agency needs to be sure that these servers fall under a contingency plan. If an agreement has not been made with DIT, the agency needs to have backup routines and fallback plans in case of a disaster in the data center.

Tests of Operating Effectiveness

- Obtained latest version of the business impact analysis and determined if it was complete.

- Reviewed RiskWatch software and determined whether a formal risk assessment has been done within the last two years.

- Determined whether DIT's contingency plans were reasonable and properly updated.

- Evaluated the amount of time needed to restore user agency operations, the percentage of user applications that can be brought online, and the impact of the process on state agencies based on the documented contingency plan.

- Determined whether the disaster recovery/hot site scenario has been tested for all environments.

- Determined whether DIT security personnel have taken courses in the last year on security-related topics.

- Verified whether a selection of recently hired DIT employees signed a DIT security agreement.

- Determined whether DIT employees receive regular security awareness training.

- Reviewed contract modifications between DIT and SunGard to determine that SunGard has been kept abreast of critical changes to the contingency requirements.

Test Results and Conclusion

No exceptions were noted. Based on the tests of operating effectiveness, the controls are operating with sufficient effectiveness to achieve this control objective.

III. SUMMARY OF CURRENT YEAR AND RESOLUTION OF PRIOR YEAR FINDINGS

Summary of Current Year Findings

Enforce Policy to Review Data Center Access

The Physical Security Officer does not monitor access to the Data Center area quarterly, as DIT's policy requires. Currently, no one performs these reviews due to the size and level of detail of the access list reports.

Failure to enforce this policy increases the risks associated with unnecessary access to the area. With unnecessary access, an employee could physically destroy equipment or make unauthorized changes to hardware and software. This scenario also increases the possibility of theft. DIT should improve the reporting mechanism used to monitor employee access to ensure the required reviews occur quarterly and remove access from individuals who demonstrate they do not need it.

The Enterprise Services Division is currently working with the Physical Security Branch to create a more user-friendly Data Center access list report for review.

Develop Policies and Procedures for Maintaining Security Controls on the UNIX Sun E10000

There are no written policies and procedures for maintaining security controls on the UNIX Sun E10000. Failure to implement proper policies and procedures could lead to improper controls placed on the system and allow for unauthorized access, placing the integrity and completeness of the data stored on the system at risk.

The agency should develop policies and procedures for security of the UNIX Sun E10000 as soon as possible to provide direction on what controls management deems necessary and what restrictions to impose for the system. The policies and procedures would allow the agency to continue to function in the same manner in the event of employee transfer or terminatio n.

The overall policy should address, at a minimum, the following specifications:

- User security (passwords controls, file protections, unattended terminal procedures, etc.)
- Establishment of new accounts
- Group assignment/unassignment
- Procedures to be followed for superusers
- Requirements for granting users root access capability
- Implementation of a shadow password file
- Implementation of security patches
- Removal of IP services not required for standard operations of the system
- Control of world writable directories and files
- Active review of security logs for unusual activity
- Procedures to be followed if security is compromised or threatened

Develop Policies and Procedures for Terminated Contractors

DIT does not have policies and procedures for terminated contractors. Existing polices and procedures for terminated employees apply to DIT employees alone.

The auditor's attempts to identify the policies and procedures, as well as to locate supporting documentation revealed that all divisions do not have the same understanding as to who has responsibility for this information. The auditor first attempted to obtain a list of terminated contractors from Human Resources and found that it does not handle terminated contractors. The auditor then questioned the individual service directorates. One division stated that they give the information on terminated contractors to Human Resources. Another division stated they handle the terminated contractors for their division. It is unclear what are the procedures for the contractors who the agency terminates.

Policies and procedures serve as a guideline for providing proper controls over daily agency operation and help eliminate unauthorized logical and physical access. DIT should develop policies and procedures for terminated contractors as soon as possible.

Implement ACF2 Password History Feature

DIT has not activated the password history feature of ACF2 in the MVS environment even though DIT has implemented the forced change of password feature. This configuration allows the reuse of the same password repeatedly when a user has to change his password every 30 days. This procedure increases the chance of unauthorized change to software and data in the MVS environment, if someone gains unauthorized access to a password the user never changes.

There are new theories that implementing forced password changes and password history features on automated systems lead to users writing down passwords, which compromise these features. Therefore, these theories suggest it is better to have a strong initial password that is hard to break and not changed than to have a series of weak passwords.

However, since DIT cannot verify the strength of user passwords, DIT should use the forced change of password and password history features in tandem. Staff should set "PSWD History" in ACF2 to require a minimum of six password changes before allowing the reuse of a password.

Resolution of Prior Year Findings

DIT has not taken adequate corrective action on the previously reported finding listed below. DIT corrected all other previously reported findings and therefore, we do not include them in this report.

Perform Review of Firewall Trusted Relationships

DIT does not perform security reviews of trusted agency firewalls to ensure adequate security. Four agencies have firewalls that have a trusted relationship with the DIT firewall. DIT's firewall does not authenticate these agencies before connecting to the MVS or UNISYS environments. Inadequate review of these trusted relationships could jeopardize the integrity of valuable information resources. In addition, DIT does not have a policy establishing the criteria for exemption from authentication and what procedures the agency must follow to maintain this exemption.

DIT has made progress toward implementing an exemption policy; however, the policy remains uncompleted. Therefore, we again make this recommendation. We further recommend that management finalize and approve this policy as soon as possible.

Considerations for Agencies Impacted by these Findings

The following reflect user agency considerations relating to each recommendation addressed in the above sections:

- Data Center access presents risks to all user agencies. While there are concerns over the number of personnel with access rights to the Data Center, as well as the procedures in place to monitor this access, we have found no evidence of any compromise of security. Compensating controls such as armed guards, surveillance cameras, and picture ID badges are present.

- Until management develops and implements UNIX security policies and procedures policies and procedures, audits of DSS should consider a higher level of risk being associated with the E10000 environment.

- Contractor access presents risks to all user agencies. While we have issues with the lack of procedures for terminated contractors, we found no evidence that unauthorized logical or physical access has occurred for a terminated contractor.

- Implementation of the password history in ACF2 environment will prevent MVS users from using the same password repeatedly for a certain period of time. The non-use of this feature presents low risk to the following agencies: Virginia Employment Commission, Department of Accounts, and Department of Motor Vehicles.

- Trusted relationships exist with some agencies that pass through other Commonwealth-controlled firewalls prior to connecting to DIT. Users from these agencies are exempt from the additional DIT firewall authentication procedures required of other agencies. While we have issue with the lack of standards for these exemptions, the exempt agencies are still required to log into the mainframe using the conventional ACF2 security routine in order to access programs and databases. This concern presents some risk to all user agencies.

IV. ADDITIONAL CONTROLS OVER THE DATA CENTER AND OTHER SERVICE AREAS

Additional controls exist over information technology services provided by DIT. While we did not evaluate these controls during the current audit, we are providing them for informational purposes. We express no opinion on the policies and procedures included in this section.

Hardware Change Control

DIT has a policy to provide the framework for the implementation and tracking of all changes involving the data center. A change is any alteration and testing to any component of the data center's hardware, software, procedures, scheduling processes, application configuration changes, movement of databases between systems, or any documentation needs. The Computer Operations Division performs changes to the MVS, UNISYS, and UNIX hardware in the data center and the Integrated Telecommunications Services Division performs the changes for the PC Desk Top Video and PictureTel Videoconferencing hardware.

The software support engineer, facility engineer operations, and operations analysts submit a change request form to their manager/supervisor for approval through e-mail. Once the manager approves the change request form, he sends it to the Operations Analyst Section (MVS, UNISYS, or UNIX) for review. The operations analyst then distributes the change request form to the appropriate personnel for review, addresses questions or concerns, and informs the requester of the time and date for the change. The customer bulletin distributed to all user agencies includes all changes.

Emergency changes require immediate implementation to resolve mainframe software or hardware system outages. After the change and restoration of the system to normal operation, the manager or supervisor documents the action taken on a change request form marked "emergency." The operations analyst will review the changes and give the emergency change request form to the operations supervisor.

Monitoring of System Performance

The Capacity Planning Branch of the Business and Technology Planning Division, in the Finance and Administration Directorate, does capacity planning for the MVS, UNISYS, and UNIX environments, as well as COVANET. The Capacity Planning Branch prepares a capacity planning report each month, which contains recommendations for procurement planning based on the performance/capacity measures. Division managers meet monthly to review the capacity planning report. Performance and capacity monitoring procedures specific to each operating environment are discussed below.

MVS Performance/Capacity Monitoring Procedures

MVS has many subsystems including MVS, VTAM, IMS, DB2, CICS, and SMS. DIT uses a product called OMEGAVIEW to monitor performance and to alert them of any issues that may impair continued processing. DIT subsystem engineers identify potential subsystem problems by using components of OMEGAVIEW called Omegaview 1 and Omegamon. Omegaview 1 alerts the engineer to the problem, while Omegamon allows the engineer to view the problem at the subsystem level, providing for a more detailed investigation.

UNISYS Performance/Capacity Monitoring Procedures

DIT monitors the lines connecting to the UNISYS system, as well as the system itself. A software package called PRISM monitors and reports the transaction traffic on the UNISYS lines. DIT provides PRISM line summary reports to customers who request it, such as the Departments of Motor Vehicles, Social Services, and Taxation, and the Virginia Employment Commission. DIT will eventually replace this software because it cannot monitor newer technologies like TCP/IP.

TORCH Performance Management System software collects and downloads UNISYS system data to VIEWPOINT software, which constantly analyzes and displays statistics about the UNISYS system. When VIEWPOINT encounters a problem, it flashes a red signal, produces an audible alarm, and alerts a UNISYS Systems Engineer on their PC. If a problem occurs, the UNISYS operator notifies the help desk or UNISYS systems engineer to take corrective action.

UNIX E10000 Performance/Capacity Monitoring Procedures

DIT, under a facilities management agreement, monitors the Department of Social Services' UNIX E10000. DIT has written UNIX scripts that automatically collect central processing unit (CPU) utilization and input/output (I/O) service time. A separate application uses this information to produce daily plots of hourly utilization and peak and average I/O service times, which DIT posts on the intranet for review by the capacity planning manager. For trending analysis, DIT also maintains a historical database of the above information.

COVANET Performance/Capacity Monitoring Procedures

WorldCom has contractual responsibility for COVANET network capacity planning and for proactively monitoring the network. Under this contract, WorldCom must provide DIT and customer agencies reports of frame relay, ATM circuits, and PVC utilization. DIT reviews these reports to monitor agreed-upon communication service levels. DIT also runs a report independent of WorldCom, which reports utilization of circuits connecting directly to DIT.

Backup and Offsite Storage of Tapes

The following reflect environment specific backup procedures not included under "Backup Controls" in Section II:

PC and LAN Backups

DIT employees regularly backup data on their individual PC hard drives. If the employee created critical data files, he is responsible for storing the backup copy off-site for purposes of disaster recovery. The DIT LAN administrator backs up data files stored on network directories nightly.

Software Development Backup

The software development branch of the Enterprise Solutions Division copies and stores offsite all systems and documents for software development customers, internal management, and administration. Offsite storage includes all software development purchased software tools and packages, and one copy of the Management and Control System (MACS) microfiche files. Every Friday night, there is an automatic backup of the software development LAN project directory in addition to an automatic incremental tape backup that runs Monday through Thursday nights. Software development can use the last incremental tape and the

Friday night backup tape for reconstruction of files. All backup tapes are stored in the DIT/MIS fireproof safe.

The Help Desk

The Help Desk in the Computer Operations Division identifies, records, tracks, and engages the appropriate resources to resolve customer and DIT system problems 24 hours a day, seven days a week. DIT uses an Automatic Call Distribution (ACD) software package that tracks the calls to Help Desk personnel. The ACD system can track and report on calls answered or disconnected before answering and the wait times for calls. Management runs and reviews these reports daily.

Help Desk personnel log all problem calls into the IBM Info/Sys Problem Management database maintained in the MVS environment. Info/Sys records problems as tickets, automatically assigns a ticket number, and tracks the call. The Problem Management Guidelines and Procedures Manual outlines procedures for creating, escalating, reviewing, dispatching, checking status, and closing tickets. Management reviews and discusses tickets open more than two weeks in the Info/Sys at a weekly meeting.

When Info/Sys is not operating, Help Desk personnel manually record calls on a Problem Entry Reporter form, but does not assign a problem number. Once the system comes back up, personnel enter the manual ticket for logging and number assignment and then call the customer with the ticket number.

Physical Security over LAN and PC Environments

LAN administrators place file servers, related equipment such as gateways and wiring components, and original copies of LAN software in an environmentally safe and physically secure area. The card access computer system alerts Capitol Police to investigate if the equipment room door remains open.

DIT employees lock (where possible) and terminate power to their PCs when leaving the premises. Also, users store magnetic media (i.e. diskettes, tapes) away from extreme temperatures and sunlight. Employees protect diskettes containing sensitive or confidential data by locking them in a secure place and advise the Software Development Security Officer of the nature of the data and its secure location. Employees do not store sensitive or confidential data/information on any PC hard disks. All employees are encouraged to challenge anyone moving about the building that they do not recognize.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

May 24, 2001

The Honorable James S. Gilmore, III
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable Vincent F. Callahan, Jr.
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

INDEPENDENT SERVICE AUDITOR'S REPORT

We have examined the accompanying description of the **Department of Information Technology's** (the Department) policies and procedures set forth in Section II of the accompanying report applicable to the automated data processing of transactions and other related services for the Commonwealth of Virginia. Our examination included procedures to obtain reasonable assurance about whether: (1) the accompanying description presents fairly, in all material respects, the aspects of the Department's policies and procedures that may be relevant to the internal control of an organization (the Customer) using these services; (2) the control policies and procedures included in the description were suitably designed to achieve the control objectives specified in the description, if these policies and procedures were complied with satisfactorily; and (3) such policies and procedures had been placed in operation as of March 31, 2001. The accompanying description includes only those policies and procedures and related control objectives of the Department and does not include policies and procedures and related control objectives of any third party vendor. Our examination did not extend to policies and procedures of third party vendors. The control objectives were specified by the Auditor of Public Accounts. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary under the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned policies and procedures presents fairly, in all material respects, the relevant aspects of the Department's policies and procedures that have been placed in operation as of March 31, 2001. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specified policies and procedures, included in Section II of this report, to obtain evidence about their effectiveness in meeting the control objectives described in Section II as of March 31, 2001. The specified policies and procedures and the nature, timing, extent, and results of the tests are listed in Section II. This information is available to user organizations of DIT and to their auditors to be taken into consideration, along with information about the internal control risk for user organizations, when making assessments of control risk for user organizations. In our opinion, the policies and procedures that were tested, as described in Section II, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section II were achieved during the period from April 1, 2000 to March 31, 2001.

The description of policies and procedures at the Department is as of March 31, 2001, and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the policies and procedures in existence. The potential effectiveness of specific policies and procedures at the Department 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 description of specific policies and procedures at the Department, as set forth in Section II, and their effect on assessments of control risk at customer organizations are dependent on their interaction with the policies, procedures, and other factors present at individual customer organizations. We have performed no procedures to evaluate the effectiveness of policies and procedures at individual customer organizations.

The information included in Section III of this report is presented by the Department of Information Technology to provide additional information to user agencies. The information in Section III has not been subjected to the procedures applied in the examination of the control objectives listed in Section II, and accordingly, we express no opinion on it.

This report is intended solely for use by management of the Department of Information Technology, its customers, and the independent auditors of its customers and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

JBS/kva
kva:44