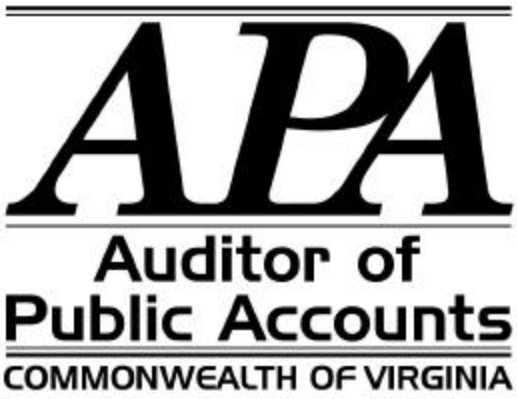
DEPARTMENT OF INFORMATION TECHNOLOGY

RICHMOND, VIRGINIA

SERVICE ORGANIZATION REVIEW

REPORT ON POLICIES AND PROCEDURES PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS AS OF MARCH 31, 2000



EXECUTIVE SUMMARY

This report reviews the Department of Information Technology's (DIT) policies and procedures placed in operation as of March 31, 2000. We conducted our review using **Statement on Auditing Standards No. 70, 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 was developed as a generally applicable and accepted standard for good practices for information technology control.

This report should provide DIT customers, 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 customer's internal control policies and procedures, is intended to assist auditors in planning the customer's audit and in assessing control risk for assertions in customer's financial statements that may be affected by policies and procedures at DIT. If customers 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 III, are suitably designed and operating effectively to provide reasonable assurance that the specified control objectives have been achieved as of March 31, 2000. The reader should evaluate this information only with a concurrent assessment of the customer's internal control.

We recommend that DIT:

- Perform reviews of firewall trusted-relationships.
- Limit data center access.
- Require vendor notification of employee terminations.
- Maintain proper controls for LAN security access.
- Review agency Unisys sub-administrator accounts.
- Review current policies and procedures periodically.

-T A B L E OF C O N T E N T S -

Section I. FINDINGS SUMMARY

Perform a Review of Trusted Relationships

DIT does not perform security reviews of trusted agency firewalls to ensure adequate security. A trusted firewall relationship is a protocol that establishes access between networks or outside entities without requiring special verification. Four agencies have firewalls that have a trusted relationship with the DIT firewall. These agencies can directly connect to the MVS or Unisys environments without authentication. Inadequate review of these trusted relationships could jeopardize the integrity of valuable information resources. In addition, DIT does have a policy establishing why some agencies are exempt from authentication and what procedures the agency must follow to maintain its exemption. We recommend that DIT develop a policy that establishes exemption requirements, procedures that agencies must follow, and require periodic security reviews.

Limit Data Center Access

Individual managers request physical access to the data center for their employees; however, they do not have any written guidelines to follow when requesting this access. While data center management annually reviews the listing of employees with data center access, they do not have specific policies on which to determine an employee's need for data center access. DIT is developing policies and procedures for limiting access to the data center. We recommend that managers regularly review the listing of employees with data center access and remove all access for all employees whose job functions do not require them to enter the data center. Limiting physical access to employees who only have the need reduces the risk of theft and vandalism.

Require Vendor Notification of Employee Terminations

DIT has given several vendors physical access to the data center. Physical security depends upon the vendor telling DIT when their employees terminate. Further, DIT does not have a policy to obtain information about vendor employee terminations. DIT is developing policies and procedures to limit data center access and require vendor notification of employee terminations. Implementation of these procedures would help to limit DIT's risk of disgruntled vendor employees returning to the Data Center after termination and causing damage to the Data Center.

Maintain Proper Controls for LAN Security Access

Local area network users can have a total of ten failed logon attempts before the system locks their account. This setting is excessive and presents a security weakness that exposes the local network to brute force attacks and unauthorized account usage. We recommend that DIT review its policies and procedures for local area network logons and reduce the number of failed logon attempts to a more appropriate number, preferably between three and five. Reducing the number of failed logon attempts will minimize the risk assumed by DIT to brute force password attacks.

Review Agency UNISYS Sub Administrator Accounts

Our review of agency sub administrators for the UNISYS mainframe found an account unused since 1991. This indicates that agency security officers have not consistently or thoroughly reviewed the agency sub administrator accounts. DIT policies do not address the periodic review of these accounts. We

recommend that DIT include in its policy procedures the periodic review of Unisys sub administrator user accounts. This policy should include specific standards detailing the frequency and methods of the review, to include reconciliation between the agencies with applications running on the UNISYS mainframe and the agencies that have an agency sub administrator account. Ensuring that only properly authorized, active agency sub administrator accounts exist on the UNISYS mainframe will enhance the level of security available to all agencies who have applications or data on this platform.

Subsequent to our review the Department of Information Technologies deleted the inactive agency sub administrator account with the permission of the agency security officer.

Review Current Policies and Procedures Periodically

DIT's policies and procedures are complex and must cover numerous areas, technologies and personnel. Keeping complex policies and procedures current and making sure that their content covers operations requires a systemic approach to their review and change. This review found several areas where the current policies and procedures do not address DIT's changing environment.

We believe a scheduled systemic review of policies and procedures would assist DIT management in adopting and addressing these changes. Additionally, this approach would allow personnel to adopt a phased approach to the review and still have the flexibility to address emergencies. We therefore recommend that DIT develop a schedule to review and update its policies and procedures.

Section II. OVERVIEW OF SERVICES PROVIDED

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 agencies and local governments with designing and purchasing information technology resources; and provides information technology solutions, such as audio and video conferencing.

DIT has two directorates: Finance and Administration, and Services. Finance and Administration organizes, manages, and provides internally the financial, human resources, information systems, technology resources, and acquisition services support. Services coordinates and supplies information technology resources to governmental entities located throughout the Commonwealth. Services' divisions are described below.

MVS Database Division

The MVS Database Division provides database support services for customers. The Division uses the Department's two Hitachi GX-8824 mainframes to provide support for ADABAS, DB2, and IMS database management systems and related products.

MVS Systems Software Support Division

The **Operating Systems Software Section** manages the MVS operating system program products and related software for security, report writing, programming languages, and data sorting that customers require for their daily production. Some of these products include ACF2, FOCUS, SYNCSORT, EASYTRIEVE, COBOL II, and FORTRAN G1. This section also modifies the MVS software definitions to match changes in the hardware configuration for central processing units; disk allocation storage devices, tape, and other systems related hardware.

The **Teleprocessing Software Section** supports teleprocessing software products such as TCP/IP, VTAM, NCP, and CICS, which is the on-line monitor for several database products.

Both sections have responsibility for acquisition, installation, availability, maintenance, performance, problem and change management, disaster recovery, and evaluation of their software as well as system configuration management.

Unisys Systems Software Support Division

The **Operating Systems Software/Program Products Section** manages the operating system and its components, media storage, interactive processing, performance monitoring software, utility processors, and language processors such as COBOL. This section also provides software configuration to match the existing hardware platform.

The **Teleprocessing Software Section** supports all teleprocessing software that runs in the four front-end processors and the host based software that provides data communications. Further, the section supports software associated with the router-based network coming into the data center, as well as the software configurations for their customers' remote based routers.

Unisys/UNIX Database Division

The Unisys/UNIX Database Division provides database support services for customers using the Unisys 2200/9844 mainframe for MAPPER and DMS 1100. The Division also provides UNIX system administration, Internet service, domain name service, e-mail service, and news feed service. The Division also services the Department of Social Services' SUN E10000 by providing Oracle Database Management and MAPPER support.

Computer Operations Division

The **Systems Operations Branch** provides a customer service support center to assist customers with service requests and resolutions to processing problems. They also communicate with customers on job status and production problems, as well as provide production support services such as coordination, delivery, and protection of physical security. Finally, this branch operates the computer systems, consoles, peripheral devices, printers, and the mounting and dismounting of tapes.

The **Technical Support Branch** coordinates vendor installation and maintenance of data processing hardware, performs data center environmental and equipment facilities management, as well as provides internal data communications and systems hardware support services. This branch also develops procurement documents for hardware and software.

Telecommunications Division

The Telecommunication Division administers local and long distance telephone and data communications services for State government. The Division competitively obtains most services from telecommunications vendors.

Information Engineering Division

The Information Engineering Division provides technology and database planning, data administration, desktop systems and local area network planning and implementation. They offer Internet services, including Internet access and server space for sites, as well as Internet web page consulting and marketing support services.

Automated Systems Division

The Automated Systems Division provides for the implementation and operation of automated operations software and storage management. They are responsible for all IBM DASD space allocations and the software implementation of various storage devices. The division is also responsible for the evaluation, acquisition, availability, maintenance, performance, and disaster recovery of software as well as providing technical assistance to clients and problem, change, and system configuration management.

The Automated Systems Division interfaces with DIT's Capacity Planning Group to relay current and projected DASD requirements based upon customer requests. They develop regular performance management reports to assist the Capacity Planning Group in their responsibilities.

Telemedia Division

The Telemedia Division provides audio and video teleconferencing services, and coordinates this service statewide. Additionally, the Division provides consultation and management services on video networks, capacity, and equipment.

Systems Development Division

The Systems Development Division provides personal computer local area network support, development, and procurement; assists the computer services division with the installation and configuration of software; develops applications; and provides support to the Governor's Office for it's local area network and system operation.

Security Division

The Security Division provides centralized physical and data security for all DIT's programs and oversees facilities management.

Technology Consulting Division

The Technology Consulting Division provides network planning, design, training, and implementation assistance for Local and Wide Area Networks, micro to mainframe communications, Client/Server Technology, and Personal Computers.

Section III. CONTROL OBJECTIVES, POLICIES AND PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS

The Auditor of Public Accounts determined the nature, timing, and extent of tests performed in order to obtain evidence to the operating effectiveness of the Department of Information Technology policies and procedures in meeting specified control objectives. The procedures used to test the operating effectiveness are listed next to the respective control objective and policies and procedures in the following matrix. The results of each test are listed next to the test procedures.

The following matrix represents testing as of March 31, 2000.

Objective 1: Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing application systems and new systems under development.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Systems Development Division (SDD) has responsibility for changes to existing and new application systems. SDD has established system maintenance standards to provide optimum service, ensure responsive systems, and manage SDD's resources. Other DIT divisions do not maintain application systems. SDD provides assistance to DIT customers for all phases of application development and maintenance. The computing environment that SDD uses to develop application systems depends on the needs of the client. SDD may use the existing hardware/software at DIT or the client's computing environment.		In response to prior year test work and finding that SDD lacked a policy and procedures to document application development, DIT created a new policy effective February 15, 1999.
New Systems Development SDD has established and defined standard phases and tasks within the division to enhance project management of systems development/modification projects and special projects, monitor operations, maintenance, and administrative activities. SDD requires Project Agreement forms for all projects. A Project Leader does a preliminary project plan. SDD procedures require a pre-project review if the analysis to determine the project's scope and objectives finds that the project requires more than 500 man-hours. If the project might exceed 1000 hours, the SDD Deputy Director attends the review. Additionally, DIT's Internal Auditor must provide written recommendation to proceed for all projects in excess of $100,000. After the SDD Director's approval, the customer receives the Project Agreement for signature and SDD opens the project in the Management and Control System (MACS). The MACS system tracks project assignments, project tasks and subtasks, estimated hours, and calendar start and completion dates. The system reflects the employee's worked hours charged and the status of the various project tasks. The system also tracks standard project task activity phases such as the project initiation phase, requirement definition phase, systems	**New Systems Development** Evaluate and document any project design tracking software that may currently be in use. Obtain a list, from the System Development Division, of new application programs that have been implemented in the last year. From this list, judgmentally choose a sample of mainframe and client server programs for testing. Determine if development of new applications is made in accordance with proper project management standards, and that the development process is authorized and documented.	**New Systems Development** Audit testing of new systems development after implementation of this policy was not performed as there were no projects on-going or completed during the audit period.

Objective 1: Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing application systems and new systems under development.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
analysis phase, detail design phase, development phase, implementation, and evaluation. After project approval, the Project Manager assigns the project to a Project Leader and informs the Project Leader of any responsibilities and expectations. The Project Leader and Project Manager then meet with the assigned project team and review their duties and responsibilities. The Project Leader conducts a monthly one on one review with the Division Director. The Project Leader documents the review agenda and results in a Project Status Report. SDD structures the review so that one member of the project team acts as a reporter. SDD documents any changes from the initial project agreement in a Modification Agreement.		
Changes to Existing Application Systems Application system customers communicate any changes for application system maintenance in writing to the SDD Project Leader. The Project Leader assigns the work to an analyst who prepares the requirements. Each Project Leader will be responsible for obtaining approval for all production changes ensuring that all changes are documented, tested, and reviewed by an individual other than the one making the change. During normal work hours, a programmer makes the change, tests the change, and signs off on the completion of all changes. Someone then reviews the change other than the programmer. The program is moved into production and the Project Leader makes sure all the documentation requirements documented in the above paragraph have been met. After normal work hours, the programmer on call receives all requests concerning critical emergency production problems. The programmer will fix the problem and move the changed program into production. The programmer must complete an "Operational	**Changes to Existing Application Systems** Evaluate and document any change control tracking software that may currently be in use. Obtain a list of application programs, from the System Development Division, of application programs that have been changed in the last year. From this list, judgmentally choose a sample of mainframe and client-server programs for testing. Determine if changes to existing applications are made in accordance with management's specifications, properly authorized, properly tested, documented, approved and that only authorized programs are moved into production.	**Changes to Existing Application Systems** Audit testing of changes to existing application systems after implementation of the new policy cited above revealed no major weaknesses. However, it was noted that due to SDD's organizational structure programmers have access to production data. As there were only six system changes during the audit period, and policies expressly forbid moving changes into production without proper documentation, except for critical production issues occuring after normal business hours, a recommendation has not been issued. User agencies should monitor program movements into and out of production to ensure

Objective 1: Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occur for changes to existing application systems and new systems under development.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
System Maintenance Activity" form, which includes listing the problem, action taken, individuals involved, time required and the name of the customer who notified the programmer of the problem. The programmer must sign the form and have it signed by either the Project Manager or the Information Technology Manager who verifies the appropriateness of actions taken. For all systems that DIT supports completely, assigned DIT personnel have constant access. The user organization is responsible for authorizing DIT personnel access to their system because DIT is not allowed to act as the security officer for any user organization application system. For systems that DIT supports only occasionally, they must request access from the user organization each time they have a service request. Upon completion of each request, DIT's access is deleted. Programmers have access to the test and production programs for only those application systems that they work on or test. Although there are some situations where programmers have the capability to move changes into production, policies expressly forbid them moving changes into production without appropriate documentation except for when critical production problems occur after normal business hours. The library shows the date the last 8 changes to any program occurred.		that all movements are authorized.

Objective 2: Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occurs for changes to existing operating system software and implementation of new systems.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The following divisions make changes in existing operating system software and new system software: Divisions with MVS Environment: Automated Systems Division MVS Database MVS System Software Support Divisions with Unisys and UNIX Environment: Unisys/UNIX Database Unisys Systems Software Support 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 procedures described below may be abbreviated and documentation completed after the emergency. The Chief Engineer or designee coordinates the analysis of the new product, version, maintenance, or removal of the operating system software. 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.	Evaluate and document any change control tracking software that may currently be in use. Obtain a list of existing system software changes from the MVS Systems Support Section, the UNISYS/UNIX Database Division, the UNISYS Systems Software and Data Communications Division. From this list, judgmentally select four changes from each division and trace back to the initiating request. Evaluating whether existing system software change procedures are in accordance with management's specifications. Determine whether changes are properly authorized, tested, documented, and approved and that only authorized programs are moved back into production.	No exceptions were noted.

Objective 2: Policies and procedures provide reasonable assurance that proper authorization, testing, approval, implementation, and documentation occurs for changes to existing operating system software and implementation of new systems.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
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. Back out plans will allow the 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 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.		

Objective 3: Policies and procedures provide reasonable assurance to limit physical access to computer equipment, storage media, and documentation to only properly authorized individuals.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Policies and procedures for physical access involve all DIT divisions and computing environments. The DIT Physical Security Section of the Security Division administers and maintains the physical security program. **Physical Access Security** DIT has established and documented policies and procedures regarding physical access security. 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 employee's access considering their job classification/function. The Physical Security Officer assigns an access card, picture ID number, the appropriate clearance codes and forwards the Access Form to the Security Manager for approval. Employees must sign, acknowledging 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 recorded on the Tracking System and assigned specific access points. The access card reader at each locked door reads the access card and only unlocks it if the Tracking System acknowledges 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 Capitol Police station 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.	**Physical Access Security** Tour DIT facilities and perform the following: a) Document where critical computer processing hardware (mainframes, servers), computer storage devices (disk packs, optical drives), telecommunication devices (modems, routers, gateways), backup devices (tape drives, mirrored servers), sensitive documentation, backup media (tapes), and Telemedia Equipment (PC desktop video and picture teleconferencing hardware) reside. b) Determine by observation, then document the current status of locked physical access points to the above listed devices. Be sure to notice doors or service windows that are propped open or have taped over lock mechanisms. c) Document all control points that must be passed through in order to get to the Data Center. Consider access from stairwells, front lobby, freight elevator and other entry points. d) Determine by observation that all people encountered in the secure areas have their picture ID displayed as required by DIT policy. Document reasons for exceptions. e) Document and evaluate who has control over the access card database and hardware. f) Document and evaluate if a master key is available for the Data Center and other areas that contains secured devices, and if so who has a copy or access to these keys Obtain from the Physical Security Manager a computer generated file or printout that	**Physical Access Security** In response to last year's testwork and finding, the physical access security policy was revised effective August 30, 1999 to include the proper display of ID badges at all times, procedures when visitors are in the building and information regarding Schlage Access Cards. As of March 31, 2000 there were 259 individuals with access to the data center. Several individuals were identified who only use their access once a month, and one individual who does not use and did not realize he had data center access. Due to the lack of written guidelines, it could not be determined if their access was appropriate. ***(Repeat Finding)*** No other exceptions were noted.

Objective 3: Policies and procedures provide reasonable assurance to limit physical access to computer equipment, storage media, and documentation to only properly authorized individuals.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
DIT employees do not allow unescorted visitors or vendors to follow behind them when entering a door requiring use of an access card. With the exception of those individuals using the DIT auditorium or classrooms, DIT requires 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 continuously manning 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. **PC & Local Area Network Security** DIT has established a security policy that will protect and safeguard information residing within the DIT Local Area Network (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. LAN equipment resides in locked rooms that require access cards to open. 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 PC when leaving the premises. Also, users store magnetic media (i.e. diskettes, tapes, etc.) in a secure container away from extreme temperature and sunlight.	includes each employee's name, ID number, and approved physical access points. Using this information, judgmentally select ten employees who have access to the data center. Determine and document if these individuals have job functions that require such access. Review the new policy on employee access to the data center. Review the Schledge Access Report that lists all users and their total access usage for the past 12 months to the data center. Determine if any employee has used their total access less than what is required in the new policy in order to be granted an access card. Determine that the computer facility is reasonably secure from foreseeable and preventable threats to its physical continuity. Consider heating and cooling requirements, fire suppression and readiness, water detection and readiness, power supply, and whether personnel have been trained for emergency responses.	

Objective 3: Policies and procedures provide reasonable assurance to limit physical access to computer equipment, storage media, and documentation to only properly authorized individuals.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Systems Development Division (SDD) PC Security DIT has established PC security standards in order to protect and safeguard both the property and data associated with PCs assigned or in the custody of the SDD. Employees protect diskettes containing sensitive or confidential data by locking them in a secure place. The employee advises the SDD 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 disk. The LAN equipment and laptop computers are stored in a cubicle that is locked at night. All employees are encouraged to challenge anyone whom they do not recognize.		
Physical Access of Promoted, Transferred and Terminated Employees DIT has established steps to promptly remove physical access for terminated employees and correctly allocate physical access to transferred and promoted employees. When a supervisor learns of an employee's termination, the supervisor immediately provides Personnel with a memorandum notifying them of the termination. Personnel 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.	**Physical Access of Terminated Contractors** Obtain a list of recently terminated contractors. Judgmentally select three contractors and verify that access has been terminated in a timely manner.	**Physical Access of Terminated Contractors** Physical Security relies upon vendor notification for information about vendor employee terminations. However, DIT does not have a policy to obtain notification from vendors of terminations of employees they are using to perform their contractual obligations at DIT. ***(Repeat Finding)***

Objective 4: Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Security Division has responsibility for logical access to programs and data. The policies and procedures cover the computing environments of MVS, Unisys, and access through firewalls. **All DIT Computing Environments** DIT has established a program to ensure the confidentiality, availability, and integrity of data DIT owns or serves as custodian. The program follows the Commonwealth of Virginia Information Technology Resource Management Standard 95-1 issued by the Council on Information Management (CIM). When customers request access to DIT systems, the procedures below are followed. **Logical Access to Programs** When customers 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, customers must take security measures to ensure that another customer cannot access their data contained within a program. It is important to note DIT provides three types of security for the Unisys system, (1) Read-Write Access (2) Access Control Records (ACR) and (3) Compartments, for protecting customer data. DIT cannot mandate that customers use these security features, but only recommends their use. If a customer does not use one of the security options, then other Unisys users have free access to the computer data. **Logical Access to Data** <u>MVS Computing Environment for DIT Employees and Customers</u> Each customer (including DIT) must appoint an Agency Security Officer (ASO), who	**MVS Environment** To obtain an understanding of the logical access controls surrounding the MVS IBM environment, document in detail the files, the file contents, and the mechanisms that are used by DIT to secure other agencies resources and access. Document any changes on how an Agency Security Officer is set up by DIT. Determine if changes have occurred in the features used to keep Agency Security Officers from writing in another agency's rules. Using the SHOW ACF2 and SHOW STATE commands, determine that the system parameters are reasonable (MAXTRY should be between 1-3, and MINPSWD should be between 4-6). In addition verify that the following settings are set properly: • MODE=ABORT which kills logon attempts not authorized by access rules. • NOSORT=NO To determine that system access by DIT personnel is restricted to authorized individuals, obtain a computer-generated printout of the Logon ID File (for DIT) and perform the following: a) Judgmentally select five users and determine that the Logon ID record is accurate for each user by reviewing the initial written request form (DIT03-001). b) From the above sample, evaluate reasonableness of the password expiration setting under 'Miscellaneous' MAX for each user. c) From the above sample, evaluate the 'Miscellaneous' STATISTICS, which shows the number of security violations. Investigate and document any large numbers reported. Produce an ACF2 'decomp' listing of the access rules for system accounts (datasets). Determine that the users in a judgmental sample of five programs or utilities are	**MVS Environment** No exceptions were noted.

Objective 4: Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
establishes, maintains, updates, and deletes access for customer end-users. The customer must complete a form for each individual user and the ASO, DIT Security Officer, System Coordinator and DASD Coordinator must sign the form indicating approval. DIT's Security Division keeps a copy of the approved form. DIT performs the following procedures after receiving the form. 1. Verify the ASO signature. 2. Verify that the logon id is seven (7) alphanumeric characters and that the first three (3) characters are the agency qualifier. 3. List the logon id's to make sure ACF2 returns message that logon id does not exist. If the logon id does exist, contact ASO. <u>Unisys Computing Environment for Customers</u> Each customer must select a Unisys Sub-Administrator and send a letter to DIT indicating the sub-administrators name and to have the appropriate security features established. DIT does not set up access of customer's employees, only the sub-administrator. The individual customer implements procedures for setting up <u>end user</u> logon-id's and privileges. <u>Unisys Computing Environment for DIT Employees</u> All DIT end-users must fill out a Unisys logon-id request form with proper authorization and submit it to the Security Division when requesting access. DIT designated personnel receive all special requests with written justification and the signature of the end-user and their supervisor before setting up the logon-id in accordance with the request.	reasonable and appropriate. Determine that all ACF2 Rules Datasets are restricted to the security officer and an alternate. **UNISYS Environment** Obtain an understanding of the logical access controls surrounding the UNISYS environment. Document in detail the files, the file contents, and the mechanisms that are used by DIT to secure other agencies resources and access. List features even if they are not in use by any agency. Review the Unisys Sub-Administrator request form (DIT10-001) for three agencies that use the UNISYS. Determine that a request letter signed by the agencies MIS Director was sent with the request form and that the forms were filled out properly before access was given. Evaluate and document how many DIT personnel can access the User ID Maintenance screen by using the DIT SIMAN Administrator sign-on. This access allows for adding deleting or changing agencies' Sub Administrator's capabilities. Contact two agencies that rely on UNISYS to determine if DIT has informed them that access security is the responsibility of the agency.	**UNISYS Environment** DIT is not performing a periodic review of agency sub administrator accounts. Of the 13 agency sub administrator accounts, we reviewed two. Of these two, one had not been used since 1991. Agency policies do not address the periodic review of UNISYS sub administrator user accounts, and therefore impairs the effectiveness of security over system access. No other exceptions were noted.
Logical Access to Programs and Data through DIT Firewalls The security firewall is a combination of hardware (SUN SPARC workstations) and	**Firewalls** Provide updated detailed documentation on the firewalls used at DIT that control access from agencies and the outside world.	**Firewalls** DIT does not perform security reviews of trusted agency firewalls to ensure

Objective 4: Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
software (Eagle Network Security Management System, Raptor Systems, Inc.) designed to provide a security barrier by blocking external networks from accessing DIT's computer environment, including the MVS and Unisys systems. The ASO requests access to the DIT firewall by contacting the DIT Help Desk. The ASO completes and signs a Commonwealth Telecommunications Network (CTN) Security Firewall Access 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 setting up access, the ASO 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.	Obtain a sample of the programming used in the Application Gateway Firewall. Determine that in fact the firewall is checking for proper system usage. Determine that the Unix files have been configured properly on the firewall by performing the following: a) Obtain a listing of the root directory. Determine that no other applications are running on this server such as compilers, other application programs, Web services, etc. b) Obtain the /etc/passwd file and determine that only the root and one administration account are active. c) Determine that all standard network services in the /etc/inetd.cof file are commented out except for the console log. There should be no telnet, rlogin, ftp, tftp or other network logins or file transfers. d) Determine that all trusted services are turned off. For example, there should be no /etc/hosts.equiv or /users/$HOME/.rhosts files. These files tell who is trusted by the mere fact that the user is trusted somewhere else. e) Inspect /etc/inittab and /var/spool/cron/crontab/root to determine what scripts and jobs are run at startup and other times. Determine that these jobs can not be written to except by owner. f) Obtain system file directory with permissions. Examine key directories for restricted permissions. Determine from interviews with key staff, what reports are generated from the firewall and how often they are reviewed. Obtain a computer-generated list of authorized users that can pass through the firewall. Trace three users back to their original CTN Security Firewall Access Form (DIT03-004). Determine that the form was filled in correctly with the proper authorizations.	adequate security. Four agencies (VDOT, DGS, DSS, and VDH) and the agencies that go through them to reach DIT (APA, etc.) are exempt from authenticating at the DIT firewall. These four agencies have firewalls of their own that DIT trusts as being secure. DIT does not have a policy as to who will be a trusted relationship and the requirements to maintain this relationship. ***(Repeat Finding)*** No other exceptions were noted.

Objective 4: Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
	LAN Environment Provide updated documentation on how many people are responsible for administering the LAN. Document names and titles. Review the Windows NT Server security system on-line with the LAN Administrator for any unusual or unauthorized log on attempts. Investigate and determine what action was taken by the LAN administrator for resolving the issue. Verify whether the Windows NT server is still being used to validate LAN users dialing into the network. If this server is being used to validate users dialing in, evaluate the strength of its settings. Provide updated documentation on whether DIT has purchased software for a more extensive automated reporting of authorized and unauthorized uses of their LAN. Determine that password controls have not changed since prior's review. If changes have occurred, evaluate and document the strength of its settings. Follow-up on the issue of LAN users being allowed 10 unsuccessful attempts before their account is locked out for LAN access. Judgmentally select 5 users from the DIT Organizational Chart. Based on the users selected, request the Agency LAN Action Request (ALAR) form to review the appropriateness of LAN access granted based n the users job functions. **Web Servers** Determine that the Unix based Web Servers are configured properly by: a) Obtain a listing of root directory. Determine that no other application is running on this server. b) Obtain the /etc/passwd file and determine that only one account has UID of "0", that a shadow password file is used with all	**LAN Environment** DIT lacks a sufficient policy and procedure for secure LAN access. Currently, a user has 10 login attempts to get the password correct. No other exceptions were noted. **Web Servers** Audit testing of web server configuration and logical security revealed no material weaknesses.

Objective 4: Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
	accounts passworded or disabled, that application users are not given a shell, that only a few users know the superuser password. c) Obtain a listing of system files with permissions. Examine key directories for restricted permissions. d) Determine that all standard network services are commented out of the /etc/inetd.cof file. e) Examine /etc/inittab and /var/spool/crin/crontab/root to determine what scripts are run at startup and other times. Determine that these are restricted. f) Determine that all trusted services are turned off. On the Windows NT based web server, perform a logical NT review by performing the following: a) Determining who has ADMIN account capability and that this is reasonable. b) Verify on-line that the GUEST account is not set up in the user domain. c) Interview the systems administrator responsible for managing the NT Web Server. Determine relative level of experience, professional qualifications, and attitude of control relative to securing the Windows NT server. d) Determine the Windows NT version and service release installed on each critical system. (Each critical system should have installed service release 5. All other systems should have a minimum of service release 3 installed). e) Determine the desktop operating system on critical computers. Determine if the installed OS provides adequate security to the desktop. Determine if individual user's log into the NT domain, enforcing authentication to connect to the network. f) Determine the domain structure used by the agency.	

Objective 4: Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
	g) Based on the domain structure, determine if trust relationships have been established between domains. h) Determine that sample pages have been removed from the Microsoft directory. i) Determine if DIT has made any effort to inform agencies that their data is at risk of exposure if they do not upgrade their NT machines to a Windows 95 or 98 prosy server that will allow for data to be encrypted as it passes over the network. j) Determine if information is uploaded from the NT box to the UNIX box, and that only the UNIX box houses web site information that is viewed by the public. k) Review the implementation of Windows NT at the agency. Determine what portions of the implementation are critical. Be aware that if log on authentication is processed through NT, the NT primary domain controller should be classified as critical. Document the basis for the determination of criticality and list all critical systems. l) Gain access to each critical system as an administrator. Install Somarsoft DumpACL and Cerberus Internet Scanner. Run reports as necessary. m) Review the DumpACL server policies report to determine the configuration of auditing for NT events. Determine the appropriateness of the configuration. n) Review the DumpACL rights report to determine if user rights have been given to specific users. If rights have been specifically granted, determine the appropriateness of the grant. o) Review the user permissions report from DumpACL to determine the password rotation policy. Determine the appropriateness of the established policies. p) Using disk manager, ensure that NTFS is the installed file system on all drives in each critical server.	

Objective 4: Policies and procedures provide reasonable assurance that only properly authorized individuals have logical access to programs and data.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
	q) Review the DumpACL directory permissions report to determine that access to REGEDIT.EXE and REGEDIT32.EXE are properly restricted. r) Review the DumpACL server policies report to verify the domain structure and trust relationships. Using auditor judgment, determine the appropriateness of the domain structure. s) Review the agencies policies and procedures that determine critical directories, files, and shares. Using auditor judgment, identify critical shares, directories, and files. On a sample basis, using the DumpACL directory permission report, determine that access is properly restricted. t) Review the DumpACL server services report to determine if the RAS service is installed and running. If it is both installed and running, review the DumpACL user report to determine if any users have RAS access. If there are users with RAS access, determine the appropriateness of the configuration. u) Review the DumpACL user permissions report to ensure that each user is included in a group. Using auditor judgment, determine on a sample basis if the group assignment is appropriate. v) Determine if the agency is using directory replication.	

Objective 5: Policies and procedures provide reasonable assurance that the computer Operations Division provides adequate controls to prevent unauthorized access to job scheduler functions in the MVS and UNISYS environment.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The Computer Operations Division schedules processing, and identifies and resolves deviations in jobs.		
MVS Environment	**MVS Environment**	**MVS Environment**
Control-M is the program DIT uses to perform job scheduling and production control. Control-M is designated in the Job Control Language (JCL) and completely automates the JCL setup tasks, job scheduling and execution, processing analysis and problem resolution, workload optimization, and recovery processing. Control-M provides comprehensive tracking and control facilities and allows for projections and graphic presentations to further enhance data center productivity. When using Control-M, the customer submits a Scheduling Request Form for additions, deletions, or changes. A DIT scheduler inputs the information from the form into Control-M. Jobs can then run daily, weekly, monthly, on holidays, on workdays, etc. Control-M assembles a schedule outlining when jobs will be run based on the day and time requested and any prerequisites to the job. A daily scheduling report runs in the morning and lists any changes during the day affecting that day's processing. All DIT customers use Control-M exclusively, except for the Department of Health, which prints some reports independently of Control-M, and the Department of Accounts, which does not use Control-M at all. For the Department of Account's jobs, DIT performs manual scheduling of nightly production jobs rather than using Control-M, while Health submits the jobs themselves and calls to let DIT know the job name, hours to run, number of drives, prerequisites, and comments. If the job errors, the console operator notifies Health. DIT personnel ensure that jobs scheduled through Control-M or manually do not interfere with one another. DIT is currently working on getting all the customers to use Control-M exclusively.	Determine if any changes have been made on who is allowed to access the Control-M and Control-R functions for adding, deleting or changing scheduling related information. Evaluate whether the changes are appropriate in reference to the user's job duties.	No exceptions were noted.

Objective 5: Policies and procedures provide reasonable assurance that the computer Operations Division provides adequate controls to prevent unauthorized access to job scheduler functions in the MVS and UNISYS environment.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
UNISYS Environment SAM (Scheduling and Activity Monitor) Control is the automated scheduler for the Unisys system. All customers run jobs through SAM except the Board of Elections. DIT is currently working on setting up the Board of Elections on SAM Control. In SAM Control, a scheduler receives an approved scheduling change request on the SAM Automated Scheduling Change Request form. DIT personnel enter the change and the SAM Control arranges the schedule and the starting of jobs. The Board of Elections sends documentation for each job they want scheduled and DIT manually schedules the job. **Error Processing in MVS and Unisys Computing Environment** Control-M and SAM Control alert the console operator when there is a problem by highlighting the line of an error. Each job submitted to scheduling has instructions for when errors occur. If the error is an agency job, the customer contact person or programmer is contacted, whomever the documentation instructs to call. If the problem is with an application, an on call engineer is contacted. Operations keeps an on call list of engineers for both agencies and DIT. In all cases of an error, a problem resolution ticket is created (see the HELP DESK Control Objective for a description of Info/Sys Problem Management Database). This ticket often helps in solving recurring problems quicker. The console operator will fix the problem or contact the on-call engineer for the application. If a job does not run through Control-M, the customer monitors the job. The only exception is if a customer calls the console operator and makes a special request for him to monitor a job. In this case, the customer must provide the console operator with a contact person and instructions on what to do if an error occurs.	**UNISYS Environment** Determine if any changes have been made on who is allowed to access the Scheduler functions for adding, deleting, or changing scheduling related information. Evaluate whether the changes are appropriate in reference to the users job duties.	**UNISYS Environment** No exceptions were noted.

Objective 6: Policies and procedures provide reasonable assurance that data completeness, accuracy, and security occurs for data transmissions/communications between DIT and customers.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
DIT provides several modes of communications such as dial-up, dedicated lines, and a telecommunications network. Our focus for this objective is the Commonwealth Telecommunications Network (CTN) used as the backbone carrier by a customer for their private network. There are three areas that customers must understand when using the CTN. First, DIT provides routers and firewalls to protect systems that reside in the DIT data centers. Second, DIT does not provide the necessary security (firewalls and routers) to protect customer networks. This security is the responsibility of each CTN user. Finally, various telecommunication companies such as MCI, Bell Atlantic, and Sprint own and control the physical lines from the customer to DIT. The customer can use frame relay, PVC (Point Virtual Circuit), or a telephone line on the CTN to send data to DIT. The customer contacts DIT to establish the proper connection and DIT contracts with various communication companies to provide the telecommunication service. DIT is currently in the process of switching from IDNX to NET99. This process will involve converting from a point-to-point multidrop IDNX environment to all frame relay circuits. DIT has one main router, the CISCO 7513. This router is used to control and direct traffic from the CTN frame relay environment, Network Virginia, and the Internet. Traffic from the Internet passes through a Network Virginia 7000 series gateway router that is maintained by Virginia Tech. Traffic will pass through the gateway router before it reaches the main router at DIT. The CISCO 7513 is configured to only allow traffic coming in from the Internet to access DIT's web page and the DNS server that provides various state agency home page information. The CISCO 7513 accepts traffic coming from the CTN and Network Virginia for users that	Document in detail the communications environment that surrounds the DIT to agency interface. Specifically account for: a) The Commonwealth Telecommunication Network (CTN) b) Frame relay circuits c) Point to Point dedicated circuits d) Analog dial-up lines Obtain the Router Table for the CISCO 7000 (or whatever router is the "first hit router") and perform the following: a) Determine that source and destination IP addresses are valid. Investigate any addresses that seem odd. The default should be to deny all traffic. b) Determine what filtering if any is being done at the router. Filtering should show up as "deny statements". c) Determine that Internet traffic that originated from outside of DIT is routed to a secure Web Page or the firewall. d) Determine that the router is using the two level password option so that the router table itself is secure. e) Determine through testwork if Telnet services are allowed on this router because this router interfaces with the Internet. All maintenance on this router should be done in person. f) Determine who is allowed to make changes to this router, who is responsible for reviewing the table and how often. g) Determine if vendors have remote access to the router. If so, verify that authentication procedures have been established for remote access capability and that access is being monitored. h) Determine that all source routed packets have been eliminated from accessing the router.	No exceptions were noted.

Objective 6: Policies and procedures provide reasonable assurance that data completeness, accuracy, and security occurs for data transmissions/communications between DIT and customers.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
need to access the mainframe systems at DIT. These users are included on an access list that is included in the router table configuration. These users will be allowed to pass through the router, and then would have to be authenticated through the firewall before they can access the MVS and Unisys mainframe systems. An access list is a security feature programmed into the router using Internet protocol (IP) addresses. Only customers using the specified IP address can gain access through the router. After the router, the raw TCP/IP data passes to the DIT Firewall; and again there is verification made to grant or deny access. Customers must request access to the DIT Firewall (see further explanation at the LOGICAL ACCESS Control Objective). DIT is no longer using the CISCO 4000 router to accept traffic coming in from the Internet. A gateway router through Network Virginia now handles the services that were once provided by the CISCO 4500. The network security division at Virginia Tech is responsible for configuring the security controls on the Network Virginia gateway router. DIT does not establish or configure customer routers unless requested. The request to have their router set up or worked on follows the procedures used for problem management (See procedures for the HELP DESK Control Objective). Various telecommunication companies own and control the physical lines between the customer and DIT. DIT has no security responsibility for these lines.	i) Determine that ports 79 and 87 have been filtered out. (Port 79 allows access to outsiders for learning about internal user directories and the names of host from which users login. Port 87 is a link commonly used by intruders for CISCO routers). j) Determine that a deny statement exist for packets received that have a source address of an internal network address (this is a precaution against spoofing). Provide updated documentation on the methods that agency employees use to dial in from laptops or home PCs. Evaluate the method and security of this arrangement. Request access to the Info Sys Database. Download a portion of the database of problem tickets into an ACL file. Document instances of line down time and how DIT and the CTN handle such an event. Determine if there are any tickets that were not resolved within a 24 hour period. Document how DIT provides incoming and outgoing Internet services for other agencies. Determine if this function is secure for DIT and whether the DIT firewall protects agencies from any Internet based threats. Investigate and document the extent of cooperation between DIT and an agency when it comes to configuring the necessary communication lines and equipment (modem, routers). Determine if this provides a secure method of communications implementation.	

Objective 7: Policies and procedures provide reasonable assurance that a quality assurance function exists to ensure the identification, implementation, evaluation, and monitoring of policies and procedures, on a periodic basis, for effectiveness.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
All DIT personnel must follow the DIT Policies and Procedures Manual. Management uses the policies and procedures to direct the decision-making process, and ensures that all DIT employees know the approved policies and procedures. DIT also has a Customer Guide, which contains procedures for their customers. **Approval Process for New/Changes to Existing Policies and Procedures** A Director/Manager initiates a draft policy and/or procedure. The Manager/Director sends the draft, usually through e-mail, to the Division Directors and Managers for input. The initiating Director/Manager takes the input into consideration and then submits a final draft to Human Resources. Human Resources submits the draft to the Agency Director for approval. If the Agency Director approves the policy or procedure, Human Resources will then distribute copies to agency staff as an e-mail attachment. The Management Information Systems Division will add the new/revised policy or procedure s to the Agency Information section of DIT's Intranet. The policies/procedures on DIT's Intranet should be considered the most up-to-date copies for reference purposes. **Division Procedures** Divisions may develop procedures that apply only to their division. Procedures developed by divisions must comply with the DIT Computer Services Division Customer Guide and the Problem Management Guidelines and Procedures Manual. The Deputy Director of Services approves divisional procedures. The Branch/Division Manager reviews the DIT Computer Services Division Customer Guide every December and makes the appropriate changes. There is no periodic review of the Problem Management Guidelines and Procedures Manual. If a manager identifies a possible change to the manual, he will present the change in writing and management conducts an analysis of the request. Management discusses the change at the weekly management meeting. If approved, management issues the change and then evaluates the success or failure of the change.	Determine that policies are initiated and approved in the manner described by the DIT Policies and Procedures Manual. Choose one new policy or procedure and one policy or procedure update and follow it through these steps: a) Division or Branch initiates a new or updated draft policy. b) Draft is distributed to Agency Director, Deputy Director and Division Directors for comments. c) If approved the final draft is submitted to Human Resources. d) Human Resources obtains approval from the Agency Director. e) The final draft is submitted to MIS to be placed on the Intranet. f) Employees are made aware of the policy by management. Document and evaluate whether a process to review policies for effectiveness and relevancy occurs on a regular basis.	DIT's policies and procedures are complex and must cover numerous areas, technologies and personnel. Keeping complex policies and procedures current and making sure that their content covers operations requires a systemic approach to their review and change. This review found several areas where the current policies and procedures do not address DIT's changing environment. There is no policy for periodically reviewing policies and procedures to ensure they are still effective in meeting the needs of the agency. No other exceptions were noted.

Section IV. OTHER INFORMATION PROVIDED BY THE SERVICE AUDITOR

Additional controls exist over information technology services provided by DIT. These controls, while not evaluated during the current audit, are described below for informational purposes. We express no opinion on the policies and procedures included in this section.

Hardware Change Control

The Computer Operations Division performs changes to the MVS and Unisys hardware in the Data Center and the Telemedia Division performs the changes for the PC Desk Top Video and PictureTel Videoconferencing hardware. Many colleges and universities use this hardware to broadcast classroom instruction to off-campus locations. Additionally, many state agencies use this service for teleconferencing.

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 all changes approved by the Computer Operations Manager.

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, he sends the request to the Operations Analyst Section (Unisys or MVS) for review. The Operations Analyst distributes the change to the appropriate personnel for review, addresses questions or concerns, and informs the requester of the time and date to schedule the change. The customer bulletin 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 them to the Operations Supervisor.

Monitoring of System Perfomance

The Capacity Planning Branch is part of the Technology Resource Management Division, which is under the Finance & Administration Directorate. Capacity planning covers the MVS and Unisys Environments and the Commonwealth Telecommunications Network.

The Capacity Planning Branch prepares a capacity planning report monthly to be used for procurement planning. The report contains recommendations, based on the performance/capacity measures. There is a capacity planning meeting monthly.

MVS Performance/Capacity Monitoring Procedures

The software used to monitor performance in the MVS environment is a product called OMEGAVIEW. MVS is comprised of many subsystems including MVS, VTAM, IMS, DB2, CICS, and SMS. DIT subsystem engineers identify potential subsystem problems by using a components of OMEGAVIEW called Omegaview 1 and Omegamon. The engineer monitors performance based on thresholds that are reasonably set to alert them of any exceptions that may occur for continued processing.

Omegaview 1 alerts the engineer that there is a problem while Omegamon allows the engineer to view the problem at the subsystem level, for a more detailed investigation of the problem.

Unisys Performance/Capacity Monitoring Procedures

A software package called PRISM monitors the Unisys lines. PRISM reports the transaction traffic on a line. DIT will eventually replace this software because it cannot monitor newer technologies like TCP/IP. DIT will provide the PRISM line summary report to customers who request it, such as DMV, DSS, VEC and TAX.

Constant monitoring of the Unisys system occurs. TORCH/PMS software (Performance Management System) collects Unisys system statistics and downloads the data to VIEWPOINT software on a PC. VIEWPOINT constantly displays statistics about the Unisys system. When VIEWPOINT encounters a problem, it flashes a red signal or produces an audible alarm. If a problem occurs, the Unisys Operator notifies the Help Desk or Unisys Systems Engineer. The same alarm also alerts a Unisys Systems Engineer on their PC.

Backup and Storage of Tapes Off-site

The Computer Operations Division performs backups of the MVS and UNISYS environment, including all shared disk packs. It is the customer's responsibility to perform backups of all dedicated disks packs. It is also the customer's responsibility to inform DIT of the information to store offsite.

The DIT scheduling group enters the backup, offsite storage, and retention time requests made by customers 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 has the next two (older) backup tapes.

Argus provides DIT off-site storage. Argus sends a courier to pick up new tapes and return old tapes. Monthly, DIT personnel go to the off-site storage location and perform and inventory of the tapes. If there is a discrepancy, DIT personnel determine the cause for the discrepancy. A bar code on the UNISYS tapes helps to reduce discrepancies.

MVS and Unisys Backups and Offsite Storage

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

PC and LAN Backups

DIT employees regularly back up data on their PC hard drive. If the DIT employee created critical data files, the DIT employee has responsibility 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.

Systems Development Backup

The Systems Development Division copies and stores offsite all systems and documents for SDD customers, internal management and administration. Offsite storage includes all SDD purchased software tools and packages and one copy of the Management and Control System (MACS) microfiche files. Every Friday night, there is an automatic back up of the SDD LAN project directory, and an automatic incremental tape backup runs Monday through Thursday night. SDD can use the last incremental tape and the Friday night back up tape for reconstruction of files. ALL backup tapes are stored in the DIT/MIS fireproof safe.

CIM Standard 95-1

DIT is in compliance with CIM Standard 95-1. Their most recent Business Impact Analysis was completed in April of 1999.

Help Desk Personnel

The Help Desk in the Computer Operations Division identifies, records, tracks and engages the appropriate resources to resolve customer and DIT system problems.

DIT provides Help Desk service 24 hours a day. DIT uses an Automatic Call Distribution (ACD) software package that tracks the calls to the Help Desk personnel. Personnel log all problem calls into the IBM Info/Sys Problem Management database maintained in the MVS environment. Info/Sys records problems as tickets and automatically assigns a number and tracks the call. The Problem Management Guidelines and Procedures manual outlines procedures for creating, escalating, reviewing, dispatching, checking status, and closing tickets.

When the MVS system is not operating, the 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.

The ACD system can track and report on calls answered, hung up before answering, and the wait times for calls. Management runs these reports daily and reviews them. Management reviews and discusses tickets open more than two weeks in Info/Sys at a weekly meeting.

Section IV. RESOLUTION OF PRIOR YEAR AUDIT FINDINGS

The Department of Information Technology has not taken adequate corrective action on the previously reported findings listed below and we included them in Section I. FINDINGS SUMMARY. The Department of Information Technology corrected all other previously reported findings and we have not included them in this report.

Perform Review of 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 why some agencies are exempt from authentication and what procedures the agency must follow to maintain this exemption.

DIT has made progress toward implementing an exemption policy; however, it has not been completed. Therefore, we again make this recommendation in this year's finding, "Perform Review of Trusted Relationships." It is recommended that this policy be finalized and approved as soon as possible.

Limit Data Center Access

As of March 31, 2000, 259 individuals had access to DIT's data center, several of which have no need for this access. Currently, there are no guidelines for area managers to follow when determining whether their employees need data center access. Individual area managers request physical access for their employees. Additionally, the data center's management only reviews annually who has data center access.

During our review, we found that DIT does not have policies and procedures in place to limit access to the data center. Therefore, we again make this recommendation in this year's finding, "Limit Data Center Access."

Require Vendor Notification of Employee Terminations

DIT does not have a policy that requires vendors to give notification when their employees with data center access terminate. Several of DIT's outside vendors have physical access to the data center. Physical security relies on the vendor to tell them when their employees terminate.

During our review, we found that DIT does not have policies and procedures in place to require vendor notification of employee terminations. Therefore, we again make this recommendation in this year's finding, "Require Vendor Notification of Employee Terminations."

Commonwealth of Virginia

Walter J. Kucharski, Auditor

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

May 24, 2000

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 III 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, 2000. 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 in 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, 2000. 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 III of this report, to obtain evidence about their effectiveness in meeting the control objectives described in Section III as of March 31, 2000. The specified policies and procedures and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided 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 III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period from April 1, 1999 to March 31, 2000.

The description of policies and procedures at the Department is as of March 31, 2000 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 III, 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.

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

AUDITOR OF PUBLIC ACCOUNTS

JBS:aom
aom:58