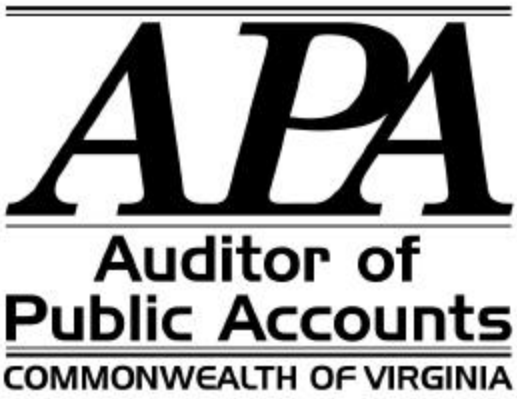
DEPARTMENT OF INFORMATION TECHNOLOGY
RICHMOND, VIRGINIA

SERVICE ORGANIZATION REVIEW

REPORT ON POLICIES AND PROCEDURES
PLACED IN OPERATION
AND TESTS OF OPERATING EFFECTIVENESS
AS OF MAY 30, 2003



EXECUTIVE SUMMARY

This report reviews the Department of Information Technology's (DIT) policies and procedures placed in operation as of May 30, 2003. 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 represents a generally applicable and accepted standard for good practices for information technology control.

This report should provide DIT customers, their independent 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 the customer's financial statements that may be affected by policies and procedures at DIT. If customers do not have effective controls, DIT's internal control policies and procedures may not compensate for such weaknesses.

We found:

As reported in Section III, DIT's policies and procedures are suitably designed and operating effectively to provide reasonable assurance that they achieve their specified control objectives as of May 30, 2003. The reader should evaluate this information only with a concurrent assessment of the customer's internal controls.

The following agencies use DIT's data center as a site to house their various servers: Virginia Employment Commission, Department of Technology Planning (Virginia Geographic Information Network), State Board of Elections, Department of Social Services, Department of Taxation, Virginia Retirement System. With the exception of Virginia Retirement System, none of the agencies has DIT handle their disaster recovery services for the servers. Agencies need to include their servers located at DIT in their own disaster recovery plans.

We recommend that DIT:

- Install an emergency alternative power source for the data center
- Require contract employees to sign Information Security Agreements

-TABLE OF CONTENTS-

SECTION I

FINDINGS SUMMARY

Install an Emergency Alternative Power Source for the Data Center

The Department of Information Technology's (DIT) data center lacks adequate emergency power in the event of a power disruption from its commercial supplier. The Data Center has equipment for maintaining conditioned power to its computer equipment and heating and cooling systems only for a short period of time; approximately two hours.

DIT is currently in transition to the new Virginia Information Technologies Agency (VITA). Also, the Operations Division is beginning a review of its facilities' needs. As the Department performs these activities, it should strongly consider the installation of an alternative emergency power source such as a diesel generator. Such a power source could provide DIT with reliable electricity to continue operating the Data Center and other critical operations for extended periods of time.

Require Contract Employees to Sign Information Security Agreements

In our review of the Department of Information Technology Information Security Agreements, we noted that one of three tested wage employees and no contract employees had acknowledged and signed Information Security Agreements. On further inquiry, we determined that contract employees do not sign an Information Security Agreement. While some contracts specified information security standards, there is no standard information security clause included in each contract. Further, we noted that DIT's policy 1.17 (Information Security Policy) specifically includes employees except contract employees. Finally, there is no standard for the location of the file copy of the Information Security Agreement that cuts across all types of employees and contractors.

The Department of Information Technology should amend its current policy number 1.17 to include a requirement that all contract employees must sign an Information Security Agreement. Additionally, there should be a uniform standard for the location of the Information Security Agreement, based on the type of employee.

The addition of this control will ensure that contract employees have the responsibility of protecting sensitive information from theft or loss. Failure to have signed agreements may hinder the enforcement of legal responsibility for breaches in information security. Consistent standards for the location of this information will aid in periodic reviews to ensure that all persons employed at DIT have signed agreements.

SECTION II
OVERVIEW OF SERVICES PROVIDED

The Department of Information Technology (DIT) provides the Commonwealth of Virginia 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.

DIT also provides a new area within their data center that acts as a server farm for customer agencies. Customers may "co-locate" servers owned by the respective agency into the data center under the auspices of

a physically controlled environment.

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 about the operating effectiveness of the Department of Information Technology policies and procedures in meeting specified control objectives. The test procedures used to review the operating effectiveness of the respective control objective and policies and procedures and the results of our work are listed in the Appendix matrix.

The Appendix matrix represents testing as of May 30, 2003.

SECTION IV
OTHER INFORMATION PROVIDED BY THE SERVICE AUDITOR

User Agency Control Considerations

User agency policies and procedures should provide reasonable assurance that they also conform to the Commonwealth's Information Technology Security Standard SEC2001-01.1. The development of these policies and procedures should consider DIT's relationship to the user agency and the services DIT provides.

Some agencies use DIT's data center as a site to house their various servers. With the exception of the Department of Social Service's E10000, each agency administers their own servers and DIT does not include their software, data, or equipment in its contingency plans. All user agencies have signed a Memorandum of Agreement (MOA) that establishes agreed-upon levels of service provided by DIT.

Disaster recovery services for the servers defined in the MOA are optional. DIT does not have an obligation for disaster recovery. Each agency has an obligation to ensure that its disaster recovery/contingency planning includes a provision to address the agency's role. The agency needs to have backup routines and fallback plans in case of a disaster in the data center. If the agencies need DIT to provide these services, they should set out what disaster recovery services they need in their MOA. With the exception of the Virginia Retirement System, none of the agencies thus far has opted to have DIT handle their disaster recovery services for their servers. DIT, however, does perform tape backups and provide offsite tape storage according to agency specifications. Each agency must contact DIT for changes to those specifications.

The following agencies have located servers at DIT:

- Virginia Employment Commission
- Department of Technology Planning
  - Virginia Geographic Information Network (sub agency of the Department of Technology Planning)
- State Board of Elections
- Department of Social Services
- Department of Taxation
- Virginia Retirement System

SECTION V
RESOLUTION OF PRIOR YEAR AUDIT FINDINGS

The Department has corrected all previously reported findings and we have not included them in this report.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

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

May 30, 2003

The Honorable Mark R. Warner
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable Kevin G. Miller
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 and if these policies and procedures were complied with satisfactorily; and (3) such policies and procedures had been placed in operation as of May 30, 2003. 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 May 30, 2003. 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 May 30, 2003. 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 as of May 30, 2003.

The description of policies and procedures at the Department is as of May 30, 2003 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

KJS/kva
kva:

OBJECTIVE 1

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
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	Obtain copies of policies and procedures used to meet the above objective. Inquire as to whether changes have been made to the policy and procedure since last audit period. Document changes and effect on objective in narrative form. Determine whether DIT has completed the implementation of the Applix Help Desk System. Determine if there are any problems with the implementation process if it still has not been implemented. Determine whether existing system software change procedures are made in accordance with management's specifications, properly authorized, properly tested, documented and approved and that only authorized programs are moved into production by performing the following: 1. Evaluate and document any change control tracking software that may currently be in use that was not already addressed. Determine how DIT stays up to date with new versions and patches for the MVS, UNISYS, and UNIX environment. 2. Obtain a list of existing system software changes for this year from the MVS Systems Support Section, the UNISYS/UNIX Data Base Division, the UNISYS Systems Software and Data Communications Division. From this list, judgmentally choose 17 changes and trace back to the initiating request. Using a matrix, evaluate the procedures. Specifically consider whether: A. All proposed changes are specified in a written change request. B. Information systems management (review meeting) initiates or accepts the change request. C. The Chief Engineer responsible is	No exceptions were noted.

OBJECTIVE 1

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
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 communicate 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.	identified in the program comments or audit trail. D. The Chief Engineer properly analyzes and tests the changes. E. Adequate measures are taken during testing to ensure production libraries are safe. F. The software change is properly documented. G. A written rollback plan is present in case of trouble after implementation. H. Information systems management reviews testing results and approves the change before it is placed into production.	

OBJECTIVE 2

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

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. **New and Current Employees** Purpose: To establish and document the Department of Information Technology's policy and procedures regarding physical access security. Scope: All Department of Information Technology employees. DIT premises are protected by an electronic security system. Access cards are required to unlock all secured doors. Each access card provides a unique level of access depending on the individual cardholder's requirements. When an access card is used, it is displayed on the security console. If the access card has been deleted, and has been so noted in the system by the Security Division, it will not allow access to DIT space. Should cardholders incur problems with their access card, they should notify either the Capitol Police or the Security Division. DIT has three types of identification badges and access cards. 1. Permanent Electronic Card Key – The Permanent Electronic Card Keys (Access Cards) are issued to all permanent and part-time employees. In some cases, vendors, consultants, and maintenance personnel are issued these access cards depending on the amount of time spent within the facility. The access card displays a photo of the individual and allows access to DIT areas based on requested access that is approved by DIT Management. They are to be worn visibly at all times. An access card will be issued by the Security Division after receipt of the properly completed form, DIT-41. DIT Access Authorization is approved by a DIT	Obtain copies of policies and procedures used to meet the above objective. Inquire as to whether changes have been made to the policy and procedure since the last audit period. Document changes and effect on objective in narrative form. Tour DIT facilities and perform the following: 1. 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. 2. 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. 3. 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. 4. 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. 5. Obtain from the Physical Security Officer, two randomly selected access log reports. These reports show instances of doors being forced or held open, etc. Determine and document whether proper responses and follow-up procedures were performed. 6. Document and evaluate who has control over the access card database and	No exceptions were noted.

OBJECTIVE 2

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Branch Manager and a Physical Security Officer. Employees should not allow anyone not wearing a picture ID to follow them when entering a door requiring the use of an access card (i.e., no tail-gating). The access card must be returned to the Security Division upon termination of DIT employment or in the case of vendors, termination of the need for access to a particular area. 2. Temporary Electronic Card Key – The Temporary Electronic Card Keys (Temporary Access Cards) can be issued to employees and authorized vendors on contract with DIT. These temporary access cards are kept at the Capitol Police station on the second floor and can be issued only by Capitol Police. They are to be worn visibly at all times. DIT employees who have forgotten or lost their access cards will be issued a temporary access card after Capitol Police have checked the employee list and checked a photo ID. Capitol Police are required to keep the employee's Driver's License or other photo ID until the temporary access card is returned. Employees without an appropriate badge will be asked to report to the Capitol Police for a temporary access card and their names will be reported to the Security Division and kept on file for one year. If a visitor cannot produce a badge, the employee responsible for the visitor will be reported to the Security Division and their name will be kept on file for one year. All filed names will be reviewed with the appropriate Division Director for patterns of violations. If a vendor requires a temporary access card, Capitol Police will check the authorized vendor list and will be required to obtain either a driver's license or company ID prior	hardware. 7. 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 of or access to these keys. 8. Obtain from the Physical Security Manager a Keyholder Access Assignment List that includes each employee's name, ID number, and approved physical access points. Using this information, judgmentally choose ten employees who have access to the secure data center. Determine and document if these individuals have job functions that require such access. Programmers, systems analyst, data base administrators, and non-systems people in general should not have such access. 9. 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. 10. Obtain from human resources or its equivalent a list of new employees. From this list, select an appropriate sample of new employees and obtain their DIT-41 form. Request from the Physical Security Manager an access profile for each employee. Determine and document whether the profile matches the requested access on the DIT-41. 11. Obtain from Human Resources a list of recently terminated employees. Judgmentally select an appropriate sample of terminated employees and determine that DIT's policy on terminated	

OBJECTIVE 2

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
to issuing the temporary access card. For security purposes, Capitol Police will keep all IDs in a locked box until the temporary access card is returned. All such access cards must be returned prior to the individual leaving DIT premises. All persons being issued a temporary access card will be required to sign the DIT Temporary Access Card Sign In/Sign Out Log. 3. Visitor Badge – These badges are issued to all visitors entering DIT space and do not allow access. These badges must be worn on the front of the chest area and have the visitor's name and date printed on it. They can be issued at all DIT reception areas and the Capitol Police area. The only time a visitor badge is not required is if an individual is attending a function in the DIT auditorium or classroom area. To be allowed in DIT space, all visitors are required to register at one of the reception areas (Third Floor Reception area, Telemedia, Telecommunications, Acquisition Services, Security/Partnership, DTP, or Capitol Police) on the Visitor Sign In/Sign Out Log. Visitors will be issued a peel-off badge on which they write their name and date. The DIT employee being visited will be contacted to escort the visitor to the appropriate area. The DIT employee is required to stay with the visitor at all times. When the visit is complete, the visitor must be escorted back to the appropriate reception area to return the visitor badge and sign out on the log. **Terminated Employees** When employees submit resignation letters to their supervisors or when a supervisor is otherwise notified of an employee's	employees is being followed. Request a memorandum from the user's supervisor to the Personnel Branch and a memorandum from the Personnel Branch to the Security Office. Determine that both notifications were timely and that access denial was timely. Review the access list requested in Step 3 to determine that the terminated employees are no longer given access. 12. Obtain a list of recently terminated contractors. Select judgmentally three contractors and verify that access has been terminated in a timely manner. 13. 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. Review a testing of the Uninterruptible Power Source (UPS). Verify that controls are still in place.	

OBJECTIVE 2

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
termination, the supervisor must immediately provide the Personnel Branch a memorandum notifying it of the termination, together with the employee's resignation letter, if available. The Personnel Branch then immediately notifies the Security Division and the Finance Division. For those employees terminating under abnormal circumstances (i.e., firing or death), the supervisor should contact Security and Finance immediately to ensure that system access is suspended, physical access to DIT premises is removed, and other fixed assets are promptly recovered. The supervisor should attempt to collect, at a minimum, the employee's ID card, American Express corporate card, door keys and access and parking badges. Security will provide the supervisor of the terminating employee with a Separation Checklist to ensure that all assets assigned to the individual are relinquished on or before the employee's termination date. The supervisor should use the checklist as an aid in determining employee assets. Copies of the separation checklist can be obtained from Security. Once Security has been notified of a termination, it will produce a list of the employee's system access record from the Security Tracking System and provide this to the supervisor to aid in completing the Separation Checklist. To further assist supervisors, Security will provide them with the paperwork to delete employees' access to selected systems and obtain assigned physical assets. Security will automatically suspend the employee's system accesses on the employee's last day, regardless of whether the appropriate paperwork has been submitted. Security will coordinate its activities with Finance to recover physical assets, if necessary.		

OBJECTIVE 2

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Transferred Employees For transferred and promoted employees, the Personnel Branch will notify Security and Finance of the change in status by providing them with a Payroll Transaction/Authorization Form. Upon notification, Security will produce the employee's system access record from the Security Tracking System and provide this to the employee's prior and present supervisors. Security will also provide the supervisors with Security's listing of physical assets (i.e., pagers, cellular telephones, and telephone credit cards), which are assigned to the individual. Security will work with both supervisors to ensure that the employee has only the logical and physical assets needed in the current position. For those assets not controlled by Security, both the employee's prior and present supervisors should use the Separation Checklist as a guide to determine the assets required and they should coordinate their activities with Finance to ensure that fixed assets are properly assigned and recorded. **Terminated Contractor** **Effective 3/2/02** Once an individual's contract is terminated or the service is no longer required by DIT, the hiring manager shall: 1. Notify the Purchasing and Support Services (P&SS) staff. 2. Notify the Security staff. Security will provide the supervisor of the terminating contractor with a Separation Checklist to ensure that all assets assigned to the individual are relinquished on or before the contractor's termination date. The supervisor should use the checklist as an aid in determining contractor assets. Copies of the Separation Checklist can be obtained from Security.		

OBJECTIVE 2

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
3. To further assist supervisors, Security will provide them with the paperwork to delete contractor's access to selected systems and obtain assigned physical assets. Security will automatically suspend the contractor's system access on the contractor's last day, regardless of whether the appropriate paperwork has been submitted. Security will coordinate its activities with P&SS to recover physical assets, if necessary. 4. Once P&SS has been notified of a termination, it will coordinate its activities with the supervisor to ensure that all fixed assets assigned to the terminated contractor are accounted for. If the fixed asset(s) (including those physical assets managed by Security) cannot be accounted for, P&SS will take the appropriate steps to ensure that the value of the asset is recovered (including, but not limited to, recovery of costs from the terminated contractor's earnings). 5. Complete an ALAR Form to terminate access to the local area network. 6. The hiring manager will retrieve the contractor's badge and any keys that were issued and turn them in to the appropriate area.		

OBJECTIVE 3

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 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 SEC2001-01. When user agencies request access to DIT systems, DIT follows the procedures below. **Logical Access to Programs** User accounts are established in the operating system. The operating system default under both MVS and UNISYS is to grant access to all programs. To mitigate this weakness, DIT uses ACF2 to provide security to all programs, except some specific IMS databases within the MVS environment. Client agencies 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	Obtain copies of policies and procedures used to meet the above objective. Inquire as to whether changes have been made to the policy and procedure since the last audit period. Document changes and effect on objective in narrative form. 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, check to make sure that the following settings are set: 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: 1. Judgmentally choose ten users and determine that the Logon ID record is accurate for each user by reviewing the initial written request form (DIT03-001). A. From the above sample, evaluate the password expiration setting under 'Miscellaneous' MAX for each user. B. From the above sample, evaluate the 'Miscellaneous' STATISTICS, which shows the number of security violations. Investigate and document any large numbers reported. For the three terminated employees selected for test work in Objective 2, verify that Logon IDs were deleted in a timely manner. Obtain from DIT's ACF2 officer the names of all ACF2 rules datasets. Determine that all DIT-controlled rules datasets are restricted to the security officer and an alternate. Using the Logon ID report, document and evaluate based on job function those DIT	No exceptions were noted.

OBJECTIVE 3

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***
users have free access to the computer programs and data. **Logical Access to Data** <u>MVS Computing Environment for DIT Employees and User Agencies</u> 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. <u>UNISYS Computing Environment for User Agencies</u> 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	employees that have one or more of the following privileges: C. ACCOUNT D. SECURITY E. AUDIT F. CONSULT G. LEADER H. READALL I. RESTRICT Produce an ACF2 'decomp' listing of the access rules for system accounts (datasets) such as SYS, COM, and ADABAS. Determine that the users in a judgmental sample of five programs or utilities are reasonable and appropriate. Contact three agencies using the MVS platform and get the names of their most recent user additions from their Security Officer. Then obtain the DIT10-001 request form for each of those users. Determine that the Agency Security Officer, the DIT Security Officer, the System Coordinator, and the DASD Coordinator have signed it. Determine what reports the security officer runs, how often the reports are run, how the reports are reviewed, what is done with the information, and their effectiveness in controlling access. Document and evaluate who is allowed to access the Control-M and Control-R functions for adding, deleting, or changing scheduling-related information. **UNISYS Environment** 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	

OBJECTIVE 3

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***
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 enduser, 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	personnel can access the User ID Maintenance screen by using the DIT SIMAN Administrator sign-on. This access allows for adding deleting or changing an agency's Sub Administrator's capabilities. Review the UNISYS request form (DIT10-001) of three DIT users that have UNISYS access. Determine that the end user and end-user's supervisor signed the request. Contact three agencies that rely on UNISYS to determine if DIT has informed them that access security is the responsibility of the agency. Document and evaluate who is allowed to use the scheduler functions for adding, deleting, or changing scheduling related information. **Firewalls** Document in detail the firewalls used at DIT that control access from agencies and the outside world. 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. Judgmentally select a reasonable number of users based on current size of population. Trace these users back to their original CTN Security Firewall Access Form (DIT03-004). Determine that the form was filled in correctly with the proper authorizations. Review firewall events from the system logs. Judgmentally select a sample of 5 events and determine what action DIT is taking and how appropriate are the responses. Compare current year firewall configuration against the prior year file and review for changes. Evaluate the changes for reasonableness and proper authorization. Obtain a sample of the programming used in the Application Gateway Firewall. Determine that	

OBJECTIVE 3

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***
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. **DSS SUN E10000** **User Accounts** The DIT Unix Branch manager or Department of Social Services' security manager must authorize user accounts	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: 1. 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.. These would appear, for example, as /payroll or /usr/payroll. 2. Obtain the /etc/passwd file and determine that only the root and one administration account are active, that a shadow password file is used with all accounts passworded or disabled, and that only a few users know the superuser password. 3. Obtain a listing of the system files with permissions. Examine key directories, those that contain common system commands and configuration files, for restricted permissions. Only the owner should have write privileges for these files and directories. 4. Determine that all standard network services in the /etc/inetd.conf file are commented out except for the console log. There should be no telnet, rlogin, ftp, tftp, or other network logins or file transfers. 5. Obtain a printout of the /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 the owner. Make sure that /etc/inittab and/var/spool/cron/ crontab/root reside in protected directories with only the owner having write access. 6. 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	

OBJECTIVE 3

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***
and user groups assigned to accounts. Accounts are established with 30-days password expiration, 5-days warning, and 5-days minimum change. A report of inactive Unix accounts will be run on the first of each month. All non-root Unix accounts with no activity for six months will be removed, and the owner notified. All individual root accounts with no activity for three months will be removed and the owner notified. Notification will also be made to the DIT Unix Branch manager and DSS security manager. A user's access authorization will be removed from the system when the user's employment is terminated or the user transfers to a position where access to the system is no longer required. Removal notification is prepared by the immediate supervisor or manager and directed to the DIT UNIX branch manager or DSS security manager. DSS security contacts their users based on no activity for one to three months to determine the need for the user to continue to have a user account. **Super User Procedures** The DIT UNIX branch manager or DSS security manager must authorize root accounts. Root accounts are not typically given to individuals unless there is a defined need for root access. Users who require root access for specific functions will be granted root privilege for only those specific items through sudo configuration. The DIT UNIX system security administrator(s) is responsible for maintaining the sudo configuration. **File protections** Files created by user accounts default to	else. 7. Obtain a list of world writable directories and examine for validity. The only world writable directories should be spool/public directories. 8. Obtain the directory of the application programs and data files. Determine that the permissions are appropriate. 9. Obtain the etc/group file and determine that group assignments are valid. System groups should only have system type members. 10. Verify that all device files are listed in /dev directory and that the directory is protected. 11. Obtain a list of files that are set as SUID SGID, which allows users to achieve capability of the owner of that file. Be suspicious of SUID SGID files that were created after the initial install date. 12. Determine 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. If users log into root directly, accountability of who logged in is lost. 13. Request a listing of vendor-supplied security patches. Determine that they have been applied. 14. Verify that the root account in the etc/passwd has an account other than / as its home directory as all users can access /. 15. Review security logs for extended periods of activity by root. **Department Of Social Service (DSS) SUN E10000** Determine that the DSS Sun E10000 is secure from unauthorized user's by performing: 1. Obtain the /etc/passwd file and determine that only one account has a UID of "0", a shadow password file is used with all accounts passworded or disabled, application users are	

OBJECTIVE 3

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***
read/write for owner, read only for group, and read only for other. The security administrator reviews world writeable files monthly. **Unattended terminal procedures** To prevent someone from viewing information without your knowledge, take precautions such as: • Use a password protected screen saver on your computer monitor • Erase white boards containing confidential information • Immediately remove confidential information from printers or facsimile machines • Remove and secure confidential information from your desktop **Password Selection Guidelines** Passwords must be: • Individually owned • Kept confidential • Changed whenever disclosure has occurred, and changed at least every 30 days • Changed significantly (i.e., not a minor variation of the current password) • A minimum of six alphanumeric characters • Encrypted when held in storage or when transmitted over communications networks • Limited to one use when initially issued or when reset or reissued by security administration personnel	not given a shell (UNIX prompt), and only a few users know the superuser password. 2. Obtain a listing of the system files with permissions. Examine key directories, those that contain common system commands and configuration files, for restricted permissions. Only the owner should have write privileges for these files and directories. 3. Determine that all standard network services in the /etc/inetd.conf file are commented out except for the console log. 4. Obtain a printout of the /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 the owner. Make sure that /etc/inittab and /var/spool/cron/ crontab/root reside in protected directories (only the owner having write access). 5. 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. 6. Obtain a list of world writable directories and examine for validity. The only world writable directories should be spool/public directories. 7. Obtain the directory of the application programs and data files. Determine that the permissions are appropriate. 8. Obtain the etc/group file and determine that group assignments are valid. System groups should only have system type members. 9. Verify that all device files are listed in /dev directory and that the directory is protected. 10. Obtain a list of files that are set as SUID / SGID which allows users to achieve capability of the owner of that file. 11. Determine that superusers do not log on as	

OBJECTIVE 3

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***
Passwords must not be: • Shared with other users • Repeating sequences of letters or numbers • Names of persons, places, or things that can be closely identified with the user (i.e., spouse, children, or pet names) • The same as the userid • Stored in any file or script where it is susceptible to disclosure or use by anyone other than its owner • Displayed during the entry process **Security Patches** The applicability of a patch is determined by the Unix system administrator(s) responsible for maintenance. The system administrator(s) are to be guided by their knowledge of the software and hardware components and previous experience. Sometimes recommended patches do not apply specifically to the E10000 and are not supported by the hardware platform. Other recommended patches do not apply because they are fixes to products that are not installed on customer systems. Software vendors provide bug reports with the details of particular problems and corrections to them. When fixes are available for specific problems encountered, patches are to be applied to correct the problems. The Unix administrator(s) responsible for maintenance will determine whether a vendor's correction applies to an encountered problem. Patches that apply to all customer	root, but instead SU (Switch User) to the root account or have a root capable account with their ID. If users log into the root directly, accountability of who logged in is lost. 12. Request a listing of vendor-supplied security patches. Determine that they have been applied. 13. Verify that the root account in the etc/passwd has an account other than / as its home directory as all users can access /. 14. Review security logs for extended periods of activity by root. **TACACS Server** Determine if DIT is currently using TACACS, XTACACS, TACACS+, or RADIUS for remote user authentication. (The TACACS and XTACACS protocols in CISCO IOS software will no longer be supported.) No further engineering development or bug fixes will be provided for these protocols. Migration should be made toward more modern protocols to support AAA requirements, i.e., TACACS+, RADIUS, or Kerberos v5. TACACS+. These are available in Cisco Secure ACS and Cisco Easy ACS). Verify who is reviewing the TACACS log files and how often they are reviewed. **Terminated Contractors** Obtain the name of the most recent terminated contractors. Determine to what projects and platforms they were assigned. Determine that access to these platforms was removed in a timely manner. **Department Of Taxation** **E-File System** Determine that the servers that support the Department of Taxation's E-File System are secure from unauthorized user's by performing: 1. Obtain the /etc/passwd file and determine that only one account has a UID of "0", a shadow	

OBJECTIVE 3

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***
systems are to be staged on test and development systems first, then migrated to production domains. The initial domain to receive software patches is the DIT test domain. After running on the DIT test domain for a minimum of two weeks without incident, the patches are next to be applied to the customer test/ development system. After running on the customer test/development system for a minimum of two weeks without incident, the patches are to be applied to the customer production domains. **Data Integrity** Regularly scheduled backups are an integral part of data security. The ultimate responsibility for establishing backup procedures lies with the data owner. Backups of mission critical data must be kept offsite to insure recoverability in the event of a natural disaster. Backups will be: • Complete file copies • Incremental backup copies, which are copies of the changes since the last full backup • Database recovery logs which track database activity since the last full backup **Department Of Taxation** Servers owned by the Department of Taxation are managed under similar policies as the E10000 owned by the Department of Social Services.	password file is used with all accounts passworded or disabled, application users are not given a shell (UNIX prompt), and only a few users know the superuser password. 2. Obtain a listing of the system files with permissions. Examine key directories, those that contain common system commands and configuration files, for restricted permissions. Only the owner should have write privileges for these files and directories. 3. Determine that all standard network services in the /etc/inetd.conf file are commented out except for the console log. 4. Obtain a printout of the /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 cannot be written to except by the owner. Make sure that /etc/inittab and /var/spool/cron/ crontab/root reside in protected directories (only the owner having write access). 5. 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. 6. Obtain a list of world writable directories and examine for validity. The only world writable directories should be spool/public directories. 7. Obtain the directory of the application programs and data files. Determine that the permissions are appropriate. 8. Obtain the etc/group file and determine that group assignments are valid. System groups should only have system type members. 9. Verify that all device files are listed in /dev directory and that the directory is protected. 10. Obtain a list of files that are set as SUID / SGID which allows users to achieve	

OBJECTIVE 3

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***
	capability of the owner of that file. 11. Determine 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. If users log into the root directly, accountability of who logged in is lost. 12. Request a listing of vendor supplied security patches. Determine that they have been applied. 13. Verify that the root account in the etc/passwd has an account other than / as its home directory as all users can access /. 14. Review security logs for extended periods of activity by root.	

OBJECTIVE 4

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
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 uses an Enterprise Backup and Recovery System with Veritas software and DLT7000 tape drives housed in an automated tape library. 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 Iron Mountain, 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	Obtain from two different agencies in the MVS environment a list of what tapes should be taken off-site. Verify that these tapes are off-site by reviewing on-line in computer operations to see that the tapes are listed on the computer as being taken off-site and then confirm this at the off-site storage facility. Obtain from two different agencies in the UNISYS environment a list of what tapes should be taken off-site. Verify that these tapes are off-site by reviewing on-line in computer operations to see that the tapes are listed on the computer as being taken off-site, and then confirm this at the off-site storage facility. Determine that LAN server backups are occurring and stored offsite and that firewall and router configurations are stored offsite. Have DIT open a storage box in the presence of the auditor to verify its contents. Visit the off-site storage area and perform the following: 1. Review the facility for physical security (access, fire, and water suppression, etc.) 2. Match the tape inventory by tracing a judgmental sample of 15 items from DIT's off-site storage list to the inventory at the off-site location. Evaluate the use of the Enterprise Backup solution. Determine if substantial (longer than one day) downtime has occurred by reviewing helpdesk logs, hardware support billing records, and inquiry of data center personnel. Determine what progress has been made for an off-site mirrored system and/or method of transferring files electronically for maintaining effective backup in the case of tape drive or primary medium failure.	No exceptions were noted.

OBJECTIVE 4

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

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
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.		

OBJECTIVE 5

Policies and procedures provide reasonable assurance that data completeness and security occur for data transmissions/communications between DIT and its 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 tele-communications 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	Document in detail the communications environment that surrounds the DIT to agency interface. Specifically account for: 1. COVANET 2. Frame relay circuits 3. Point to Point dedicated circuits 4. Analog dial-up lines Obtain the router table and perform the following: 1. Determine that source and destination IP addresses are valid. Investigate any addresses that seem odd. The default should be to deny all traffic. 2. Determine what filtering if any is being done at the router. Filtering should show up as "deny statements." 3. Determine that Internet Traffic that originated from outside of DIT is routed to a secure web page or the firewall. 4. Determine that the router is using the two level password options so that the router table itself is secure. 5. Determine that telnet services are not allowed on this router because this router interfaces with the Internet. All maintenance on this router should be done in person. 6. Determine who is allowed to make changes to this router, who is responsible for reviewing the table and how often. 7. 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. 8. Determine that all source routed packets have been eliminated from accessing the router. 9. Determine that ports 79 and 87 have been filtered out. (Port 79 allows access to outsiders for learning about internal user	No exceptions were noted.

OBJECTIVE 5

Policies and procedures provide reasonable assurance that data completeness and security occur for data transmissions/communications between DIT and its customers.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
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.	directories and the names of the host from which users login. Port 87 is a link commonly used by intruders for CISCO routers). 10. Determine that a deny statement exists for packets received that have a source address of an internal network address (this is a precaution against spoofing). Tour the DIT offices and data center and look for analog lines that are connected to systems equipment. Determine the need for such lines and their security. Determine if DIT allows employees or agency employees to dial in from laptops or home PCs. Evaluate the method and security of this arrangement. Document instances of line down time and how DIT and the CTN handle such an event. 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 6

Policies and procedures provide reasonable assurance that Department of Information Technology conforms to SEC2001-01.1 as it relates to the following areas: Business Impact Analysis, Risk Assessment, Security Awareness/Training Program, Contingency Management Plan, Technical Training, Technical Communications, Authentication, Authorization and Encryption, Data Security, Systems Interoperability Security, Physical Security, Personnel Security, Threat Detection, Security Tool Kit, Incident Handling, and Monitoring and Controlling System Activities.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
The 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. **Business Impact Analysis** DIT has completed a Business Impact Analysis. The Business Impact Analysis only covers systems that affect DIT's business, not customer applications. DIT sent a questionnaire to each DIT Division Director and DIT Project Leader requesting they identify their critical systems and the resulting impact if the system was not operational for a period of time. DIT compiled the information into the Business Impact Analysis and the DIT Director approved it. When adding new systems, a business impact analysis should determine if the system contains critical or confidential information and should be included in the overall Business Impact Analysis. **Risk Assessment** DIT uses a risk assessment software package called RISKWATCH. Risk assessments are conducted 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.	Determine that a recent Business Impact Analysis exists. Review this analysis for reasonableness. Obtain the name of any new system addition over the last year. Determine that this new system has been added to the Business Impact Analysis. Obtain a copy of the last prepared formal risk assessment. Determine that it is no more than two years old and that it reflects major system changes that have occurred in the past year as DIT policy requires. Review the contingency plans for DIT and evaluate for reasonableness. Consider time frames, percentage of operations that could be brought on-line, and the effect on the state agencies that rely on it. Request, from the Contingency Plan Administrator, three of the DIT-required quarterly division updates from the Disaster Recovery Coordinators.	**Install An Emergency Alternative Power Source for the Data Center** DIT's data center lacks adequate emergency power in the event of a power disruption from its commercial supplier. The data center has equipment for maintaining conditioned power to its computer equipment and heating and cooling systems only for a short period of time; approximately two hours. DIT is in transition to the new Virginia Information Technology Agency (VITA). Also, the Operations Division is beginning a review of its facilities needs. As DIT performs these activities, it should strongly consider the installation of an alternative emergency power source such as a diesel generator. Such a power source could provide DIT with reliable electricity to continue operating the data center and other critical operations for extended periods of time. **Require Contract Employees to Sign Information Security Agreements** In our review of DIT's Information Security Agreements, we noted that one of three tested wage employees and no contract employees had acknowledged and signed Information Security Agreements. On further inquiry, we determined that contract employees are not required to sign an Information Security Agreement.

Objective 6

Policies and procedures provide reasonable assurance that Department of Information Technology conforms to SEC2001-01.1 as it relates to the following areas: Business Impact Analysis, Risk Assessment, Security Awareness/Training Program, Contingency Management Plan, Technical Training, Technical Communications, Authentication, Authorization and Encryption, Data Security, Systems Interoperability Security, Physical Security, Personnel Security, Threat Detection, Security Tool Kit, Incident Handling, and Monitoring and Controlling System Activities.

Provided by the Department	**Provided by the Auditor of Public Accounts**	
Policies and Procedures	**Tests Performed**	**Results**
DIT's risk assessment procedures include: identifying the likelihood of an occurrence of a threat, 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. DIT plans to perform an agency-wide Business Impact Analysis and Risk Assessment to comply with the new and updated standards for Information Technology Standard SEC2001-01.1. **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.	Determine that they exist or if no changes were needed that an email was sent to the Contingency Plan Coordinator. Make an inquiry to SunGard (DIT's hot site vendor) and determine that they have been kept abreast of any critical changes to the contingency requirements. Obtain a schedule and proof that the "hot site" scenario has been tested for both the MVS and UNISYS environment. Obtain the names of five recently hired DIT employees and request to see their signed Information Security Agreement. Obtain the training attendance logs for the DIT Systems Security personnel. Determine that they have taken courses in the last year on security related topics. Verify that all DIT employees have had	While some contracts specified information security standards, there is no standard information security clause included in each contract. Further, we noted that DIT's policy 1.17 (Information Security Policy) specifically includes employees, but not contract employees. Finally, there is no standard for the location of the file copy of the Information Security Agreement that cuts across all types of employees and contractors. DIT should append its current policy number 1.17 to include a requirement that all contract employees be required to sign an Information Security Agreement. Additionally, there should be a uniform standard for the location of the Information Security Agreement, based on the type of employee. The addition of this control will ensure that contract employees are held responsible for theft/loss of sensitive information. Failure to have signed agreements may hinder enforcement of legal responsibility for breaches in information security. Consistent standards for the location of this information will aid in periodic reviews to ensure that all persons employed at DIT have signed agreements.

Objective 6

Policies and procedures provide reasonable assurance that Department of Information Technology conforms to SEC2001-01.1 as it relates to the following areas: Business Impact Analysis, Risk Assessment, Security Awareness/Training Program, Contingency Management Plan, Technical Training, Technical Communications, Authentication, Authorization and Encryption, Data Security, Systems Interoperability Security, Physical Security, Personnel Security, Threat Detection, Security Tool Kit, Incident Handling, and Monitoring and Controlling System Activities.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
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 part of the divisional action plans. When the divisional action plans change, the DIT Configuration Review Committee communicates the plan changes to SunGard. **Security Awareness/Training Program** Human Resources and Security require that new employees 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, annually	security awareness training.	

Objective 6

Policies and procedures provide reasonable assurance that Department of Information Technology conforms to SEC2001-01.1 as it relates to the following areas: Business Impact Analysis, Risk Assessment, Security Awareness/Training Program, Contingency Management Plan, Technical Training, Technical Communications, Authentication, Authorization and Encryption, Data Security, Systems Interoperability Security, Physical Security, Personnel Security, Threat Detection, Security Tool Kit, Incident Handling, and Monitoring and Controlling System Activities.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
at the end of November, the Security Division sponsors a Computer Security Day. DIT places a notification in each employee's pay envelope letting the employee know the training date. There are also posters displayed 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. DIT is currently working on developing a formal security and awareness-training program. **User Agency Control Considerations** User agency policies and procedures should provide reasonable assurance that they also conform to SEC2001-01.1. 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 off-site 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.		

OBJECTIVE 7

Policies and procedures provide reasonable assurance that the DIT Server Farm is properly secured both logically and physically from unauthorized access, backups are performed, and contingency plans are in place.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
DIT has established a Memorandum of Agreement (MOA) to establish mutually agreeable levels of service between DIT and the agency requesting use of the server farm. DIT will provide the system access control mechanisms through which the customer will secure its data residing on the customer system. DIT, as custodian of the data, will ensure that this data is not available to other users without authorization by the customer. Access to the data center will be restricted to authorized personnel. Access to the hardware by the customer can be arranged upon request through the current data access policy. Customers requiring access authorization must contact the DIT point of contact. DIT will provide the following operations and network support: • Tape management for system backup • Console management and monitoring activities • Onsite job scheduling, print management, and production control • Problem resolution through the DIT help desk and Network Control Center • Network infrastructure configuration and management of the DIT internal LAN, switches, routers, and WAN. **Disaster Recovery Services** Disaster Recovery Services for the customer-owned hardware are optional. If these services are provided, they will be stipulated to the customer in the MOA. System backup tapes produced will be vaulted and stored off site as requested by	1.Document the controls in place for backup of critical information on the server farm. 2.Evaluate the contingency plans in place. Determine if on-site and off-site storage is available. 3.Many features are required to build a highly resilient server farm. Evaluate the DIT server farm based on the following features: • Highly fault-tolerant hardware (Is the hardware Network Equipment Building System (NEBS) certified? This includes: (1) hardware that protects telecommunications equipment from service outages; minimizes the risk of fires to telecommunications equipment; ensures equipment operation under the range of temperature, humidity, vibration; and (2) equipment that will operate reliably and be serviceable, operate properly in adverse environmental conditions, and not cause harm to the environment or personnel). • A variety of connectivity options • Highly optimized software features • High speed integrated servers providing for fast processing of information 4.Document the controls in place to protect the server farm from the following threats and natural disasters: • Power outage or failure (What type of UPS system is in place? What is the current UPS size? Types of power conditioning/surge prevention systems, power source grids, and extended generator power for the full data center. Is the computer power supply sufficient?). • Environmental controls (Determine the type of H.V.A.C. system. Is the data center air conditioning separate from the building	No exceptions noted.

OBJECTIVE 7

Policies and procedures provide reasonable assurance that the DIT Server Farm is properly secured both logically and physically from unauthorized access, backups are performed, and contingency plans are in place.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
the customer. DIT will be responsible for: • Assigning a DIT primary point of contact who will be responsible for accepting requests for installation, modification, and/or removal of major systems hardware and software. • Responding to day-to-day operational issues reported through the DIT Help Desk, where a ticket number will be assigned and tracked. • Loading all systems and related system software releases for test and production servers. • Maintaining a system-operating log. • Coordinating an agreeable backup schedule and providing backup of system, database, and application files. • Notifying the customer of unscheduled outages and operational problems. • Participating in a monthly meeting with the customer. • Controlling, measuring, and reporting to the customer regarding system availability. • Implementing and administering remote monitoring services. • Data center floor configuration, connectivity, and equipment location. Customer will be responsible for general activities as follows: • Application Installation and Maintenance • Application Availability • Application Performance	system? Is sufficient cooling integrated?). • Fire Suppression (What fire suppression system is in place? Is the fire suppression redundant? Are wet sprinklers and/or Halon available?) • Flooding potential (What is the height of the raised floor?) 5.Document the network security controls in place that secures the data on the server farm from the outside world. 6.Determine how customer traffic is controlled, (i.e., through the use of hubs or if every client is housed on a dedicated Ethernet type server. If it is through the use of hubs, clients can sniff each other's traffic). 7.Determine if DIT is using open racks, closed racks, or 'Intelligent Rack Security' to discretely secure the client's server in a locked, stand-alone cabinet. If not, document what type of physical security is provided for the client's server. 8.Determine if agencies are allowed physical access to their servers. Evaluate the controls in place for protecting each agency server from being accessed by someone from another agency. 9.Determine if secured configuration/repair areas exist for the server farm. 10.List the number and experience/certification level of technicians on site for maintenance and updates to the server farm.	

OBJECTIVE 7

Policies and procedures provide reasonable assurance that the DIT Server Farm is properly secured both logically and physically from unauthorized access, backups are performed, and contingency plans are in place.

Provided by the Department	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
• Database Management and Administration • Application Problem Management • Application Change Management The customer security officer is responsible for ensuring all users are furnished with proper User IDs, Logons, and Passwords for the use of their systems.		