VIRGINIA INFORMATION TECHNOLOGIES AGENCY
RICHMOND, VIRGINIA

SERVICE ORGANIZATION REVIEW

REPORT ON POLICIES AND PROCEDURES

PLACED IN OPERATION

AND TESTS OF OPERATING EFFECTIVENESS

AS OF APRIL 1, 2004

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

EXECUTIVE SUMMARY

This report reviews the Virginia Information Technologies Agency (VITA) policies and procedures placed in operation as of April 1, 2004. 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. This report should provide VITA customers, their independent auditors, and report users with sufficient information about VITA's internal control policies and procedures. If customers do not have effective controls, VITA's internal control policies and procedures may not compensate for such weaknesses.

We found:

As reported in Section III, VITA's policies and procedures are suitably designed and operating effectively to provide reasonable assurance that they achieve their specified control objectives as of April 1, 2004. The reader should evaluate this information only with a concurrent assessment of the customer's internal controls.

The 2003 General Assembly created VITA to consolidate and oversee the Commonwealth's information technology resources. The information system resources reside at VITA's data center or at VITA's client agency locations. Small agencies (with employees less than 100) have already transitioned over to VITA while medium and large agencies transition in upcoming months. Dependent on the applications running on particular equipment, VITA will own and operate the hardware. Most information technology workers employed by in-scope agencies have already or will transfer to the employment of VITA. One of the tenants of this endeavor is to increase security over the information system resources. Inherent with this transition is the necessity to create security standards and assignments of responsibilities for implementing and monitoring the effectiveness of these standards.

Although large agencies have yet to transition to VITA the following agencies use VITA's data center as a site to house their various servers: Virginia Employment Commission, Department of Social Services, Department of Taxation, and Virginia Retirement System. With the exception of Virginia Retirement System, none of the agencies has VITA handle their disaster recovery services for the servers. Agencies need to include their servers located at VITA in their own disaster recovery plans until such time that another arrangement with VITA is established.

We recommend that VITA improve and implement security standards for client agencies.

-TABLE OF CONTENTS-

EXECUTIVE SUMMARY

SECTION I: FINDINGS SUMMARY

SECTION II: OVERVIEW OF SERVICES PROVIDED

SECTION III: CONTROL OBJECTIVES, POLICIES AND PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS

SECTION IV: OTHER INFORMATION PROVIDED BY THE SERVICE AUDITOR

SECTION V: RESOLUTION OF PRIOR YEAR AUDIT FINDINGS

INDEPENDENT SERVICE AUDITOR’S REPORT

AGENCY RESPONSE LETTER

APPENDIX

SECTION I

FINDINGS SUMMARY

Improve and Implement Security Standards for Client Agencies

The Commonwealth has implemented and maintained decentralized information system security for the past 15 years. Before the creation of VITA, each agency had to follow general standards created by the Department of Technology Planning (now part of VITA). Effective December 7, 2001, the current security standard (SEC-2001) replaced an older version of the standard, which had been a modification of past standards such as Council of Information Management's standard (CIM-95-1).

The current standard has 13 attributes that clarify agencies' responsibilities towards securing their information systems. This standard is general and non-technology or vendor specific, so that agencies have leeway to determine what works best in their environment. While this approach leaves room for judgment, it equally leaves open an opportunity to ignore detailed security features. Most technologies at the application level, operating system level, database level, and network component level now have security standards and guidelines based on "best practices" from the federal government and industry. These best practices are common for vendor specific equipment such as Cisco routers. The National Security Agency Router Security Configuration Guideline describes effective ways to secure Cisco routers. The same types of configuration standards and guidelines exist for UNIX, Oracle, Firewalls and more.

A lack of detailed guidelines and standards for configurations within the Commonwealth has led to a patchwork approach to security. Some agencies are extremely security conscience, while others are not. In the past, the Secretary of Technology as the Chief Information Officer of the Commonwealth had the authority to "direct the formulation and promulgation of policies, standards, specifications and guidelines for information technology in the Commonwealth." This authority per legislation has now passed this responsibility onto the newly hired Chief Information Officer who heads VITA. This authority encompasses not only in-scope agencies that transition to VITA but other agencies and universities as well.

Historically, each agency head has had responsibility for the security over their agency systems. As VITA absorbs the agency information system professionals and their knowledge, it is incumbent upon VITA to make sure that they increase their share of the security responsibility. As the centralized technology agency for the Commonwealth, it is now time for VITA to address the lack of detailed security guidance and coordinate who implements and maintains security.

During our audit, we found improper security configurations, such as risky services enabled and improper file permissions on a Department of Tax (Tax) server managed by VITA. Tax gave VITA a UNIX Standard to follow for managing their UNIX servers; however, VITA is not following this standard.

The above is symptomatic of a much larger issue as VITA absorbs more responsibility for the Commonwealth's computing architecture. VITA has developed generic Memorandum of Agreements (MOAs) for servicing their client agencies. These agreements do not specifically address information security concerns other than to state that VITA, as custodian of client's data, will ensure that the data is not available to unauthorized users.

The lack of detailed security information in the MOAs requires VITA to take steps to avoid miscommunication of roles and responsibilities of each party.

We recommend VITA take the following actions to ensure the security over the Commonwealth's systems.

- VITA create and distribute to the client agencies a detailed checklist that defines the roles and responsibilities for information security.

- VITA create or define the "Industry Best Practices" for detailed security configuration standards in our computing environment to include configurations at the operating system level, database level, and network component level.

- VITA use the configuration standards to manage client agencies systems and in cases of potential disagreement, miscommunication, or other questions, take actions to protect the data pending resolution of the matter with the client agency.

- VITA review and correct the Department of Tax server configuration issues.

SECTION II

OVERVIEW OF SERVICES PROVIDED

VITA provides the Commonwealth of Virginia and local governments with a source for meeting their information technology needs. VITA 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.

VITA 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. In addition, many of these same servers and others will transition to ownership of VITA under control of VITA as dictated by Memorandum of Agreement with client agencies.

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 VITA's policies and procedures in meeting specified control objectives. 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.

The appendix matrix lists the test procedures used to review the operating effectiveness of the respective control objective and policies and procedures and the results of our work. The appendix matrix represents testing as of April 1, 2004.

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 VITA's relationship to the user agency and the services VITA provides.

Some in-scope agencies that have not transitioned yet to VITA use VITA's data center as a site to house their various servers. With the exception of the Department of Social Service's E10000 and Department of Tax E-File system, each agency administers their own servers and VITA 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 VITA.

Disaster recovery services for the servers defined in the MOA are optional. VITA 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 VITA 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 VITA handle their disaster recovery services for their servers. VITA, however, does perform tape backups and provide offsite tape storage according to agency specifications. Each agency must contact VITA for changes to those specifications.

The following large agencies have located servers at VITA:

- Virginia Employment Commission
- Department of Social Services
- Department of Taxation
- Virginia Retirement System

SECTION V

RESOLUTION OF PRIOR YEAR AUDIT FINDINGS

VITA 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

April 1, 2004

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

The Honorable Lacey E. Putney
Vice 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 **Virginia Information Technologies Agency** (VITA) 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 VITA'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 April 1, 2004. The accompanying description includes only those policies and procedures and related control objectives of VITA 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 VITA's policies and procedures that have been placed in operation as of April 1, 2004. 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 April 1, 2004. 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 VITA 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 April 1, 2004.

The description of policies and procedures at VITA is as of April 1, 2004 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 VITA 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 VITA, 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 VITA of Information Technology, its customers, and the independent auditors of its customers.

AUDITOR OF PUBLIC ACCOUNTS

KJS/kva
kva:

COMMONWEALTH *of* VIRGINIA

Lemuel C Stewart, Jr.
Chief Information Officer
Email: lem.stewart@vita.virginia.gov

Virginia Information Technologies Agency
411 E. FRANKLIN STREET, SUITE 500
RICHMOND, VIRGINIA 23219
(804) 225-VITA

TDD VOICE -TEL. NO.
(804) 371-8076

July 29, 2004

Walter J. Kucharski
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Mr. Kucharski,

This letter is in response to your report following a SAS-70 audit conducted by your staff of relevant policies and procedures in place by the Virginia Information Technologies Agency (VITA) as of April 1, 2004.

We are pleased that only one exception was noted in relation to a server owned by the Department of Taxation and managed at VITA. The following are the four APA recommendations associated with that exception and the corrective actions VITA will take to address them.

APA Recommendation 1: VITA create and distribute to the client agencies a detailed checklist that defines the roles and responsibilities for information security.

VITA Response: VITA's Security Director has created a checklist to explain the roles and responsibilities for VITA and those of customer agencies in information security. VITA's Enterprise Service Directors are currently in the process of providing this document to responsible agency staff for comment and acceptance. VITA's Security Director will finalize the document and ensure acceptance and understanding by agency management by October 1, 2004.

APA Recommendation 2: VITA create or define the "Industry Best Practices" for detailed security configuration standards in our computing environment to include configurations at the operating system level, database level, and network component level.

VITA Response:: VITA Security will develop an action plan to address this recommendation by October 1, 2004. The timeframe for implementation is dependent upon resources and funding. Initial start up funding has been approved for Risk Assessment and Security Incident Management for FY05.

APA Recommendation 3: VITA use the configuration standards to manage client agencies systems and in cases of potential disagreement, miscommunication or other questions, takes actions to protect the data pending resolution of the matter with the client agency.

VITA Response: VITA will adopt the configuration standards and in cases of potential disagreement, miscommunication or other questions, take appropriate action to protect the data pending resolution of the matter with the customer agency. Such immediate actions will be determined based on a case specific risk assessment. VITA will mitigate the risk of adverse impact to agency business services or operations by working closely with each customer agency. VITA Security will develop a policy and procedure to govern this process and put it in place by October 1, 2004.

APA Recommendation 4: VITA review and correct the Department of Taxation server configuration issues.

VITA Response: The standard that applies to management of this server is based on "Industry Best Practices" and was finalized in December 2003. It was developed jointly by VITA and Taxation. At the time the standard was finalized Taxation elected not to make changes as a result of weighing limited security exposure against business process risk should a failure occur. Taxation's infrastructure has not yet been consolidated into VITA. Steps are underway to completely resolve issues with configuration of the server belonging to the Department of Taxation. Actions have been completed to remove world writable files that would not impact applications and to disable unused network services and other candidate services identified by Taxation. File permissions will be documented and provided to VITA bu the Department of Taxation by August 2, 2004. The server will be managed by VITA in accord with best practice standards and procedures. A joint change management process will be established monthly for ongoing assurance.

We appreciate the valuable work done by APA staff on this audit and look forward to the opportunity for continuing dialogue and guidance from APA as VITA completes the transition of agency infrastructure and moves into the transformational stage of the IT reform initiative.

Sincerely,

Cheryl Clark
Deputy Chief Information Officer

cc: Ben Herman, VITA Audit
Jeff Deason, VITA Security Director
Leslie Carter, VITA Computer Services Director
Jerry Simonoff, VITA Director of Strategic Management Services

OBJECTIVE 1

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

Provided by VITA	**Provided by the Auditor of Public Accounts**	
Policies and Procedures	**Tests Performed**	**Results**
Policies and procedures for physical access involve all VITA divisions and computing environments. The VITA Physical Security Section of the Security Division administers and maintains the physical security program. **New and Current Employees** Purpose: To establish and document the VITA's policy and procedures regarding physical access security. Scope: All VITA employees. VITA uses an electronic security system to protect its premises, which requires access cards to unlock all secured doors. Each access card provides a unique level of access depending on the individual cardholder's requirements. When someone uses an access card, the card displays on the security console. If someone attempts to use a deleted access card, the system will notify the Security Division, and will not allow access to VITA space. Should cardholders encounter problems with their access card, they should notify either the Capitol Police or the Security Division. VITA has three types of identification badges and access cards. 1. Permanent Electronic Card Key – All permanent and part-time employees receive the Permanent Electronic Card Keys (Access Cards). In some cases, vendors, consultants, and maintenance personnel also receive 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 VITA areas based on requested and VITA Management approved access. Card holders must wear visibly the card at all times. The Security Division issues access cards after receipt of the properly completed form, VITA-41. A VITA Branch Manager and a Physical Security Officer approves VITA Access Authorization.	Obtain copies of policies and procedures used to meet the above objective. Inquire as to whether there have been changes to the policy and procedure since the last audit period. Document changes and effect on objective in narrative form. Tour VITA 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 necessary 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 VITA policy. Document reasons for exceptions. 5. Obtain from the Physical Security Officer, two randomly selected access log reports. Do these reports show instances of doors being forced or held open, etc. Determine and document whether security preformed the proper responses and follow-up procedures. 6. Document and evaluate who has control over the access card database and hardware. 7. Document and evaluate if a master	No exceptions were noted.

OBJECTIVE 1

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

Provided by VITA	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Employees should not allow others to follow them through access-card controlled doors unless they are wearing a picture ID (i.e., no tail-gating). The Employee must return the access card to the Security Division upon termination of VITA employment or in the case of vendors, termination of the need for access to a particular area. 2. Temporary Electronic Card Key – Employees and authorized vendors on contract with VITA receive the Temporary Electronic Card Keys (Temporary Access Cards). The Capitol Police keep and issue these temporary access cards kept at the station on the second floor. Cardholders must visibly wear the card at all times. VITA employees who have forgotten or lost their access cards receive a temporary access card after Capitol Police have checked the employee list and checked a photo ID. Capitol Police must keep the employee's Driver's License or other photo ID until the employee returns the temporary access card. Employees without an appropriate badge must ask the Capitol Police for a temporary access card, who reports their names to the Security Division where the name remains on file for one year. If a visitor cannot produce a badge, the employee responsible for the visitor must report to the Security Division, the visitor's name, which remains on file for one year. Security Division review all filed names for patterns of violations and report them to the appropriate Division Director for further follow up.. Capitol Police must check the authorized vendor list and obtain either a driver's license or company ID prior to issuing a temporary access card to a vendor. For security purposes, Capitol Police keep all IDs in a locked box until the return of the temporary access card. Cardholders must return all such access cards before	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 employees 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 nonsystems 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 was necessary in the new policy in order to receive 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 VITA-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 VITA-41. 11. Obtain from Human Resources a list of recently terminated employees. Judgmentally select an appropriate sample of terminated employees and determine if management is following VITA's policy on terminated employees. Request a memorandum from the user's supervisor to the Personnel Branch and a memorandum from the Personnel Branch to the	

OBJECTIVE 1

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

Provided by VITA	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
the individual leaves VITA premises. All persons receiving a temporary access card must sign the VITA Temporary Access Card Sign In/Sign Out Log. 3. Visitor Badge – All visitors receive these badges prior to entering VITA space and do not have access without them. Visitors receive a peel-off badge on which they write their name and date and must affix to the front of the chest area. VITA reception areas and the Capitol Police area can issue visitor badges. Visitors attending a function in the VITA auditorium or classroom area do not need a visitor badge. All visitors to VITA must register by signing the Visitor Sign In/Sign Out Log located at one of the reception areas (Third Floor Reception area, Telemedia, Telecommunications, Acquisition Services, Security/Partnership, DTP, or Capitol Police) The visited VITA employee must escort the visitor to the appropriate area. The VITA 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 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,	Security Office. Determine that both notifications were timely and there was a timely denial of access. 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 timely access termination. 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 had training for emergency responses. Review a testing of the Uninterruptible Power Source (UPS). Verify that controls are still in place.	

OBJECTIVE 1

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

Provided by VITA	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
physical access to VITA 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 must provide the supervisor of the terminating employee with a Separation Checklist to ensure that employee returns all assets assigned to the individual on or before the employee's termination date. The supervisor should use the checklist as an aid in determining employee assets. Security has copies of the separation checklist. Once Security receives notification of a termination, it produces a list of the employee's system access record from the Security Tracking System and provides this to the supervisor to aid in completing the Separation Checklist. To further assist supervisors, Security must 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 it has received the appropriate paperwork. Security coordinates its activities with Finance to recover physical assets, if necessary. **Transferred Employees** For transferred and promoted employees, the Personnel Branch notifies Security and Finance of the change in status by providing them with a Payroll Transaction/Authorization Form. Upon notification, Security produces the employee's system access record from the Security Tracking System and provides 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.		

OBJECTIVE 1

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

Provided by VITA	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
Security must 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 VITA, 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 the supervisor receives all assets assigned to the individual on or before the contractor's termination date. The supervisor should use the checklist as an aid in determining contractor assets. Security has copies of the Separation Checklist. 3. To further assist supervisors, Security must provide them with the paperwork to delete contractor's access to selected systems and obtain assigned physical assets. Security automatically suspends the contractor's system access on the contractor's last day, regardless of whether the supervisor has filed the appropriate paperwork. Security coordinates its activities with P&SS to recover physical assets, if necessary. 4. Once P&SS knows of a termination, it coordinates its activities with the supervisor to ensure the contractor accounts for all fixed assets assigned to the contractor. If the contractor can not account for the fixed asset(s) (including		

OBJECTIVE 1

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

Provided by VITA	Provided by the Auditor of Public Accounts	
Policies and Procedures	**Tests Performed**	**Results**
those physical assets managed by Security), P&SS will take the appropriate steps to recover the value of the asset (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 must retrieve the contractor's badge and any keys and turn them in to the appropriate area.		

OBJECTIVE 2

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 VITA Computing Environments** VITA has established a program to ensure the confidentiality, availability, and integrity of the data VITA 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 VITA systems, VITA follows the procedures below. **Logical Access to Programs** VITA establishes user accounts in the operating system. The operating system default under both MVS and UNISYS grants access to all programs. To mitigate this weakness, VITA 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. VITA 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. VITA recommends, but cannot mandate that user agencies use these security features. If a user agency does not use one of the security options, then other UNISYS users have free access to the computer programs and data. **Logical Access to Data** MVS Computing Environment for	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 VITA personnel is restricted to authorized individuals, obtain a computer-generated printout of the Logon ID File (for VITA) 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 (VITA03-001). 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 testing in Objective 1, verify the deletion of the Logon IDs in a timely manner. Obtain from VITA’s ACF2 officer the names of all ACF2 rules datasets. Determine that all VITA-controlled rules datasets are restricted to the security officer and an alternate. Using the Logon ID report, document	No exceptions noted except for Department of Taxation Unix review. See objective 6 for comments.

OBJECTIVE 2

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***
VITA Employees and User Agencies Each user agency (including VITA) 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, VITA Security Officer, System Coordinator, and Direct Access Storage Device Coordinator must sign the form indicating approval. VITA'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 VITA's Security Division contacts the Agency Security Officer. UNISYS Computing Environment for User Agencies Each user agency must select a UNISYS sub-administrator and send a letter to VITA indicating the sub-administrator's name to have the appropriate security features established. VITA does not set up access for any of the user agency's employees except the sub-administrator. The individual user agency implements procedures for setting up end-user logon ID's and privileges. UNISYS Computing Environment for VITA Employees All VITA 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. VITA-designated personnel receive all special requests with written	and evaluate based on job function those VITA 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 VITA10-001 request form for each of those users. Determine that the Agency Security Officer, the VITA Security Officer, the System Coordinator, and the DASD Coordinator have signed it. Determine what reports the security officer runs, how often; what information undergoes review, what are the results of the review, and their effectiveness in controlling access. Document and evaluate who can 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 (VITA10-001) for three agencies that use the UNISYS. Determine that the agency's MIS Director sent a signed request letter with a properly completed request form before granting of access. Evaluate and document how many VITA personnel can access the User ID Maintenance screen by using the VITA SIMAN Administrator sign-on. This access allows for adding deleting or	

OBJECTIVE 2

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***
justification, the signature of the end-user, and the end-user's supervisor before setting up the logon ID in accordance with the request. UNIX Computing Environment for VITA Employees and User Agencies The Department of Social Services (DSS) owns the E10000 located at and administered by VITA. 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 VITA via e-mail to request access for an end-user in accordance with the form. DSS users have access only to those applications that they need and not blanket access to the E10000. Other UNIX-based equipment housed at VITA on behalf of agencies not transiting to VITA do not rely on VITA logical access controls. Agencies locate these servers at VITA for the physical security, environmental controls, and logistics reasons, but retain responsibility for administrating the equipment. Logical Access to Programs and Data through VITA Firewalls The security firewall is a combination of hardware (SUN SPARC workstations) and software (CISCO PIX, Raptor Systems, Incorporated) designed to provide a security barrier by blocking external networks from accessing VITA's computer environment, which includes the MVS and UNISYS systems. The Agency Security Officer requests access to the VITA firewall by contacting the VITA Help Desk and completing and signing a Firewall Access IBM or Firewall Access UNISYS form. The VITA 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.	changing an agency's Sub Administrator's capabilities. Review the UNISYS request form (VITA10-001) of three VITA 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 VITA has informed them that access security is their responsibility. Document and evaluate who has use the scheduler functions for adding, deleting, or changing scheduling related information. **Firewalls Note:** Completed testwork on VITA's firewalls through performing a penetration test, as documented in the appendix for objective four. See that appendix for details on the tests performed. Document in detail the firewalls used at VITA that control access from agencies and the outside world. Determine from interviews with key staff, what reports the firewall generates and how often someone reviews them. 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 (VITA03-004). Determine that user had a correctly completed form with the proper authorizations. Review firewall events from the system logs. Judgmentally select a sample of 5 events and determine what action VITA 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	

OBJECTIVE 2

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***
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. VITA has established procedures for each of these additional services. **User Agency Control Considerations** User agencies must establish, maintain, and monitor procedures for logical access to resources located at VITA. This includes appropriate procedures for authorizing who can access user applications and at what level, and controlling who can modify user access. Agencies have responsibility for giving access, including to VITA personnel. This audit did not review the appropriateness of agency employee access, other than VITA personnel. **DSS SUN E10000** **User Accounts** The VITA Unix Branch manager or Department of Social Services' security manager must authorize user accounts 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 must 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 VITA 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	authorization. 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: 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	

OBJECTIVE 2

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***
immediate supervisor or manager and directed to the VITA 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 VITA UNIX branch manager or DSS security manager must authorize root accounts. Individuals do not typical receive root accounts unless there is a defined need for root access. Users who require root access for specific functions normally receive root privilege for only those specific items through sudo configuration. The VITA UNIX system security administrator(s) maintains the sudo configuration. **File protections** Files created by user accounts default to 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)	/users/$HOME/.rhosts files. These files tell who is trusted by the mere fact that the user is trusted somewhere 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: 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	

OBJECTIVE 2

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***
• . 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 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 Unix system administrator(s) responsible for maintenance determines the applicability of the need for a patch. Assisting the system administrator(s) are their knowledge of the software and hardware components and previous experience. Sometimes recommended patches do not apply specifically to the E10000 and the hardware platform will not support the patch. Other recommended patches do not apply because they are fixes to products 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, The Unix system administrator(s) responsible for maintenance will apply the patches and will determine whether a vendor's correction applies to an encountered problem. The Unix system administrator(s) responsible for maintenance stages patches that apply to all customer	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 run at startup and other times. Determine that only the owner can write to these jobs. 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 /dev directory has all device files listed and there is protection for the directory. 10. Obtain a list of files that are set as SUID / SGID which allows users to achieve capability of the owner of that	

OBJECTIVE 2

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 on the test and development systems first, then moves them to the production domains. The initial domain to receive software patches is the VITA test domain. After running on the VITA test domain for a minimum of two weeks without incident, personnel apply the patches next to the customer test/ development system. After running on the customer test/development system for a minimum of two weeks without incident, personnel apply the patches 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. Data owner should keep backups of mission critical data 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** The Department of Taxation manages its servers under similar policies as the E10000 owned by the Department of Social Services.	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. **TACACS Server** Determine if VITA is currently using TACACS, XTACACS, TACACS+, or RADIUS for remote user authentication. (The TACACS and XTACACS protocols in CISCO IOS software are no longer 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 their projects and platforms assignments. Determine that Security removed their access from these platforms 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	

OBJECTIVE 2

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***
	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 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.	

OBJECTIVE 2

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***
	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 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 3

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 VITA of the data files and application programs to store offsite. **MVS, UNISYS, and UNIX Backups** VITA backs up all data files and application programs that reside on shared disk packs nightly (Sunday through Friday, except holidays) at midnight. VITA 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, VITA uses an Enterprise Backup and Recovery System with Veritas software and DLT7000 tape drives housed in an automated tape library. VITA is reviewing technology for backing up this data to direct access storage devices. The VITA scheduling group enters the backup, offsite storage, and retention time requests made by user agencies and in-house divisions into an automated system. VITA maintains the latest disk file backup tapes at the data center for on-request file restoration. As part of VITA's disaster recovery plan, the offsite storage facility retains the two previous backup tapes. **Offsite Storage** VITA contracts with Iron Mountain for offsite storage and sends a courier to pick up new and return old tapes. VITA personnel perform an offsite storage inventory of the tapes monthly. If there is a discrepancy, VITA personnel determine its cause. VITA uses a robotic tape library to	Obtain from two different agencies in the MVS environment a list of off-site tapes. 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 off-site tapes. 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 offsite, 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 VITA 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 VITA'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 VITA has made for getting 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 3

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***
manage the MVS tapes. The robots pull the tapes for offsite storage and MVS librarians scan the tapes to ensure the shipment of the correct tapes. A bar code helps VITA employees perform the same function for UNISYS and UNIX tapes. **User Agency Control Considerations** User agencies need to communicate to VITA 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 4

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

Provided by the Department	***Provided by the Auditor of Public Accounts***	
Policies and Procedures	***Tests Performed***	***Results***
VITA provides several modes of communications such as dial-up, dedicated lines, and a telecommunications network. Our focus for this objective is the COVANET, which is the backbone carrier user agencies employ for their private network. The user agency contacts VITA to establish the proper connections and can use frame relay, PVC (Point Virtual Circuit), or a telephone line on the COVANET to send data. VITA 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 VITA. VITA takes no security responsibility for these lines. VITA has one main router 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 VITA. The network security division at Virginia Polytechnic Institute configures the security controls on the Network Virginia gateway router. VITA configures its router to allow traffic coming in from the Internet to only access VITA's web page and the DNS server that provides various state agency home page information. The router table configuration includes an access list of users that need to access the mainframe systems at VITA through COVANET and Network Virginia. The access list is a security feature programmed into the router using Internet Protocol (IP) addresses. Only user agencies using the specified IP address can gain access through the router. Though these users can pass through the router, they must also go through an authentication by the firewall	Document in detail the communications environment that surrounds the VITA to agency interface. Specifically account for: 1. COVANET 2. Frame relay circuits 3. Point to Point dedicated circuits 4. Analog dial-up lines Note: We use network penetration testing to perform all tests noted below. Penetration testing provides positive assurance that the controls are functioning as designed, and implicitly, rather than explicitly tests each of the controls noted below and those noted in the tests of firewalls in the appendix for objective two. 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 VITA 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	No exceptions were noted.

OBJECTIVE 4

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

Provided by the Department	***Provided by the Auditor of Public Accounts***	
Policies and Procedures	***Tests Performed***	***Results***
before they can access the MVS, UNISYS, and UNIX mainframe systems. User agencies must formally request access to the VITA firewall (see further explanation at the LOGICAL ACCESS Control Objective). Upon user agency request, VITA will establish or configure routers physically located at the user agency. The Help Desk handles these requests by initiating a ticket to complete the work. **User Agency Control Considerations** User agencies need to communicate to VITA the criticalness and level of sensitivity of connections from the user to VITA, so that VITA 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 VITA are the user agency's responsibility to control. Firewalls at VITA protect the MVS, UNISYS, and UNIX systems and the VITA local area network located at the VITA data center. These firewalls do not provide security for user agency internal networks. User agencies have responsibility for the proper control of those networks.	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 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 VITA offices and data center and look for analog lines connected to systems equipment. Determine the need for such lines and their security. Determine if VITA 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 VITA and the CTN handle such an event. Document how VITA provides incoming and outgoing Internet services for other agencies. Determine if this function is secure for VITA and whether the VITA firewall protects agencies from any Internet-based threats. Investigate and document the extent of cooperation between VITA 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 5

Policies and procedures provide reasonable assurance that Virginia Information Technologies Agency 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** VITA has completed a Business Impact Analysis. The Business Impact Analysis only covers systems that affect VITA's business, not customer applications. VITA sent a questionnaire to each VITA Division Director and VITA Project Leader requesting they identify their critical systems and the resulting impact if the system was not operational for a period of time. VITA compiled the information into the Business Impact Analysis and the VITA 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** VITA uses a risk assessment software package called RISKWATCH. VITA staff conduct risk assessments at least every two years or as major system changes occur to determine whether measures exist to counteract threats to assets under VITA's control. VITA'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	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 VITA added this new system 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 VITA policy requires. Review the contingency plans for VITA and evaluate for reasonableness. Consider time frames, the percentage of operations restored and brought online, and the effect on the state agencies that rely on it. Request, from the Contingency Plan Administrator, three of the VITA-required quarterly division updates from the Disaster Recovery Coordinators. Determine that they exist or if they made no changes that an email went to the Contingency Plan Coordinator. Make an inquiry to SunGard (VITA's hot site vendor) and determine that they maintained knowledge of any critical changes to the contingency requirements. Obtain a schedule and proof that tests had occurred of the "hot site" scenario for both the MVS and UNISYS environment. Obtain the names of five recently hired VITA employees and request to see their signed Information Security Agreement. Obtain the training attendance logs for the VITA Systems Security personnel. Determine that they have taken courses in the last year on security related	No exceptions were noted.

OBJECTIVE 5

Policies and procedures provide reasonable assurance that Virginia Information Technologies Agency 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***
vulnerabilities of service areas to potential threat, estimating the loss potential of a service area, and developing proactive countermeasures to reduce business loss. VITA 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 VITA have a contingency management plan, which VITA'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. VITA 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. VITA tests the restoration of the systems and data at these hot sites regularly. Annually, the contingency plan administrator requests that user agencies provide a list of critical applications	topics. Verify that all VITA employees have had security awareness training	

OBJECTIVE 5

Policies and procedures provide reasonable assurance that Virginia Information Technologies Agency 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***
processed by VITA 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 VITA Configuration Review Committee communicates the plan changes to SunGard. **Security Awareness/Training Program** Human Resources and Security require that new employees read VITA Directive 92-1 - System Access Control and sign an Information Security Access Agreement. This agreement details the proper use of employee access to VITA systems. If the new employee will have Internet access, they must sign an Internet Use Form. VITA does not have any formal procedures for security awareness/training for existing employees. The Security Division sponsors a Computer Security Day annually. VITA 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. VITA 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		

<u>***OBJECTIVE 5***</u>

Policies and procedures provide reasonable assurance that Virginia Information Technologies Agency 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***
that they also conform to SEC2001-01.1. The development of these policies and procedures should consider VITA's relationship to the user agency and the services VITA provides. Some agencies to use VITA's data center as a site to house their various servers. With the exception of the E10000, each respective agency administers these servers and VITA does not include them in the contingency plans. VITA, however, is willing to work with each agency to determine if VITA can provide contingency services through either SunGard or other means such as off-site mirrored servers. Each agency must determine if these servers fall under a contingency plan. If the agency does not have an agreement with VITA, the agency needs to have backup routines and fallback plans in case of a disaster in the data center.		

OBJECTIVE 6

Policies and procedures provide reasonable assurance that the VITA 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 or Public Accounts*	
Policies and Procedures	*Tests Performed*	*Results*
VITA has established a Memorandum of Agreement (MOA) to establish mutually agreeable levels of service between VITA and the agency requesting use of the server farm. VITA will provide the system access control mechanisms through which the customer will secure its data residing on the customer system. VITA, as custodian of the data, will ensure that this data is not available to other users without authorization by the customer. VITA restricts access to the data center to authorized personnel. Customers can arrange access to the hardware upon request through the current data access policy. Customers requiring access authorization must contact the VITA point of contact. VITA 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 VITA help desk and Network Control Center • Network infrastructure configuration and management of the VITA internal LAN, switches, routers, and WAN. **Disaster Recovery Services** Disaster Recovery Services for the customer-owned hardware are optional. If VITA provides these services, they cover this service in the customer's MOA. VITA will produce and store system backup tapes in a vault off	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 VITA 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	Improve and Implement Security Standards for Client Agencies During our audit we found improper security configurations, such as risky services enabled and improper file permissions, on a Department of Tax (TAX) server managed by the Virginia Information Technologies Agency (VITA). Tax gave VITA a UNIX Standard to follow for managing their UNIX servers; however, VITA is not following this standard. The above is symptomatic of a much larger issue as VITA absorbs more responsibility for the Commonwealth's computing architecture. VITA has developed generic Memorandum of Agreements (MOAs) for servicing their client agencies. These agreements do not specifically address information security concerns other than to state that VITA, as custodian of client's data, will ensure that the data is not available to unauthorized users. The lack of detailed security information in the MOAs, requires VITA to take steps to avoid miscommunication of roles and responsibilities of each party. We recommend

OBJECTIVE 6

Policies and procedures provide reasonable assurance that the VITA 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 or Public Accounts***	
Policies and Procedures	***Tests Performed***	***Results***
site as requested by the customer. VITA will be responsible for: • Assigning a VITA primary point of contact who accepts requests for installation, modification, and/or removal of major systems hardware and software. • Responding to day-to-day operational issues reported through the VITA Help Desk, who will assign a ticket number to track the call. • 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 • Database Management and Administration • Application Problem Management • Application Change Management	(Determine the type of H.V.A.C. system. Is the data center air conditioning separate from the building system? Does the system have sufficient cooling integrated into the building?). • 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 VITA 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 VITA is providing for the client's server. 8. Determine if agencies have physical access to their servers. Evaluate the controls in place for protecting each agency server from access by someone from another agency. 9. Determine if secured configuration/repair areas exist for the server farm. List the number and experience/certification level of technicians on site for maintenance and updates to the server farm.	VITA take the following actions to ensure the security over the Commonwealth's systems. • VITA creates and distributes to the client agencies a detailed checklist that defines the roles and responsibilities for information security. • VITA creates or defines the "Industry Best Practices" for detailed security configuration standards in our computing environment to include configurations at the operating system level, database level, and network component level. • VITA uses the configuration standards to manage client agencies systems and in cases of potential disagreement, miscommunication or other questions, takes actions to protect the data pending resolution of the matter with the client agency. • VITA review and corrects the Department of Tax server configuration issues.

OBJECTIVE 6

Policies and procedures provide reasonable assurance that the VITA 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 or Public Accounts***	
Policies and Procedures	***Tests Performed***	***Results***
The customer security officer will ensure all users have proper User IDs, Logons, and Passwords for the use of their systems.		