REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS FOR THE COMMONWEALTH OFFICE OF TECHNOLOGY

For the Period July 1, 2005
through June 30, 2006

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS
www.auditor.ky.gov

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE (502) 573-0050
FACSIMILE (502) 573-0067

CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
John Farris, Secretary
Finance and Administration Cabinet
Mark Rutledge, Commissioner
Commonwealth Office of Technology

The enclosed report prepared by Crowe Chizek and Company LLC, Certified Public Accountants, presents the report on controls placed in operation and tests of operating effectiveness for the Commonwealth Office of Technology for the period July 1, 2005 through June 30, 2006.

We engaged Crowe Chizek and Company LLC to perform the SAS 70 audit of the Commonwealth Office of Technology. We worked closely with the firm during our report review process.

Respectfully submitted,

Crit Luallen

Crit Luallen
Auditor of Public Accounts

Enclosure

Commonwealth
Office of Technology

REPORT ON CONTROLS
PLACED IN OPERATION AND
TESTS OF OPERATING EFFECTIVENESS

For the Period July 1, 2005
Through June 30, 2006

Prepared by:

Crowe

Crowe Chizek and Company LLC
http://www.crowechizek.com

Commonwealth
Office of Technology

Commonwealth of Kentucky
Commonwealth Office of Technology

Frankfort, Kentucky

REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

**For the period July 1, 2005
Through June 30, 2006**

Table of Contents

Crowe

REPORT OF INDEPENDENT ACCOUNTANTS

Commonwealth of Kentucky
Commonwealth Office of Technology
Frankfort, Kentucky

We have examined the accompanying description of controls related to the systems of the Commonwealth Office of Technology (COT) located at the Commonwealth Data Center on Cold Harbor Drive in Frankfort, Kentucky. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of COT's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of COT's controls, and (3) such controls had been placed in operation as of June 30, 2006. The control objectives were specified by the Auditor of Public Accounts in conjunction with the COT. 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 presents fairly, in all material respects, the relevant aspects of COT's controls that had been placed in operation as of June 30, 2006. Also, in our opinion the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the internal controls contemplated in the design of COT's controls relating to the systems at COT.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Appendix A, to obtain evidence about their effectiveness in meeting the control objectives, described in Appendix A, during the period from July 1, 2005 to June 30, 2006. The specific controls and the nature, timing, extent, and results of the tests are listed in Appendix A. This information has been provided to user organizations of COT and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations.

In our opinion the controls that were tested, as described in Appendix A, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Appendix A were achieved during the period from July 1, 2005 to June 30, 2006. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Appendix A were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Appendix A.

The relative effectiveness and significance of specific controls at COT and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls at COT is as of June 30, 2006 and information about tests of the operating effectiveness of specified controls covers the period from July 1, 2005 to June 30, 2006. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls at the COT is subject to inherent limitations and, accordingly, errors or fraud 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.

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

Crowe Chizek and Company LLC

South Bend, Indiana
June 30, 2006

GENERAL CONTROLS

General Controls are those policies, procedures, and safeguards that relate to all internal information system activities. Their purpose is to ensure the continued, consistent, and proper functioning of information systems by controlling, protecting, and maintaining application software and computer operations. These controls are divided into the following areas:

- Organization Structure and Personnel
- Application Maintenance and Documentation
- Systems Software and Hardware
- Physical Security
- Contingency Planning
- Mainframe/UNIX/Windows
    - Operations and Scheduling
    - Security
    - Output Data Distribution
    - Backups and Recovery
- Infrastructure Support

It should be noted that, if these areas are not segregated, they can overlap to affect all information systems activities. As a result, the adequacy of these controls is considered fundamental to the effectiveness of specific applications, and weaknesses within these General Controls can have pervasive effects that are detrimental to many applications.

Organization Structure and Personnel

During the 2005 Legislative Process, Senate Bill 49 changed the name of the Governor's Office for Technology to the Commonwealth Office of Technology (COT), and transferred it from the Office of the Governor to the Finance and Administration Cabinet. COT is responsible for providing leadership, policy direction, and technical support to executive agencies of state government in the application of information technology. The Commonwealth Office of Technology, under the direction of the Commissioner, is composed of four offices. These are outlined below.

The *Office of the Commissioner* is responsible for enterprise policy direction and the general management of COT. COT's mission is to provide leadership in the use of information technology to enhance government services, improve decision making, promote efficiency and eliminate waste. The Finance and Administration Cabinet's Office of the General Counsel provides all legal services to COT and advises the Commissioner on the legal implications of information technology policy as it relates to government operations.

The *Kentucky Information Technology Advisory Council (ITAC)*, attached to the Office of the Commissioner, is responsible for advising the Information Technology Officers on approaches for coordinating information technology solutions among libraries, public schools, local governments, universities, and other public entities. Also, to provide a forum for the discussion of emerging technologies that enhances electronic accessibility to various publicly funded sources of information and services. The Council consists of members that are either appointed or serve by virtue of an office. No member receives compensation, but is reimbursed for actual and necessary expenditures in accordance with travel and subsistence requirements established by the Finance and Administration Cabinet.

KRS 11.5163 was amended with the passage of HB226 during the 2004 General Session to include the *Kentucky Wireless Interoperability Executive Committee*. This committee is attached to the Office of the Commissioner and is responsible for the evaluation and recommendation of all wireless communications architecture, standards, and strategies.

All state agencies in the Commonwealth shall present all project plans for primary wireless public safety voice or data communications systems for review and recommendation by the committee, and the committee shall forward the plans to the Commissioner for final approval. Local government entities shall present project plans for primary wireless public safety voice or data communications systems for review and recommendation by the Kentucky Wireless Interoperability Executive Committee.

The committee shall develop funding and support plans that provide for the maintenance of and technological upgrades to the public safety shared infrastructure, and shall make recommendations to the Commissioner, the Governor's Office for Policy and Management, and the General Assembly.

The *Office of Enterprise Policy and Project Management* is responsible for long-term capital IT planning and project management of IT work within the Executive Branch. The Office of Enterprise Policy and Project Management consist of three (3) divisions:

- The Division of Enterprise Project Management supports the greater Project Management community within the Executive Branch through Project Management procurement, mentoring, training, and other resources or services pertinent to this skill-set.
- The Division of Enterprise Program Management is responsible for providing oversight and management to large, multi-project undertakings such as the Uniform Criminal Justice Information System (UCJIS).
- The Division of Geographic Information collects, compiles, and facilitates the production of geospatial data for the Commonwealth. It is this Division's responsibility to be an active voice in leading the direction of GIS across state government through cabinet and agency engagements as well as participation in the Kentucky Geospatial Board.

The *Office of Infrastructure Services* is responsible for the operations of the enterprise computing environment. This Office includes the daily operations of the Commonwealth Data Center, operation and maintenance of the Kentucky Information Highway, all communication services, including data, voice, video and wireless, and securing the infrastructure. Other responsibilities include: network planning, design, and management, help desk assistance to end users, desktop support, systems administration, research and evaluation of desktop and departmental computer technologies, server administration, technical support for data center servers, change management, end-user computing support, computer operations, systems programming, data storage, and problem management. This office is also responsible for the physical security of the Commonwealth Data Center, as well as four other COT buildings. It is also responsible for disaster recovery planning activities.

The Office of Infrastructure Services consists of six (6) divisions:

- The Division of Communications maintains network and security services.
- The Division of IT Operations **c**oordinates change management, maintenance, and day-to-day operations of existing infrastructure services.
- The Division of Client Services operates the help desk and manages enterprise-wide customer support.

- The Division of Technical Services is responsible for system software, operating system support, and data maintenance.
- The Division of Field Services is responsible for telephony support for state agencies and the Kentucky Wireless Interoperability Network System (KYWINS). In addition, the division supports KYWINS in the field and IT operations, where appropriate – to include network administration and on-site PC maintenance and repair throughout the Commonwealth.
- The Division of Printing Services manages copy and print services for the Commonwealth, and is the result of the transfer of responsibilities from the previous Division of Printing within the Office of Administrative Services within the Finance and Administration Cabinet.

Additionally, this Office has the responsibility for maintaining the state's Kentucky Emergency Warning System (KEWS), which is a completely redundant microwave network with over 150 towers that span the Commonwealth.

The *Office of Application Development* is responsible for providing comprehensive systems analysis, design, and development services, and application/consulting services to designated state agencies. This Office provides cost-effective application systems support to state programmatic agencies. Successful attainment of agency service requirement necessitates utilization of a broad and variable spectrum of information systems technology, to include: automation of new services, integration of diverse management systems, and enhancement of existing systems. This Office is responsible for the analysis, design, development, and maintenance of systems related to the administration and collection of Kentucky taxes; systems related to the management of state government, including personnel and financial management systems; systems related to a variety of activities within the Transportation Cabinet; systems related to the registration and titling of vehicles and boats; systems related to the licensing of drivers within the Commonwealth; systems related to the education and training of adults, and all systems which support the business requirements of the Justice and Public Safety Cabinet, Environmental and Public Protection Cabinet, Commerce Cabinet and other agencies within the Executive branch who request assistance. The Office of Application Development consists of four (4) divisions:

- The Division of Portfolio Management is responsible for the Commonwealth's IT application development.
- The Division of Data Architecture Services is responsible for the development and support of data integration and data warehouse environments.
- The Division of Support Services is responsible for quality control and testing.
- The Division of Consulting & Project Management is responsible for gathering of requirements, business and technical analysis, prioritization, co-ordination and management of system application projects.

In 2005 this office completed a major reorganization of divisions which allowed the organization to be functionally based.

Policies and Procedures

Employee Policies

Within the Commonwealth Office of Technology, executive directors and division directors are responsible for the development and maintenance of technical policies, procedures, standards and forms for the Commonwealth Office of Technology.

COT Employees/contractors are required to complete and sign form COT-F015 - Acknowledgement of Responsibility, which requires a COT employee to accept the responsibility to protect the confidentially and integrity of all Commonwealth of Kentucky data. This responsibility is inclusive of systems and software that the Commonwealth owns, develops or acquires from third parties. This policy requires that COT employees abide by all COT/Enterprise policies and procedures. Further, it requires all hardware, software and data that a COT employee accesses to be used in the performance of assigned job duties. Any violation to the above statements is subject to disciplinary or legal action by the Commonwealth of Kentucky under KRS Chapter 434.840-855.

For contracted personnel, COT-F011 – Acknowledgement of Confidentiality Agreement outlines the responsibility of the contractor/vendor regarding the confidential nature of access to the Commonwealth of Kentucky's data resources. All contracted personnel are required to read and sign this form. The contractor shall be granted access to agency documents, records, programs, files, and any pertinent data resources as needed and shall maintain confidentiality and data integrity of these data resources. The contractor agrees that all developments made and works created by him/her shall be the sole and complete property of the Commonwealth of Kentucky and all copyright and other proprietary interest shall belong to the Commonwealth of Kentucky. Violations of this agreement will result in immediate termination of the contractor/vendor. Upon termination of the contractor/vendor, all forms of data resources and any copies will remain with COT.

Other policies exist which set guidelines for purchasing (COT-031 - Discretionary Purchases & Payments and COT-061 - Procurement Card Program), asset management (COT-024 - Acquisition of Surplus Property and COT-055 - Shipping and Receiving), personnel (COT-026 - Employee Time Reporting and COT-043 - Employee Performance Evaluation), travel (COT-021 - Travel & Travel/Training), consulting (COT-016 - Task Order Agreement for Contractor Programming/Analyst Services and COT-011 - Systems Life Cycle Methodology), customer relations (COT-015 - Communications Standards and COT-014 - Customer Request for Professional Services) , and end-user support (COT-008 - Change Management Policy).

Security Policies

The Security Policies and Procedure Manual (SPPM) was revised in November 2002 and distributed to all COT staff. The manual is available on GOTSource. Recently this document has been formatted into sections to allow for easy updating and distribution. The formatting also allows for selected sections to be extracted and distributed to COT customers. In addition, security policy tip documents were prepared that provided a summary of many of the COT security policies. The policy tip documents were customized for three different audiences: COT All, COT managers, and the COT application developers.

The following manuals were updated in July 2004, which are available on GOTSource: Security Administrator Manual for Microsoft Windows NT, Security Administrator Manual for Microsoft Windows 2000, Security Administrator Manual for UNIX (AIX), Security Administrator Manual for UNIX (Solaris), and the pcAnywhere Configuration Guide. A new Security Administrator Manual for Microsoft Windows 2003 was developed and implemented in July 2004, and the Administrator Manual for z/OS was implemented in November 2003.

COT initiated the development of enterprise policies that specifically relate to security.

The policies have been approved by the CIO Advisory Council and the Enterprise Architecture and Standards Committee. Some of the policies are:

- Revised Internet and Electronic Mail Acceptable Use Policy (CIO-060). Revised November 2005.
  http://www.gotsource.net/dsweb/Get/Document-5282/AUP_1-20-2000.doc

- Network Security Architecture Policy (CIO-074)
  http://cot.ky.gov/NR/rdonlyres/EAD860BF-157F-494C-A81B-EF9121DC8743/0/COT067.doc#CIO_074

- Wireless LAN Policy (CIO-078)
  http://gotsource.ky.gov/dsweb/Get/Document-21536/CIO-078%2B--%2BWireless%2BLAN%2BPolicy.doc

- Logon Security Notice (CIO-079)
  http://gotsource.ky.gov/dsweb/Get/Document-35941/CIO-079%2B--%2BLogon%2BSecurity%2BNotice.doc

- Password Auditing and Policy Enforcement for Network Domains (CIO-080)
  http://gotsource.ky.gov/dsweb/Get/Document-35938/CIO-080%2B--%2BPassword%2BAuditing%2Band%2BPolicy%2BEnforcement%2Bfor%2BNetwork%2BDomains.doc

- Securing Unattended Workstations (CIO-081)
  http://gotsource.ky.gov/dsweb/Get/Document-35939/CIO-081%2B--%2BSecuring%2BUnattended%2BWorkstations.doc

- Critical Systems Vulnerability Assessments (CIO-082)
  http://gotsource.ky.gov/dsweb/Get/Document-37850/CIO-082%2B--%2BCritical%2BSystems%2BVulnerability%2BAssessments.doc

Strategic Planning

The 2003-2007 Direction of Enterprise Information Technology describes the IT vision of the Commonwealth to "Enable Excellence in Government Services." It outlines a strategy that stresses development of a Commonwealth enterprise-wide application of IT and a focus on the customer - the citizens of Kentucky. This vision emphasizes using IT as an enabler in business processes, recognizing that information is a strategic resource and electronic access to information and services must be provided while maintaining privacy and security. It replaces the Commonwealth of Kentucky Strategic Information Technology Plan (SITP), which was adopted by the KIRM Commission on July 1, 1997 that was originally supported by the EMPOWER Kentucky Initiative. When the KIRM Commission was abolished, the responsibility for review and maintenance of the SITP was transferred to the Commonwealth Office of Technology.

Application Maintenance and Documentation

1. Request for Services

All requests for new applications or changes to existing applications are received on an appropriate request form. This is formal authorization for requesting work. Prioritization of the request is completed at the agency level. If COT is unable to support a request or meet requested completion dates due to resource constraints, some prioritizing will be done in conjunction with the agencies.

COT Internal Systems follow the Management of Internal Systems Policy (COT-101). In this policy the section "New Systems/Systems Service Requests" outlines the authorization requirements for work date and request tracking number associated with the work being completed.

2. Perform Requested Work

Developers make software changes, noting a description of the modifications in comments within the source code or as a separate "Read Me" document when appropriate. The comments include the date and request tracking number associated with the work being completed.

3. Validate Requested Work

Developers test the software modifications. The complexity and the extent of the testing will depend on the nature of the software change, the importance of the modifications, the application environment and other factors. In all cases written approval will be obtained from the user that the software is acceptable before initiating the process to promote new or modified software to production.

4. Promote to Production Environment(s)

Step a: Once user approval is received to promote the software to production, COT initiates the process to move the new/modified software into production. COT initiates this move by completing a production cut over form. This form will tie the move to the tracking request number in step 1 above.

Step b: COT OAD management signs the production cut over form approving the movement of the software into production. During the fall of 2004, an additional step was added that required the director's and/or designee's written approval before the Librarian promotes the software to production.

Step c: The Librarian promotes the software to a designated staging area. The staging area could be on the mainframe, on a production server at Cold Harbor, on a server at the user agency, or in a secured area on an OAD development/test server. The staging area directory/path/folder will have access restricted to the Librarian and Operations staff. The Librarian signs the production cut over form, documenting that the software has been moved to the staging area and is ready for movement to production.

Step d: Operations staff promotes software from the staging area to production. Access to the production area is restricted to Operations staff. When a DBA is serving as operations staff, they may move or apply database resident application code directly from the development/test server or from the database staging area to the production area.

Step e: The requesting agency is notified that COT has promoted the software to production and the new software is operational. COT maintains documentation for each promote.

5. Request Close Out

After all the requested work per Customer Request for Professional Services form (COT-F001) or equivalent in step 1 above is completed and moved to production, see COT policy COT-014 steps 5-7 for close out procedures

Access to Production Files

In order to resolve production problems, developers may need access to production files. This access will be approved, in writing for a specific duration, by COT management and the user agency. Periodically, COT management review staff access levels to production files and program cut over practices to ensure compliance with policy.

Systems Software and Hardware

Changes/Implementation/Documentation

Mainframe

The Systems Software Branch is responsible for all system software upgrades and ongoing maintenance of system software. Systems programmers follow System Support Software Life Cycle procedures maintained online by Systems Software Branch staff. Upgrades, changes, and testing are scheduled through the change control process. The manager of the Systems Software Branch assigns software products to the selected individuals who maintain each product. Local modifications of system software by technical staff are not permitted unless specifically authorized by the manager of the Systems Software Branch. Testing of systems software is usually conducted in the Systems Software Branch Test LPAR (Logical PARtition) region rather than in one of the two production LPARs. A full system backup is performed prior to any changes to system software being moved to production. The Systems Software Branch using IBM’s SMP software maintains all documentation regarding system software releases. This software stores detailed documentation regarding release levels and maintenance levels for system software. As new maintenance is installed, an assigned Systems Software employee updates a list of software titles and version numbers that is available to user agencies through the Systems Software Branch web site. Product manuals and documentation are usually stored online using IBM's BookManager product. The change control process also maintains a historical record of system changes.

Windows

All system changes are implemented according to the COT change control process wherein changes are submitted to change control by Wednesday morning and reviewed during the change control meeting on Wednesday afternoon. Emergency changes can circumvent this process but must be approved in advance by the Operating Systems Branch Manager and change control staff. When possible all changes must be applied to test servers and given the appropriate time for the users to test. Security changes, unless emergencies will be applied to the test servers between the 15th and 20th, and applied to the production servers on the first weekend of the month. Users will be notified and are encouraged to test changes after the fixes have been applied. "Emergency changes" must be approved by the manager of the Operating Systems Branch and then processed through change control. Detailed documentation of changes made to each server is maintained within the Operating Systems Branch. In addition, the change control process maintains a historical list of changes made.

UNIX

All system changes are implemented according to the COT change control process wherein changes are submitted to change control by Wednesday morning and reviewed during the change control meeting on Wednesday afternoon. Emergency changes can circumvent this process, but must be approved in advance by the Operating Systems Branch Manager and change control staff. Changes are applied (not committed) when possible so that they can be backed out if necessary. System changes are, except in emergencies, made by the system administrator responsible for a particular UNIX host. In an emergency, any available system administrator may make the required change.

System changes are documented in the change control request. Patches are also documented briefly in a text file on each server so that a list of patches applied can be included in each month’s collection of system information.

Physical Security

COT issues a standardized identification badge/proximity card, which allows authorized employees/contractors access into COT facilities. The badge should be prominently displayed by the employee/contractor while they are in a COT facility. All employees are encouraged to challenge unescorted strangers and anyone not wearing visible identification. Requests for badge access and/or changes are completed via the form COT-F019 and signed by both the employee and the supervisor of the employee. All badges are required to include the employee's photo and are color coded in respect to their status (e.g., COT employee, contractor, etc.). A corresponding policy has been implemented and is included in the Security Policies and Procedures Manual (SPPM). Access rights to areas within COT facilities, particularly the Commonwealth Data Center, are regularly reviewed and documented.

To ensure no one enters the CDC without appropriate access, a facilities security guard is stationed at the front desk 24 x 7 each day. Visitors must sign in, are issued a visitor's badge, and must be escorted by appropriate COT personnel. The front desk visitors’ log is archived for one year and then shredded.

COT employees who are located in one of the other COT facilities are not required to wear a visitor's badge, as they have valid COT badges and are frequently required to attend meetings at the CDC. Entrance via the back door is restricted, and is only available as an exit in emergency situations.

The Commonwealth Data Center is currently equipped with video cameras that are located throughout the building at sensitive access points. A camera surveillance system has been installed at the guard station and a backup library of surveillance footage is maintained on CD for an indefinite period of time. Outside cameras have also been added for enhanced security. The building is partially surrounded by bollards to protect access to the building, the parking area is access controlled, the entrance to the building has additional safeguards, and interior doors have been added on the first floor to reduce access to the computing facility.

Badge readers are located at the front door, back door, east warehouse door, west warehouse door, second floor east, second floor west, second floor service closet, third floor east, third floor west, fourth floor east, fourth floor west, elevator glass doors east, elevator glass doors west, and maintenance room. Access to any area other than an employee’s assigned work area must be approved via the COT-F019 form.

The software controlling the doors is equipped to monitor all activity concerning physical entry, doors open for significant periods of time, invalid badge attempts and other activities and/or alarms. Reports can be created for anything from all activity on a specific door, to a particular individual and all access attempts at any location.

In addition to ensuring badge access is kept up-to-date, a formal process exists for entering/departing employees/contractors/vendors. This is accomplished by a web-based program, and is based on the forms COT-065 and COT-F042 respectively. The COT-F042 not only helps assist that badges are disabled, but that all access to any computer resources assigned via the COT-065 is revoked. When all areas of access have been removed, a copy is filed with the employee's personnel file.

Delivery/Loading Areas

The delivery and loading areas are controlled and isolated from information processing. Deliveries must be acknowledged by appropriate building maintenance staff before they can be accepted and the delivery door opened.

Since other state agencies use the mainframe to complete many of their computing needs, COT frequently must use tapes provided by the agency. It is the responsibility of the agency to pick up and/or drop off those tapes for COT's use. The forms used are COT-F082 (Authorization for release of reel tapes, cartridges and diskettes) and COT-F033 (Tape Library Storage Request). The tapes cannot be left on the front desk for quick pickup. The agency must wait for an operator to bring the tape down, and also must wait for the operator to come pick it up. The forms are signed by the person from the agency picking up/dropping off the tapes. It is not necessary for this person to sign the visitor's log, as they never leave the front desk area.

Security of Resources Off-Premises

As more telecommuting from home is necessary, COT does allow personal computers to be checked out as defined by COT-012 (Personal Computer Equipment Assignment). A form (COT-F018) must be completed by each employee and signed by the branch manager, with specifics about the assignment. The form must be signed and dated by both individuals on the date the equipment is released, as well as the date it is returned.

Environmental Protection

The environmental protection is divided into three (3) areas of control: UPS, HVAC and Fire Protection/Halon.

UPS

An Uninterruptible Power Supply (UPS) services all critical electrical systems including the COT computer systems. In June 2000, the UPS was upgraded for performance reasons. The new UPS is a redundant dual rotary system. Either side of the UPS is capable of supplying the CDC’s electrical requirements. In the event of a utility outage, the Division of Mechanical Maintenance, Finance and Administration Cabinet, operates the Central Utility Power System (CUPS) facility, which has diesel generators that will automatically start in the event of a power outage. There are two strings of batteries located in the CDC to provide power transition. New batteries that are more proficient were recently installed. The manufacturer of the UPS located in Middletown, NY is automatically notified of equipment fault status to the UPS. This is accomplished through a modem that is programmed to dial a specific telephone number and is also password protected. The UPS system is covered by a service contract with semi-annual service and inspection. The system is still under the original three-year warranty.

HVAC

The temperature control for the building is also provided by the CUPS facility. It is a dual deck system providing a mixture of heated, fresh, and chilled air. The system was designed to operate in a building facility of computer equipment. Over the last two years, the HVAC controls have been updated to meet standards. The two large control boxes for each air handling unit were upgraded.

Fire Protection/Halon

A fire alarm/notification system is installed. This system includes detection for the elevator and has new visual and auditory alarms. The system on floors two, three and four is an air sampling system, which is extremely sensitive. The system has an automatic escalation, which will remove the likelihood of a Halon release if the intensity of the danger increased. The Halon suppression system covers floors two, three and four in the equipment areas, including the electrical and communication rooms. The main mechanical room on the first floor and the other areas are covered by a sprinkler system. The fire protection and Halon system is covered by a service contract, which has semi-annual inspections. The sprinkler system is also covered by service contract and is inspected annually. Training for employees in the monitoring and usage of the system is ongoing. Some is provided during inspections and service calls. Formal training for building fire monitors is being scheduled for this fiscal year.

COT Contingency Planning

Documented procedures for re-establishing computer operations and critical applications in the event of disaster are detailed in the Disaster Recovery Manual. These procedures include off-site storage of system and application files at a contracted off-site location. Instructions in this manual include, but are not limited to, general information (statements, requirements, and responsibilities), recovery preparations, recovery actions and return to normal processing procedures. A copy of the Disaster Recovery Manual and the instructions are stored off-site at a secure underground storage facility and can be accessed via a secure web site. The agency responsible for each application also provides a designated representative who is responsible for the recovery or restoration of the application system. On May 9, 2006, COT’s Disaster Recovery Coordinator and independent auditors visited the Commonwealth's offsite storage vendor, Kentucky Underground Storage, Inc. (KUSI), at Wilmore, Kentucky. The Director of Business Development at KUSI led the tour which lasted approximately two hours and included the document and electronic media storage areas, as well as KUSI's new hotsite facilities.

COT, recognizing the need to strengthen its ability to recover the Commonwealth’s critical systems and functions, in the event of a disaster, contracted with LBL Technology Partners, from Minneapolis, to assist in the development of a disaster recovery plan. This project was started in July 2002, and was completed in February 2003. The new plans include systems running on the IBM OS/390 (mainframe computer), but also agency applications running on UNIX or Windows based servers that are maintained by COT. The plans also address networking and those functions running on enterprise servers (email, firewall, etc.) maintained by COT. The business owner identified these critical systems and functions through a Business Impact Analysis (BIA) process.

In July 2004, COT contracted with a new vendor to provide hot/cold site services in the event of a disaster. The contract was expanded from previous contracts in that recovery for distributed systems is now available at the hot site. Previously, only critical applications residing on the z/OS platform were included in a hot-site contract. This new contract significantly expanded COT's ability to recover all critical systems in the event of a disaster. The contract includes services for 66 Intel serves, 10 RS6000 servers, 22 Sun boxes, z/OS mainframe, and 1 data circuit from Columbus, Ohio to a COT building to be used for testing purposes. After a review of the monthly cost required to provide hot site services for network equipment; i.e., hubs, routers, firewalls, etc., a management decision was made to exclude network equipment from the hot site contract. The savings from not including this in the new contract could be better spent in building the infrastructure required to provide network redundancy (See section on KIH for more detail).

- In November 2004, six distributed systems were tested at the hot-site location. The TSM server, which is critical to the recovery of many systems, was also included as part of this test. In June 2005, two distributed systems were tested at the hot-site location. The TSM server, which is critical to the recovery of many systems, was also included as part of this test. Another COT biannual disaster recovery test was conducted February 3-5, 2006. Three critical distributed systems and applications and the TSM Server were recovered within the 48-hour allotted recovery timeframe. The first *remote* recovery of distributed systems from the Plain City Recovery Center was completed and Disaster recovery plans and procedures were updated.

Mainframe
Operations and Scheduling

COT Operations provides monitoring and support from the Main Console 24 hours per day, seven days per week. A supervisor is assigned to each shift. Activities performed and issues identified during each shift are documented via a newly implemented Electronic Message Board that is maintained and updated by each shift. Entries to the log are posted in predefined topics for routine procedures and monitoring or in specific topics defined as events occur. Each posting contains the time, date, and name of the operator posting the reply as well as a brief description and any associated Remedy ticket number. Standard topics are created by 1st or 4th shifts, depending on the day of the week. Topics for the previous 24 hours are then printed by 3rd or 5th shifts, again depending on the day of the week.

Each shift also completes a checklist that includes all of the standard activities for that shift. They are still undergoing development and will include the date, time, and initials of the operator completing each item on the checklist. The shift supervisor ensures that the checklist is printed out at the beginning of each shift. The 3rd or 5th shift supervisors collect all checklists for the 24-hour period and have them available for review in the morning. These are reviewed by the Operations Supervisor and filed at the Main Console.

Documentation is available online to operators outlining the specific tasks to be performed during their shifts and the approximate time of day that they should be performed. On-line documentation also includes instructions for operators on handling ad-hoc situations including system failures, restart procedures, and other emergency situations. Documentation is maintained in GOTSource, although hard copy manuals are also maintained in the event the GOTSource server fails. Unless specifically requested, only Operations staff can access Operations documentation on GOTSource.

Ad hoc requests require a change request approved by a director, per COT Policy or a Remedy Problem ticket. Operators create problem tickets at the request of authorized support staff. Operations is in the process of building a contacts database that lists for each piece of equipment on the 4th floor authorized support staff as identified by the agency.

Most batch jobs are scheduled using CA Scheduler, which is protected by RACF security. Only a few selected operators have access to add or modify the batch process schedules administered by COT. COT is also responsible for the administration and support of CA Scheduler. Most agencies are then responsible for their own batch operations and schedules. COT Production Services Branch is responsible for batch operations and scheduling CHFS, MARS, Revenue and Workforce Development's UI (unemployment insurance) job streams. In addition to Batch processing, the COT Production Services Branch is responsible for Production Cut-Over (PCO) processes for all COT Batch supported Job Control Language (JCL), Documentation, and Programs. COT operators have access to agency job schedules; however, they do not have access to agency job codes. COT also runs a daily audit job that generates the COT Scheduler Audit Report. This reports shows user changes to their job schedules. The job output is monitored daily on-line by the Systems Support Technician. This process is logged by the administrator and reviewed by operations management personnel.

Security-Mainframe

The Security Administration Branch is responsible for RACF administration. This branch currently has three employees in the mainframe security group. The branch reports to the Division of Communications and is part of the Office of Infrastructure Services.

Access to the z/OS/IBM Mainframe and its resources is controlled by the IBM package RACF, which is administrated by the mainframe security group. This application controls all user identifications and access to datasets or resources. There are password restrictions regarding length, composition and frequency of expiration. Passwords expire every thirty-one days. After three unsuccessful logon attempts with a bad password, the user identification will be revoked and cannot be used again until a RACF Security Administrator resets the user identification.

User identifications are revoked after sixty days of inactivity. The use of common names is discouraged, writing down and taping of passwords to terminals is prohibited, and storing a password in a batch job is prohibited.

Limited security administration functions may be assigned at the agency level if defined in the Agency OS/390 Security Agreement. The Manager of the Security Administration Branch must approve authorization of these functions.

Each agency is required to designate an IBM z/OS security contact. The request for agency security permissions (Agency contact) must be in a written or electronic form in order to request authorization from the Manager of the Security Administration Branch to become a security contact at an agency. The Security Administration Branch maintains a list of each agency and who is authorized to request mainframe security changes from those agencies.

Each agency will fall into one of the following three classes of support:

- Agencies that are self supported for day-to-day RACF and security administration
- Agencies that are able to reset their user's password only with all other administration being completed by COT Security Administrators

- Agencies that the COT supports in all aspects of security administration

The self-supported agencies will take care of their own administration but must follow COT guidelines and procedures. Each self-supporting agency is provided daily violation reports that show any of their users trying to access the mainframe and having problems. Another daily report shows those trying to access data sets or resources that are denied.

The Logon Violation Reports are broken into three data sets, which show the following information:

- Detail Logon information showing a line for each attempted logon.
- Summary of information showing a line for each user with the total count for each type violation
- Threshold information showing only those users having more than three violations

The last violation report shows violations against the agency data sets or resources. Each agency has been made aware of these reports and encouraged to review the reports. COT reviews the reports for those agencies that fall into the COT supported category. A log is maintained to track the review of the violations. As an additional security precaution, multiple people review the logs.

Every Sunday night (for each self-supporting agency prefix), a data set is created giving the agency the following weekly reports:

Member Name	**Description**
CONNECTS	This member contains a list of the agency's groups and what user ids are connected to those groups.
DATASETS	This member contains a list of the agency's data set profiles and what user ids & groups have access and at what level (read, update, control, alter).
LASTUSED	This member contains a list of the agency's user identification sorted in last used order. A user identification that has never been used will show up as Blanks which sort to the top followed by the user identification that has not
RESOURCE	This member contains a list of the agency's Resource profiles with the RACF class and what user ids / groups have access and at what level. (read, update, control, alter).
UACC	This member contains a list of the agency's profiles that have a UACC other than "NONE".
USERGRPS	This member contains a list of the agency's user ids with information about each user id.
USERIDS	This member contains a list of the agency's user identifications with information about each user id. This report is sorted by the user identification and then within user identification by Default Group.
USERTSO	This member contains a list of the agency's user identifications that have TSO access.

User identification requests are assigned sequentially by the Security Administration Branch and require a COT-F181, RACF/Security User-ID Request form or an email from one of the agency contacts. The COT-F181 form has recently been consolidated and is being used for all COT type Security requests (Network, Mainframe, UNIX, Windows, etc.).

As mainframe requests come in to the mainframe security group, they are entered into an MS Access Database and validated against the agency contact list to make sure the requestor is an authorized requestor. The requests with all the information are entered, given a unique tracking number and assigned to someone in the mainframe security group. When the request has been completed, the individual completing it updates the tracking system and the request by filling in the "date", "time" and "completed by" fields. Queries are available in MS Access to list the requests by request number, agency or requesting individual.

The Employee Departing Checklist (on-line web based system) notifies the Security Administration Branch of any terminations or transfers of COT employees/contractors. The Employee/Contractor Exit Request is sent to all of the mainframe security administrators to ensure that access is removed. When the mainframe security group is notified of someone leaving, a query is run to check for mainframe user identification. Any user identifications owned by the individual will be revoked on their last day or when notified. These user identifications will be left on the system while management ensures that data set cleanup is performed, and then removed.

When COT users change departments, their old user identification is put into REVOKE status. User identifications are then deleted and a new user identification is issued via the above procedure. User identifications with the prefix PS, only used for COT, are not deleted, but remain in REVOKE status until it can be determined that the information to which the IDs have access is no longer needed by COT. The branch is working with the Personnel Cabinet to obtain a monthly file of all Commonwealth personnel changes; i.e., terminations, resignations, transfers, new hires, etc. This file can then be used to ensure that RACF userIDs are kept current.

The Security Administration Branch has been regularly communicating with customer agencies to promote the importance of mainframe security. Listed below are examples:

- Cleanup of user identifications – Reports related to these cleanup procedures have been produced for each agency.

- Password Strengthening – Password cracking software has been utilized to produce a list of mainframe passwords that need to be strengthened. This list has been distributed to agency security contacts.

- Reports – The COT has developed several reports for agencies to use in order to assist them in identifying violations and reviewing access levels.

- RACF Administration – Several guidelines have been sent to the agencies suggesting the proper way to administer RACF, change a user's password and add user identifications.

The Security Administration Branch utilizes the Vanguard software suite to assist in security administration:

- Vanguard RACF Administrator – Allows cloning of user identifications and groups and allows reporting on RACF entities.
- Vanguard Advisor – Eases reporting on RACF Violations and System Management Facility (SMF) monitoring.
- Vanguard Analyzer – Produces many useful RACF system setup reports

With the implementation of the Enterprise password auditing policy, http://gotsource.ky.gov/dsweb/Get/Document-35938/Password_Auditing_and_Policy_Enforcement_for_Network_Domains%2C_CIO-080.doc password audits are required on a quarterly basis. A RACF Password Cracking utility is used to test the strength of the mainframe passwords and identify those user identifications with weak passwords. Reports are then sent to the agency contacts so that they may take steps to ensure the passwords are strengthened. The cracking utility was run at the beginning of fiscal year 2005. Reports are generated for internal COT use also.

With the implementation of the Enterprise userID/password policy, http://gotsource.ky.gov/dsweb/Get/Document-13212/UserID+and+Password+Policy%2C+CIO-072.doc, non-expiring passwords must be approved by the Commonwealth Office of Technology. COT is now responsible for these passwords and ensures that the password composition meets the enterprise standard. Agencies must identify the need for requiring a non-expiring password and must identify special security precautions put in place to minimize the risk of having a non-expiring password.

Access to DBMS databases is granted through RACF security software. Access must be authorized by the owner of the database and must be a written or electronic request to Division of Security Services.

The password for the System Emergency User Identification and the passwords for the RVARY Switch and RVARY Status have been sealed in envelopes and put in the COT storage safe. In addition, dual control access is required. The password is split so that two individuals are required to use the user identification/password. The use of the password will be monitored and a log is kept recording the use of the profile to ensure that it is restricted to emergencies. The password is periodically changed.

In October 2002, COT implemented the RACF option, Erase on Scratch. This option will prevent sensitive and/or confidential data from being recovered from a deleted dataset. Agencies were notified of the option change and were provided instructions as to how to implement this option for selected datasets.

In May 2001, the COT enabled the cryptographic co-processor on the IBM OS/390 server, allowing the enhanced use of Secure Socket Layer (SSL) on this platform.

Output Data Distribution-Mainframe

COT provides and supports two online report distribution products – RMDS and RDS. Both products are for electronic report storage and retrieval on tape and/or optical disk for viewing and printing by customers. Security for both products is provided by RACF. The owning agency of each report must authorize access to their reports. An agency contact list is maintained of individuals that may authorize access to agency reports. A form is currently being developed that will be used to formalize the request process.

Backups and Recovery-Mainframe

The disaster recovery strategy insures that all critical data files are backed up and taken offsite for storage. The mainframe strategy utilizes weekly full volume, full data recovery backups of most of the DASD volumes attached to the IBM OS/390 server. The only mainframe volumes that are not backed up weekly are the ones whose data changes too rapidly for a backup to be of any use and those that are more easily created at the hot-site from scratch. There are also daily backups of critical files that are taken offsite that include DB2 and IMS archive logs, some of the Information Management System (IMS) client nodes and selected application backups. Critical data files and enterprise functions residing on UNIX and Windows servers are backed up daily or weekly and sent to the offsite storage facility. The backup tapes are returned four weeks later.

UNIX

Operations and Scheduling

UNIX Operations support is provided 24 hours by seven days a week from the same staff that operates the mainframe systems. This support consists of monitoring the UNIX servers, restarting applications, occasional UNIX userID and password resets, rebooting servers, and notifying support personnel of problems and issues. However, operations do not reboot a server or restart any UNIX computers OR reset and UNIX userID and password unless a request is sent via e-mail from a person on an authorized contact list, and the request is followed up with a phone call from the requestor.

A server manual is available at the main console in the operations area outlining responsibilities of individuals, procedures to follow and includes a list of support personnel. Server user identifications and passwords are kept in a padlocked metal box for which only the shift supervisors and server administrators have a key. Shift Supervisory personnel log any access to the metal box.

Batch-work processing in the UNIX environment is a manual process and these systems require monitoring during all phases of processing. Generally, batch-work processing starts at the same time that the batch-work for the mainframe is started for a particular software application. Most software applications require processes that coordinate between the UNIX system and the mainframe.

Issues identified during a particular shift are documented in a Production Control log each day, and the log is reviewed by the next shift during a shift turnover time period. The log includes the date, known problems, production migrations, special requests or runs, and other shift information. A Nightly Cycle document is also used by the Production Control Analysts, which is updated with statistics and other pertinent information regarding the cycle. Any problems affecting availability of the UNIX environment are explained at the top of the document. The Nightly Cycle document also contains primary contact names and numbers for system ABENDS and resolutions for each cycle. The analysts discuss resolution actions and confer with the individual that is on-call prior to any changes or course of action.

On the business day following each cycle, further statistics are gathered, and the Nightly Cycle document is updated and sent to senior COT and agency management personnel for review. This provides them with explanations of problems from the previous night and any resolutions taken during the day to help prevent further problems.

Security-UNIX

A comprehensive Security Policies and Procedure Manual is available on-line that addresses mainframe, UNIX and NT concerns. In addition, a UNIX (Solaris and AIX) administrator's manual is available that includes topics such as policy settings, file system security, etc. These policies are available in COT's document management system-GOTSource.

An audit of user identifications was performed again this year. Some user identifications were reconfigured to be "su-only" (not loginable) so that their use could be tracked through available logging mechanisms. Agencies are required to designate an owner for each generic user identification and the owner who would be responsible for everything that is performed with the specific unique user identification as well as being the only person authorized to ask for a password reset. Any generic user identifications that require login capability must have documentation from the owner of the identification as to why the identification requires this capability. COT security personnel periodically verifies with the agencies the particular hosts that each user identification should be able to access and ensures that the user identifications can access only those particular hosts.

Virus scanning is being run daily on the Unix servers. A daily report is produced and reviewed every day. Also, staff is checking every day for DAT files.

Password restrictions are implemented so that all users must change passwords on a regular basis, have a 5-day grace period in which to change the password, will be locked out after 5 unsuccessful login attempts, and must use a password with at least 3 non-alpha characters. Administrator passwords are stored in a locked box and access to the safe is restricted, logged and reviewed. A few generic user identifications are not required to have passwords that expire on a monthly basis. In these cases, written justification is prepared by the owner of the identification and submitted to the Director of the Division of Security Services.

The COT-F181 is being used for user identifications creations and changes. Password resets and failed login count resets are performed by the Division of IT Operations. The KCCMS help desk has "sudo" capabilities to add new users, reset passwords, and reset failed login counts and they define their own method of requesting changes. Requests to lock/unlock user identifications must also be sent using the COT-F181.

A daily report of security log files is generated and emailed to all system administrators. In addition, a system administrator reviews log files once a day, Monday through Friday. These logs include the error report, "wtmp," "sulog," "sudo.log," "syslog," messages, and the login log (depending on the particular operating system). Any anomalies will be reviewed with the UNIX team leader and the Systems Software Branch Manager before filing a Security Incident Report. The daily check of these logs will be documented on a checklist and filed daily in a binder. In addition, Operations staff also monitors these logs on a shift-by-shift basis, thereby expanding coverage.

As employees depart, the security administrators are notified via a web based system (COT-F042 Departing Employee Checklist) to remove their user identification. The security administrators deactivate the user identification and produce a list of files owned by that user identification. If the user identification does not own any files other than standard system files, security administrators delete the user identification immediately. If the user identification owns files other than the standard system files, security administrators email this list to the system owner and give him/her 30 days to determine what should happen to these files. At the end of 30 days, security administrators remove the user identification and files in the home directory. Security administrators do not remove files in shared directories as group ownership may provide access to other users.

Security patch information will be analyzed as patches are identified. Those security patches that are deemed critical are applied as soon as the outage can be scheduled. Patches that are less critical are collected and reviewed. The security patch information will be compiled and a list created for review. The Security Administrator will review the patches and those that are required will be installed on test systems, with the owner's permission. After a week of evaluation, if no problems are found, patches will be rolled out to the remaining hosts according to the change control process. The exceptions to these procedures are the two KCCMS F50 servers. They are running old versions of operating systems that are no longer supported.

Security administrators run Saint, a freeware utility that checks for system vulnerabilities, against each host, except for the older KCCMS F50 servers. This utility is run after a major release is installed. Security administrators fix problems that they can without causing problems in the application or the system. Security administrators will run Saint whenever a major change is made to the operating system or a newer version of Saint is obtained. Further, basic system auditing is activated and the output files produced are reviewed on a daily basis.

Output Data Distribution-UNIX

There are no special output distribution procedures since reports are available on-line to those that have appropriate access.

Backups and Recovery-UNIX

Selected application data from the UNIX enterprise servers are backed up using the Tivoli Storage Manager (TSM) product, which is a client-server product. Those TSM clients who participate in our offsite disaster recovery process have copies of their data taken offsite daily and stored at our secure storage facility for safekeeping. (Backups for systems that have been deemed critical for disaster recovery are being taken off-site to underground storage.)

Windows

Operations and Scheduling

Windows operations support is provided 24 hours by seven days a week by the same staff that operates the mainframe. This support consists of monitoring the Windows-based servers, restarting applications, rebooting servers, and notifying support personnel of problems and issues. However, operations does not reboot a server or restart any Windows servers unless a request is send via e-mail from a person on an authorized contact list, and the request is followed up with a phone call from the requestor.

A server manual is available at the main console in the operations area outlining responsibilities of individuals, procedures to follow and includes a list of support personnel. Server user identifications and passwords are kept in a padlocked metal box for which only the shift supervisors and server administrators have a key. Shift Supervisory personnel log any access to the metal box.

Batch-work processing in the Windows environment is a manual process. It requires monitoring during all phases of processing. Generally, batch-work processing starts at the same time the batch-work for the mainframe is started for a particular software application. Most software applications require processes that coordinate between the Windows system and the mainframe.

Issues identified during a particular shift are documented in a Production Control log each day and the log is reviewed by the next shift during the shift turnover time period. The log includes the date, known problems, production migrations, special requests or runs and other shift information. A Nightly Cycle document is also used by the Production Control Analysts, which is updated with statistics and other pertinent information regarding the cycle. Any problems affecting availability of the Windows environment are explained at the top of the document. The Nightly Cycle document also contains primary contact names and numbers for system ABENDS and resolutions for each cycle. The analysts discuss resolution actions and confer with the individual that is on-call, prior to completing any changes or undertaking a course of corrective action.

The business day following each cycle, further statistics are gathered, and the Nightly Cycle document is updated and sent to senior COT and agency management personnel for review. This provides them with explanations of problems from the previous night and any resolutions taken during the day to help prevent further problems.

Security-Windows

A comprehensive Security Policies and Procedure Manual is available to address both UNIX and Windows security considerations. In addition, an administrator's manual is available to outline topics such as policy settings, file system security, etc. These policies are available in COT's document management system-GOTSource. One is available for NT, Windows 2000, and Windows 2003.

A security baseline is established for all enterprise servers. As each server is configured, a baseline script is applied to the server to ensure that adequate security settings are established. This script has also been applied to all existing servers.

Security hot fixes are reviewed on a regular basis. The NT team meets on the 1st and 15th day of the month to review all security vulnerabilities that have been identified. The team decides the impact of each vulnerability and makes a decision as to the implementation of a fix. Spreadsheets are maintained to track the testing and implementation of the fixes for each of the Windows servers. Documentation is maintained for each server that shows the security fixes that have been applied. Due to the large number of servers housed at COT, tracking fixes from development, testing, and production can be cumbersome. The team stores and updates all documentation related to applied security fixes in a common location, which is accessible only to the security team. Each month all administrator passwords are changed and secured in a locked safe. Team administrators and/or management in the event of an emergency can retrieve these passwords.

Standards have been established for Windows audit settings. The required audit settings have been identified and each administrator is responsible to ensure that these settings are used on the server for which they are responsible.

The Security Administration Branch reviews the Windows logs. See section on Review of Enterprise Logs.

COT utilizes BMC to provide notification of problems with security, server hardware, and system services. Alerts are generated based upon thresholds established within the BMC application. Automatic emails are sent to administrative staff when designated thresholds are reached.

SSL certificates have been installed on Commonwealth IIS servers where secure client/server communications is required. Certificate administration has been centralized and a list of certificates/servers is maintained on a server for documentation.

The Windows staff is notified when COT staff members (contractors and employees) are terminated. A web based notification system (COT-F042 Departing Employee Checklist) is used to inform the appropriate individuals that the departing employee's security access can be removed. This process is initiated by an email from the automated system. An NT team member responds to the email by accessing and updating the web page.

Output Data Distribution-Windows

There are no special output distribution procedures since reports are available on-line to those that have appropriate access.

Backups and Recovery-Windows

Selected application data from the NT enterprise servers is backed up using the Tivoli Storage Manager (TSM) product. TSM clients have copies of their data taken offsite daily and stored at our secure storage facility for safekeeping. (Backups for systems that have been deemed critical for disaster recovery are being taken off-site to underground storage.)

Infrastructure Support

Change Control

The Commonwealth Office of Technology implemented a revised Change Management process effective April 1, 2001. The responsibility for this function lies within the Office of Infrastructure Services.

The process is outlined in COT Policy Number COT-008. The policy describes the responsibilities, policies, and procedures to be followed by COT when making changes or recording events to the Commonwealth of Kentucky's IT infrastructure. The purpose of the Change Management process is to minimize service disruptions to the computing environment and promote system availability. This covers any and all changes to the hardware, software or applications. This process also includes modifications, additions or changes to the LAN/WAN, Network or Server hardware and software, and any other environmental shutdowns (i.e. electrical).

COT managers are responsible for pro-active planning in managing their environments. Change Requests should be submitted as soon as all planning has been completed, but no later than the mandatory deadline of 10:00 a.m. Tuesday. All Change Requests are submitted on the Change Request Form located at: http://www.state.ky.us/got/ois/enduser/helpdesk/changcntl/ccform.html. The Change Request must include enough detail so that all areas know the relative impact of the change and how it may affect other areas.

Each request is discussed at the weekly Change Advisory Board meeting, which is held each Wednesday at 3:00 p.m. The purpose of the weekly meeting is to share information, concerns, and comments in a cooperative environment in order to eliminate potential disruptions of service to COT customers. The Change Manager or designee facilitates the meeting. Anyone submitting a change should be represented at the meeting.

Items discussed at the meeting include:

Reviewing the last changes implemented and any pertinent issues/problems encountered;
Reviewing the proposed changes for the upcoming week;

- Identifying conflicts and plan for resolution
- Identifying customers affected and notification requirements to those customers;
- Schedule a time frame to implement a change, while considering application restrictions and upcoming events such as month-end, year-end, heavy business days, holiday, or any justified business need.
- Ensuring availability of a back-out or fallback plan;
- Ensuring support is defined in the event of a back out; and
- Finalizing and approving changes.

The Change Control schedule is then posted each Thursday morning on the COT Change Control website, and an email is sent out to the Change Control distribution list noting that a new schedule has been posted.

The primary participants of the Change Management process are the areas that affect the COT infrastructure. COT applications/development areas are to submit major events affecting production systems.

Awareness Notification

The COT Help Desk will send the Awareness Report via email within ½ hour, if they are aware or notified of an occurrence affecting the production IT environment. It is the responsibility of the support group working on the problem to send an email to the Help Desk with a brief description of a problem and assessment of the services and users affected by the situation. A follow-up notification is sent once the issue is resolved. The Awareness Notification distribution list is made up of not only COT personnel, but also many of the key individuals within the agencies. Anyone can be added/deleted to the list by contacting the COT Help Desk.

Internet and Intranet Firewalls

Access to the Internet is controlled and monitored by the firewall. Firewall and router logs are reviewed for suspicious activity including any known attack signatures, SNMP attempts to the Firewalls, unauthorized Telnet sessions, IP spoofing, unusual packet routing, port scanning, and other suspicious activities. The Firewall, backbone routers, and HP Openview gather these logs.

Symantec, the COT security vendor, administers the Internet firewall, yet the process is managed by COT. The security vendor documents these attempts and completes a security incident report that is sent to the Security Administration Branch for follow up. On attacks originating from the Internet, the offending IP addresses are filtered at various points in the infrastructure until the attacks have ceased, or

COT has communicated with management from that party. On Intranet attacks, the offending IP or entire IP subnet of the offending party is blocked. Communications will not be re-established until the offending entities' ITO responds as required by COT policy. Resumption of services is at the discretion of COT since COT may conduct protocol analysis at multiple points throughout the infrastructure to determine if the agency has corrected the situation. Network services will resume and continue as long as the offending party demonstrates they are in compliance with COT network security policies.

A security architecture was designed and approved by the Commonwealth Technology Council (CTC) in 2002. COT has created an enterprise e-government zone and has added additional firewalls to separate the Intranet from the e-government zone. The e-government zone has multiple DMZ's to help protect services and customers. All agencies are required to move all public visible services such as web severs FTP servers, SMTP servers, etc., to the e-government zone. The goal is to create a "block all, allow few" approach on the Intranet firewalls. COT is working with agencies to reduce the protocols allowed. Until the "block all, allow few" rule is applied, COT is auditing all protocols. COT is capturing the traffic and reviewing the logs files for future enhancements and blocking.

Both the Internet and Intranet firewalls are Tier 1 firewalls. (Refer to Enterprise CIO-076, Firewall and Virtual Private Network Administration Policy). Agency/cabinet firewalls are Tier 1 or Tier 2. Tier 1 firewalls use Checkpoint software and are managed by COT but administered by the COT security vendor. The logs from Tier 1 firewalls are correlated to the IDS. Tier 2 firewalls utilize Nortel's Contivity and they are managed and administered by COT. These logs are not correlated to the IDS.

Agency/Cabinet Firewalls

COT provides firewall services for various state agency applications. The customer owns the rules set for each firewall. COT works with customers to strengthen each agency's firewall rule sets. The application requirements and the degree of security the application owners wish to implement determine how strict to make the rules base.

The firewall software is kept current with the latest releases, vendor-recommended patches, and enhancements. Modifications to firewall configurations can only be performed from the firewall's console. For Tier 1 firewalls, the security vendor must obtain COT approval before applying the patches and upgrades to the servers.

The firewall requires a user identification and password to access or to change configuration settings. Only authorized persons have access to the password to change firewall information. Access is also restricted to certain IP addresses. All of the firewall consoles, servers, and other network hardware are maintained in a secure, physical access-controlled location.

The Nortel Contivity product for VPN and firewall is available for Tier II firewalls. COT recommends Tier II for network protection and agency firewalls not protecting enterprise class material and/or sensitive data that could result in loss of life or financial repercussions.

Intrusion Detection Systems (IDS)

Internet Security Systems (ISS) is the enterprise standard for network based IDS. This system interfaces with COT's Checkpoint Firewall-1's management console for alerts and actions based upon the rule sets established. When the IDS agents identify attack signatures that are critical, a page is sent to the firewall team to determine of the IP address should be blocked. COT has greatly enhanced the number of sensors at strategic locations throughout the infrastructure.

COT's security vendor, Symantec, manages the IDS as well as the Tier 1 firewalls. This will provide 24x7 coverage at various points throughout the network. COT has a security contract that provides product, maintenance, and professional services. Three vendors hold the contract jointly.

A Layer 4-7 switch has been placed at the perimeter that allows COT to filter on content a well as port numbers.

Virtual Private Networking (VPN)

A Virtual Private Network (VPN) is also available for clients wanting a secure connection from their access point to the VPN Server or to their own COT administered Contivity firewall. All VPN users are required to enter a username and password to connect. Once the connection is accepted, a "secure tunnel" is created from their workstation to the VPN server. This service is available upon request for all KIH users. This is commonly referred to as tunnel mode and allows COT to create a virtual KIH for all agencies participating. Placing a Contivity switch at each agency remote location and establishing a secure connection back to the agency's VPN bridgehead located at the COT data center accomplishes this. All other communications are shut off to the participants and each communication must pass through a common firewall and approved before it is routed to the end node. The only allowed protocol and communications to each node is through the firewall and via the branch office tunnel. This eliminates all unsolicited traffic that is not approved to reach agency nodes. Also, COT is purchasing a SSL VPN appliance that restricts access to specific applications for specific servers.

Outlook Web Access (OWA)

Encryption for Outlook Web Access (OWA) utilizing the SSL option is available. This service provides confidentiality for COT clients using web services to obtain email while traveling or not having access to the Outlook Client.

Network

HP Openview monitors routers and switches and identifies potential problems. COT measures the performance of the WAN links with HP Openview, ServiceLink, and MRTG. These tools allow the ability to provide measurements for customers and to take a more proactive approach in Network performance monitoring. COT measures availability, response time, and error conditions. ServiceLink has a web interface that can be used to track these issues and allows the ability to report problems and update trouble tickets. Senior engineers in both the Enterprise Services area and the Network Engineering area perform capacity planning with the help of these tools. COT has implemented Distributed Sniffer from Network General to help manage and protect the network. Protocol analysis can be performed at multiple points throughout the infrastructure. The product helps COT to determine where internal security issues are such as virus infection, mischievous behaviors, and other types of unwanted traffic.

The goal is to have the ability to isolate traffic anywhere on the entire COT backbone (ATM, Frame Relay, Switched Ethernet, Server Farms, Frankfort MAN).

Kentucky Information Highway (KIH)

An RFP was released to establish a method for COT to obtain cost effective connectivity solutions for KIH eligible entities throughout the state. The contract was awarded in February 2005, and COT is in the process of planning the transition to the new infrastructure.

Virus Protection

McAfee of NAI is the enterprise IT standard for virus scanning. COT has Total Virus Defense (TVD) and Active Virus Defense (AVD) agreements with McAfee, which validates COT’s multi-tiered approach to virus protection.

TVD includes the following:

- VirusScan: Virus protection for desktops and servers
- NetShield: Virus protection for servers

VirusScan’s and NetShield’s AutoUpdate feature uses pull technology to keep our virus protection current at all times. The agent checks daily for DAT updates and weekly for engine upgrades.

- GroupShield: Virus protection for Exchange servers
- WebShield: Virus protection for in-bound Internet mail

The combination of WebShield and GroupShield helps promote a nearly virus-free messaging environment.

AVD includes the following:

- All of the above products
- ePolicy Orchestrator (ePO)

ePO provides additional power in maintaining a complete virus security solution. It is designed to manage policies and deploy protection while generating detailed graphical reports on McAfee's anti-virus products. It has the ability to provide up-to-the-minute information that the virus signature and scan engines are up to date.

McAfee provides timely virus warnings and software updates as well as DAT files during emergency outbreak situations, at which time COT will alert our McAfee enterprise clients. McAfee's DAT updates and/or engine upgrades are provided and posted to the dedicated FTP anti-virus server, and notification is provided to our clients.

Enterprise support from McAfee is available for each anti-virus contact in each cabinet that participates in the agreement.

Incident Reporting

COT implemented a security incident reporting policy that requires employees and/or contractors to report suspected security violations immediately. A security incident reporting form (COT-F012) is made available for use in reporting security incidents. As incidents are reported, the Security Administration Branch performs investigation and follows up as required.

Review of Enterprise Logs

The Security Administration Branch is responsible for the review of logs. This results in a system of checks and balances between the server support teams and the security group.

FTP, IIS, and event logs are retrieved hourly from all windows servers and placed in an oracle database. This provides a replication of all logs, in event that a server is hacked and the log files are erased, as well as creates a searchable back up system of all server log activity for reporting purposes. Virus scan log files are retrieved daily and put into the same database. The Black Ice logs are retrieved via a web site and analyzed daily, as well.

The log files for each server are set to a default location, allowing a script to find all the log events for the past hour. The script uses tables listing all servers in each domain. The data is then stored in the database, which builds on those hour increments and allows daily, weekly, monthly and quarterly reports to be generated and reviewed.

The database currently has a variety of views based on the raw data. These views allow faster reporting off the vast amount of log file information in the database. The views can be manipulated into a variety of formats. The views are filtered, using a list of triggers that pull out common hack attacks and known vulnerabilities, as well as filters that strain out information that is commonplace and not considered a security threat. The use of updateable filters and triggers allows us to get reports that are then reviewed.

The Security Administration Branch is responsible for reviewing the logs daily. If any suspicious activity is determined, an Incident Report (COT-F012) is completed. These F012's are then escalated to the forensics group for more in-depth review.

Commonwealth Data Center Assessment (Operations)

The Commonwealth Office of Technology contracted with Microsoft to conduct an operations assessment of the Commonwealth Data Center. The objective of the assessment was to review the IT management processes involved in operating and supporting the Microsoft based client/server technologies. The scope of the processes included change management, configuration management, release management, service monitoring and control, incident management and problem management. Prioritized recommendations by service function were provided as part of the deliverable of this assessment.

Security Alerts

COT provides a structured, routine, and timely service of announcing security alerts to proper personnel by emailing them using distribution lists, and posting them on the Security Services web page. The information on the web page is restricted and viewable only by state intranet service customers. It is the intent of COT to be the clearinghouse for the identification, collection, analysis, and dissemination of information to other Commonwealth Agencies to save each of them the effort of performing the same tasks. It is important to note that the Security Administration Branch and the System/Network

Administrators, who are responsible for implementing security measures, must continue to stay updated of the latest security threats, vulnerabilities, software patches, etc. For this reason, COT has a contract with Security Focus. COT receives security alerts as soon as they are issued by Security Focus via email. The Security Focus Alerting system was recently purchased by Symantec, and is now referred to as Symantec DeepSight Alerting Service.

Analysts within the division are charged with the responsibility to review these notifications as soon as they arrive. Once an alert has been determined to be critical for supported products and systems, the security analyst will supply the necessary value-added information to other security staff members who finalize and publish the alert notification to selected email groups and post the detailed information of the alert on the COT security alerts web page. (The Security Alert notification is also posted on COT's website home page.) The security alerts web page has been designed specifically to contain technical information on each alert. On a weekly basis, COT produces a "Weekly Security Alert Recap." The recap attempts to cover all security alerts not deemed as an immediate threat to the Commonwealth of Kentucky computing environment, yet still important enough to be highlighted in a weekly communication. This weekly recap is emailed to the COT regular security contacts and other appropriate distribution lists. This weekly information is posted and updated regularly on the security alerts web page. The web page contains only the latest cumulative update to any particular vulnerability posted. Staff archives alerts with no new updates approximately every 90 days. The Archives are also available to authorized customers on the website.

Homeland Security

In response to the development of the Homeland Security Advisory System created by the National Homeland Security Office, COT developed strategy and implementation procedures for each of the advisory levels. A Homeland Advisory Alert Plan can be found at http://www.gotsource.net/dsweb/Get/Document-37879/GOT_Homeland_Advisory_Alert_Plan.doc

The threat level was last raised to orange (high) on December 20, 2003, at which time COT implemented the procedures defined as “high condition” (orange). It was lowered back to yellow on January 9, 2004. COT is currently operating at the “elevated condition” (yellow) which is consistent with the national office.

Microsoft’s Active Directory

The Commonwealth of Kentucky has chosen Microsoft's Active Directory for the database of users and objects within the Commonwealth. Previously the Commonwealth had a variety of domains which contained the users and objects including Microsoft Windows NT 4.0 and Novell networks. The largest repository of user information in a directory today is the Exchange 5.5 Global Address list which requires several (one way) trust relationships between the Windows NT 4.0 domain. As the Commonwealth moves to Active Directory, the directory of users and objects will be contained within the Commonwealth forest. Currently the forest consists of an empty root domain and one level of child domains. There is a "foster domain" which by default is the domain that the users would come into Active Directory. A Cabinet can choose to write an Exception request to request that their cabinet comes into Active Directory as a child domain under root. COT’s migration is complete, and several cabinets are currently in the migration process. As they migrate into Active Directory, their previous system (Windows NT 4.0/Novell) are decommissioned. Moving forward, the Commonwealth will leverage the directory for such applications as Exchange 2003.

Secure E-mail

COT is operating in its second year using Entrust Express with Outlook. Currently there are over 1,750 users enrolled. Initially, a small number of employees from across state government piloted the security software. Since the service was offered to state employees, several agencies have signed on to use the product. Among the offerings include encrypted e-mail and Ice. Ice is a program that allows users to encrypt files/folders for themselves or groups. The encrypted files can be stored locally or on network drives. The program will allow customers using COT provided Microsoft Exchange services to purchase licenses to enable secure email with other participating customers, or with any external email address that supports S/MIME compliant encryption. Please note, Entrusts only supports operating systems WIN2K and XP.

Content Management

In April 2004, COT entered into an agreement with Network Appliance to provide the Commonwealth with a Content Security Management (CSM) solution. Webwasher CSM Suite provides anti-spam protection, website filtering, email content filtering, and anti-virus protection to the Commonwealth's executive branch agencies.

Data Consolidation Project

COT is undertaking a project to potentially consolidate all IT functions, except for business development, from four Cabinets into COT. These Cabinets are Finance, Commerce, GOLD and Justice. The approach is to perform, in conjunction with the agency IT staff, a discovery process whereby we document the current situation, products, procedures etc. Based upon the fact finding COT will develop plans for the integration, conversion or replacement of products and processes to provide the agencies with services. At the same time COT have a planning process underway to look at COT internal procedures to ensure COT is positioned to offer these services in a responsible way.

Once the discovery and planning processes are completed, recommendations will be presented for management review. Upon acceptance of the plans, those that are agreed to will be implemented. This project is being viewed as a pilot for the integration of all Executive Branch IT functions.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

Organization Structure and Personnel

Control Objective 1

Controls provide reasonable assurance that COT policies and procedures are documented and COT functions and responsibilities are appropriately segregated.

Tests of Operating Effectiveness Achieved

- Inspected policies and procedures related to oversight and management of the organization.
- Reviewed the organizational chart for completion, accuracy and appropriateness to the situation.
- Reviewed the COT organization chart noting the degree to which operations/programming functions are segregated.
- Interviewed computer operations management and programming management to determine adherence to policy.
- Reviewed the organization chart to verify existence of specific functions and departments.
- Reviewed the policies and procedures of the COT to verify that COT personnel do not initiate or authorize transactions.
- Reviewed the policies documents related to enterprise security.
- Ascertained that personnel policies exist and reviewed them for inclusion of policies for hiring, termination, salary administration, performance evaluations, vacation, employee benefits, building and system security and emergency procedures.
- Reviewed policies related to COT specific personnel, security, and administrative policies.
- Obtained and reviewed the strategic planning and major accomplishment documents.

Application Maintenance and Documentation

Control Objective 2

Controls provide reasonable assurance that changes to applications are authorized, tested, approved, properly implemented, and documented to provide an audit trail to facilitate future program changes.

Tests of Operating Effectiveness Achieved

Mainframe

- Reviewed program change control procedures with management noting detailed procedures for program implementation.

- Inspected a judgmental sample of program change requests from the “EPM Projects Requested Report” with a request date between July 1, 2005 and June 30, 2006 and traced the request from authorization, initial agency approval, and prioritization, to properly implemented program in the production directory. Projects not completed were inspected to ensure the current project status was identified as "active."
- Inspected a judgmental sample of program executables from the production directories with a last modified date between July 1, 2005 and June 30, 2006 and verified that the System Life Cycle was followed, and supporting documentation was properly completed.
- Reviewed the Systems Life Cycle Manual (SLCM) for documented policies and procedures for development and maintenance of applications.
- Inspected SLCM to determine whether it outlines that certain deliverables are required for change requests.
- Inquired of management to determine whether the System Life Cycle Manual is followed for larger projects.
- Reviewed EPM reports and discussed with management to determine its use in documenting program change requests and the status of those requests.
- Inquired of Project Management to determine the types of testing performed by COT.
- Inquired of Project Management to determine that Production Program Cutover Process was used to promote mainframe program changes.
- Inspected a judgmental sample of Production Program Cutover Forms for appropriate approval and authorization.
- Inquired of Project Management to determine user involvement in testing changes to programs.
- Inspected a judgmental sample of documentation maintained by COT programmers for changes to programs.
- Inquired of Project Management to determine that documentation was provided to the agencies for changes that affect users.
- Reviewed access to COT managed and controlled production and source libraries to ensure that proper separation was maintained between developers and the individuals promoting the change.

UNIX and Windows

- Reviewed program change control procedures with management noting detailed procedures for program implementation.
- Inspected a judgmental sample of program change requests from the “EPM Projects Requested Report” with a request date between July 1, 2005 and June 30, 2006 and traced the request from authorization, initial agency approval, and prioritization, to properly implemented program in the production directory. Projects not completed were inspected to verify the current project status was identified as "active".
- Inquired of management to determine whether the System Life Cycle Manual is followed for larger projects.

- Reviewed EPM reports and discussed with management to determine its use in documenting program change requests and the status of those requests.
- Inquired of Project Management to determine the types of testing performed by COT.
- Inquired of Project Management to determine user involvement in testing changes to programs.
- Inspected a judgmental sample of documentation maintained by COT programmers for changes to programs.
- Inquired of Project Management to determine that documentation was provided to the agencies for changes that affect users.
- Inspected a judgmental sample of UNIX and Windows implementations.
- Reviewed the Systems Life Cycle Manual (SLCM) for documented policies and procedures for development and maintenance of applications.
- Inspected SLCM to determine whether it outlines that certain deliverables are required for change requests.
- Inspected access to production directories for appropriateness for a judgmental sample of production directories.
- Inquired of Project Management to determine that appropriate implementation procedures are used for UNIX and Windows program changes.
- Inspected a judgmental sample of program executables from the production directories with a last modified date between July 1, 2005 and June 30, 2006 and verified that the System Life Cycle was followed, and supporting documentation was properly completed.

System Software and Hardware

Control Objective 3

Controls provide reasonable assurance that changes to system software and hardware are authorized, tested, approved, properly implemented and documented to provide an audit trail to facilitate future system changes.

Tests of Operating Effectiveness Achieved

- Inquired of the Server Administration Branch Manager to determine whether only the Server Administration Branch is responsible for implementing and maintaining system software in the Enterprise Application Domain at COT.
- Inquired of the Server Administration Branch Manager and LAN Supervisor to determine how system software is selected and authorized.
- Inquired of the Server Administration Branch Manager and the LAN Supervisor to whether testing is performed in a test region.
- Inspected a judgmental sample of Change Control schedules to determine whether upgrades, changes, and tests were scheduled appropriately.

- Inquired of the Server Administration Branch Manager and the LAN Supervisor to determine that a full system backup is performed prior to implementation of any changes to system software.
- Inquired of the Systems Programming staff to determine that SMP is used to manage and monitor changes to system software.
- Inspected a judgmental sample of documentation for mainframe system software products, which included release, version, and vendor information.
- Inspected a judgmental sample of the on-line user documentation including product manuals and help files maintained in BookManager.
- Inquired of the LAN Supervisor to determine that the Technical Services Branch is responsible for implementing and maintaining system software on the file and print, email and Internet servers.

Physical Security

Control Objective 4

Controls provide reasonable assurance that safeguards and/or procedures are used to protect computer equipment, storage media, and program documentation against intrusions, fire, and other hazards.

Tests of Operating Effectiveness Achieved

- Discussed with management procedures revoking physical access for departing employees, contractors, vendors and others separated from active involvement with COT.
- Inspected a judgemental sample of employees who had been terminated and ensured that the appropriate forms had been properly filled out by management and the physical access to the building had been removed.
- Discussed with management procedures for issuance of card keys to determine whether terminated or inappropriate personnel have access to the doors at the Commonwealth Data Center.
- Observed physical security procedures throughout the audit and verified the compliance with the Security Policies and Procedures Manual.
- Inspected a sample of card key access levels and discussed with management the appropriateness of the access levels.
- Verified card key access levels by selecting a sample of card keys and attempting to access doors and areas for which those keys should have been restricted.
- Observed physical security over the closet and safe that is used to store emergency user identifications for the various systems.
- Inspected reports from the card key system to determine that invalid access attempts and other reports are reviewed on a daily basis and significant issues are reported to management.
- Observed the armed officer monitoring the building entry sign-in forms and access to the Commonwealth Data Center and discussed the times and procedures for monitoring the CDC.

- Observed video cameras at the access points to the Commonwealth Data Center and computer rooms and discussed with management the procedures for reviewing and storing the CDs.
- Discussed procedures for admitting and escorting visitors in the Commonwealth Data Center and observed application of the procedure throughout the audit.
- Discussed procedures for training provided to employees regarding physical security and emergencies.
- Discussed Homeland Security procedures with management.
- Toured the Commonwealth Data Center building and the computer room and noted the presence and location of portable fire extinguishers (recent inspection), fire detection sensors and alarms, automatic fire extinguishing system, electrical power shut-off switch, telephone in the computer room that can dial directly outside, emergency lighting, and emergency exit signs.
- Toured the Commonwealth Data Center and computer room and noted the presence and location of a UPS system and generator.
- Toured the computer room and noted the presence and location of separate air conditioning units.

Logical Security

Control Objective 5

Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals.

Tests of Operating Effectiveness Achieved

- Reviewed the Security Policies and Procedures Manual and other security policies and brochures to evaluate management direction of logical security of the COT.
- Discussed with management the security policies for the various platforms at the COT.
- Discussed with management the policies and procedures for modifying the agency security contact list to determine appropriateness.
- Discussed with management procedures for adding, deleting, and changing user identifications and inspected documents to determine whether procedures for granting access and issuing user identifications and passwords are followed.
- Discussed with management procedures for revoking users and use of the Departing Employee Checklist.
- Discussed with management procedures for reviewing violation reports and security logs on the UNIX platforms at the COT to determine appropriateness.
- Inspected documents and reports to determine that COT security policies are implemented on the system settings for the various platforms at the COT.
- Inspected documents and reports to determine whether access to COT managed and controlled source program libraries is properly restricted.

- Inspected documents and reports to determine whether access to COT managed and controlled production program libraries is properly restricted.
- Discussed with management procedures for implementing security patches and “hot-fixes” on the systems at the COT.
- Discussed with management the procedures for individuals to gain dial-up access to system resources.
- Discussed with management procedures and responsibilities of staff to monitor the network security.
- Discussed with management procedures for reviewing violation reports and security logs on the mainframe platforms at the COT to determine appropriateness.
- Discussed with management the RACF Security Administrator System Emergency user profile.
- Discussed with management the firewall rules. Internet architecture, and controls in place to restrict network traffic to and from critical COT servers and the Kentucky Information Highway (KIH).
- Reperformed the application of the control procedure by inspecting a sample of exemption requests from the exemption request log to ensure deviations from the SPPM had documented authorization from the Security Branch.

Tests of Operating Effectiveness Not Achieved

- Inspected documents and reports to determine that COT security policies are implemented on the system settings for the Windows platforms at the COT.

  Finding: - Windows Server Password Expiration - Passwords for certain Windows domain servers are set to expire every 42 days, but the Security Policy and Procedures Manual (SPPM) dictates that passwords be set to expire every 31 days. In order to comply with policy as well as to decrease the possibility of password compromise, we recommend that management enforce a maximum password expiration of 31 days. Further, we encourage management to enforce security policies in the SPPM. Finally, we recommend that management perform a regular review of Windows servers to determine whether they remain in compliance with the SPPM.

  Management Response: COT agrees that the Windows servers’ password setting should be set to expire every 31 days. The 42 day setting was in the EAS domain only. This setting has been corrected to expire every 31 days in compliance with the SPPM. COT management is committed to the enforcement of our policies in the SPPM. COT will investigate the possibility of performing a regular review of the Windows servers.

- Discussed with management procedures for reviewing violation reports and security logs on the Windows platforms at the COT to determine appropriateness.

  Finding: - Windows Server Log Review - Windows server events are being logged, but review of the server logs occurs when server problems or incidents are identified. Therefore, Windows server event logs are not being proactively monitored to identify suspicious or unauthorized activity, which could result in potential risks going unidentified. From our discussions with management, Crowe Chizek understands that COT’s systems generate a large volume of events which are difficult to parse through for valid information. Due to the burdensome log size, manual log reviews do not result in value added procedures. To make this a meaningful control, we encourage management to continue evaluating automated tools for monitoring security logs. Once an automated solution is identified, we recommend management implement procedures for timely event log review. Procedures should include steps to be taken in the event suspicious activity is identified.

Management Response: COT management acknowledges the importance of proactively monitoring Window server event logs. Log reviews have been performed previously but did not result in cost effectiveness. The Security Administration Branch is currently reviewing a software solution that would attach to each server and pull the log information from the server into a centralized database. Once collected, the logs can be reviewed by automated rules that could be used to issue alerts to the Security group for further investigation. Once the current product has been tested COT will be able to make a determination as to whether it meets this need, by not only collecting and alerting from the logs, but also has retention capabilities to assist in retaining logs for historical review. If this product is not deemed sufficient or is cost prohibitive other products or processes will be considered for a long term solution to this issue.

Contingency Planning

Control Objective 6

Controls provide reasonable assurance that system and application backup procedures are performed; significant files are stored off-site.

Tests of Operating Effectiveness Achieved

Mainframe, UNIX, and Windows

- Discussed with management to verify that full system backups are created weekly and retained in the off-site storage facility.
- Reviewed procedures used to take daily backup tapes off-site to result in an adequate rotation schedule.
- Reviewed the log listing of the backup tapes, which are maintained off-site and verified that the tapes were present off-site.
- Observed the procedure of preparing the backup tapes for off-site delivery.
- Toured the off-site storage facility and noted that proper controls exist in the storage of backup tapes.
- Toured the off-site storage facility to determine whether a copy of the Disaster Recovery Manual and operations, systems and other reference materials are maintained off-site.
- Discussed with management the backup procedures in place for the systems at the COT.
- Toured the COT tape library and noted the organization of the tape-based media.
- Discussed tape labeling and logging procedures with management.

- Inquired of the Security and Recovery Branch Manager to determine the involvement of agencies in developing and testing back-up and recovery procedures.

Infrastructure

- Reviewed the log listing of the backup tapes, which are maintained off-site and verified that the tapes were present off-site.
- Discussed with management the backup procedures in place for the systems at the COT.
- Discussed with management the backup procedures in place for configuration files (firewalls, routers, email, LAN).
- Reviewed checklists, which document the procedures for the backing up of the e-mail servers.
- Toured the COT tape library and noted the organization of the tape-based media.
- Discussed tape labeling and logging procedures with management.
- Reviewed procedures used to take daily backup tapes off-site to result in an adequate rotation schedule.

Control Objective 7

Controls provide reasonable assurance that formal recovery plans have been developed to facilitate continued operations.

Tests of Operating Effectiveness Achieved

- Reviewed the Business Impact Analysis (BIA) performed and related documentation for appropriateness.
- Discussed with management the availability of compatible systems at the hot-site location and reviewed the hot-site agreement for all critical systems identified in the BIA and recovery strategies document.
- Obtained a copy of the recovery strategies document and reviewed it with management for discussion of strategies.
- Reviewed the results of the most recent disaster recovery test.
- Verified that off-site copies of the Disaster Recovery Manual exist.
- Reviewed the results of the inspection of the off-site storage location performed by COT.
- Toured the off-site storage location and observed physical security controls and presence of backup tapes according to schedules provided by COT.

Tests of Operating Effectiveness Not Achieved

- Reviewed the results of walkthroughs and table-top exercises with management.
- Reviewed the results of the Risk Assessment performed by management for potential disasters and the related effect on the Business Impact Analysis.

- Reviewed the recovery strategies document for infrastructure recovery strategies.
- Obtained a copy of the Disaster Recovery Manual and reviewed it for inclusion of systems identified as critical.

  Finding: - Contingency Planning **-** Crowe Chizek reviewed the Disaster Recovery procedures and related testing performed by management in the time period. Eight of the Disaster Recovery Manuals for applications that management has deemed critical do not have recovery procedures developed. Management has performed a Business Impact Analysis; however, the related Risk Assessment had not been performed. The plan also does not contain discussion of alternative recovery strategies for the infrastructure. Finally, management had not performed walkthroughs and table-top exercises in the time period. We encourage management to take the necessary steps to improve and continue to provide for a comprehensive disaster recovery plan.

  Management Response: COT management is committed to implementing a comprehensive DR plan. Therefore, COT will continue to identify critical systems and enhance recovery procedures for all systems. COT acknowledges the importance of assessing the risks and vulnerabilities of its information technology infrastructure and is currently working on a risk assessment of the Commonwealth Data Center (CDC) that will identify and outline risks to the facility and their associated impact to the State's information systems. Currently the assessment is in rough draft. Network Infrastructure alternate recovery strategies can not be fully completed until the risk assessment is complete. Departmental "walk-through" tests will continue to be scheduled throughout the year.

Computer Operations

Control Objective 8

Controls provide reasonable assurance that processing is scheduled appropriately and deviations are identified and resolved.

Tests of Operating Effectiveness Achieved

- Discussed with management as to the procedures of scheduling batch jobs.
- Discussed with management as to the appropriateness of users with access to modify job schedules and reviewed access to the schedule by inspecting documents and reports.
- Discussed with management their review of audit reports, which show changes made to agency job schedules.
- Reviewed operations, console logs, and job scheduling manuals for completeness.
- Discussed with management to verify that job scheduling reports are produced, which specify the completion of mission critical processing jobs, along with any abends or problems that occurred.
- Discussed with management the procedures used to monitor system activity, downtime, or system outages.
- Inquired of the management to determine that operators were on duty during regular shifts.
- Inspected a judgmental sample of the shift turnover logs to determine their use by operators.

- Inspected the Shift Procedures Manual to determine that it identifies specific tasks and approximate times that they should be performed.
- Inspected the COT Operator Manual to determine that the manual contained the following information:
    - Problem and Emergency Notification Contacts and phone numbers
    - System Service phone numbers
    - Problem Handling \ Escalation Procedures for the system as well as system applications
    - System and system application restart procedures
    - Weekly Maintenance Procedures
- Inspected a sample of daily console logs for system downtime documentation.
- Inspected a judgmental sample of the daily COT Evening Reports for help desk service items and abend documentation.
- Inspected a judgmental sample of Monthly Availability Reports displayed on-line as Server Metrics to determine whether system downtime is published.
- Inspected a judgmental sample of Weekly Change Schedules to determine that scheduled changes were included on the Monthly Availability Reports.
- Inquired of the management to determine communication of the Weekly Change Schedule to the users.
- Inquired of the management to determine what type of monitoring is performed in the LAN environment.
- Inquired of management to determine what tools were used by COT employees to perform capacity planning in the LAN environment.
- Inspected a judgmental sample of Nightly Cycle Documents to determine their use in reporting key information to senior management.
- Inquired of the Production Control Manager to determine the monitoring of the COT Scheduler Audit Report.

Tests of Operating Effectiveness Not Achieved

- Inspected a judgmental sample of the shift checklists to determine if they were completed by operators and reviewed by supervisors to ensure daily activities required for processing are performed.

  Finding: - Checklist Completion - Crowe Chizek reviewed 30 Shift Checklists to verify the existence, storage, completeness and evidence of managerial review of the shift turnover summary sheets and shift checklists. One of the 30 checklists sampled did not include evidence of supervisory review and 22 of the 30 checklists sampled lacked sign off on at least one task/job. Therefore, there was no assurance that the task/job was performed. We recommend that each summary sheet show evidence of managerial review and each task/job be signed off or at the minimum, note why the task/job was not required for the shift. These actions would provide additional assurance that the task/job was either performed or accounted for.

Management Response: COT is strongly committed to adhering to current operating procedures and concurs with the suggestions mentioned above. Our procedures work when enforced and therefore, COT Operations has implemented a double check for the accuracy and completion of the Shift Turnover documents. Each shift supervisor has been charged with ensuring items are checked by shift end and initialed. Each morning the Operations Supervisor or his designee goes through the check lists for verification and also initials the cover sheet. These actions will provide additional assurance that the task/job was either performed or accounted for.

Control Objective 9

Controls provide reasonable assurance that output data and documents are distributed to authorized recipients on a timely basis.

Tests of Operating Effectiveness Achieved

- Inquired of management as to the distribution methods for reports run by agencies.
- Inspected reports printed for agencies to determine banner pages included appropriate information.
- Inquired of management to determine that reports were being packaged and labeled for distribution to agencies.
- Inquired of the management to determine that RACF is used to control access to reports.
- Discussed print output distribution methods with operations management and personnel to determine adherence to standards.
- Discussed with management the use of schedules listing the reports to be provided to each agency.
- Toured the print operations room and noted that proper controls exist in limiting access to the room.
- Discussed with management the procedures in place to control the storage of outside vendor tapes.
- Reviewed agency forms used to control the storage and distribution of outside vendor tapes.

APPENDIX B – USER CONTROL CONSIDERATIONS

This section outlines specific user control considerations, or issues each agency may want to consider and address for the purpose of monitoring the data processing done by the COT. These considerations are not necessarily a comprehensive list of all internal accounting controls that should be employed by the user agency, nor do they represent procedures that may be necessary in all circumstances.

Organization Structure and Personnel

- Controls should be established to ensure that agency employees are adhering to Enterprises Policies.
- Controls should be established to ensure agencies are maintaining appropriate separation of duties.
- Controls should be established to ensure that the agency strategic planning documents follow the SITP and agencies actively participate in implementing the strategies defined in the SITP.

- Controls should be established to ensure that agencies properly use COT forms, policies, and procedures when interacting with or requesting items from the COT.

- Controls should be established to ensure cost allocations from COT services are appropriate.

- Controls should be established to ensure that employees are adequately trained.

Applications Maintenance and Documentation

- Controls should be established to ensure that all requests sent to COT are prioritized.

- Controls should be established to ensure that if time and budget estimates are presented by the COT, the time and budget estimates are reviewed and approved by the appropriate individuals at the agencies.

- Controls should be established to ensure that agencies properly test application changes prior to implementing changes or actively participate in user acceptance testing with the COT.

- Controls should be established to ensure that agencies creating changes and forwarding these changes to COT for promotion into production control the movement of changes to COT.

- Controls should be established to ensure that software supported by out-side vendors is properly tested prior to implementation of the software application or change.

- Controls should be established to ensure that the agencies, when responsible, make only approved, tested and documented changes to software when appropriate.

- Controls should be established to ensure that the agencies, when responsible, determine and authorize access to programming source and programming load libraries/directories to ensure proper segregation of duties between development and change control.

APPENDIX B – USER CONTROL CONSIDERATIONS

System Software and Hardware

- Controls should be established to ensure that agencies, when responsible, install only appropriate system software in the their systems.

- Controls should be established to ensure that the agencies, when responsible, make only approved, tested, and documented changes to system software.

- Controls should be established to ensure that the agencies participate or review change control documentation at the COT for the weekly change control meetings.

- Controls should be established to ensure that agencies, when responsible, install only appropriate system software in the network environments.

Logical Security

- Controls should be established at the agencies for reviewing the COT Agency IBM OS/390 Security Agreement and ensuring compliance with the terms of the agreement.

- Controls should be established at the agencies for designating an IBM OS/390 authorized security contact.

- Controls should be established for those agencies that are responsible for their own RACF administration to restricting access to data sets and programs under the RACF Security software and for monitoring security reports provided by the COT.

- Controls should be established for those agencies that are responsible for their own RACF administration to review and monitor the CA Scheduler listing to identify and remove users that are no longer required to have access to the system.

- Controls should be established for those agencies that are responsible for resetting their own passwords on the IBM OS/390 to ensure that this activity is appropriately restricted.

- Controls should be established at the agencies to ensure that only authorized individuals have access to their programs and data in both the mainframe and client/server environment.

- Controls should be established at the agencies for controlling access to IBM’s RMDS and Mobius’s View Direct for reports and assigning access to these in RACF.

- Controls should be established at the agencies to ensure that agency employees are using strong passwords and adhering to COT recommended standards for passwords.

- Controls should be established at the agencies to ensure that agency employees are appropriately removed from the systems at the COT upon termination of their employment or changes in responsibilities.

- Controls should be established at the agencies to ensure that agency employee access to applications and data are properly controlled.

- Controls should be established at the agencies to ensure that each generic user identification is assigned to the appropriate authorized individual.

- Controls should be established at the agencies to ensure that the agencies are adhering to COT enterprise security standards.

- Controls should be established at the agencies to ensure that proper firewall rule sets are in place to protect the agency network from malicious content that may originate from within the KIH intranet.

- Controls should be established at the agencies to ensure that proper controls exist to only permit authorized individuals VPN access.

Back-up and Contingency Planning

- Controls should be established to ensure that agency data residing on tapes or cartridges is backed up by the agency and communicated to COT for off-site storage.

- Controls should be established to ensure that the agency informs the COT of the criticality of the data, files, programs, etc. that should be backed up and the off-site rotation for these items.

- Controls should be established to ensure that the agency designates a disaster recovery coordinator that is responsible for coordination of recovery procedures with the COT.

- Controls should be established to ensure that the agencies participate in business impact analysis with the COT to determine risks and recovery priorities.

- Controls should be established to ensure that Agency Disaster Recovery procedures, critical applications, and critical circuits are identified and communicated to COT.

Computer Operations

- Controls should be established to ensure that agency batch jobs are properly scheduled and run in accordance with the schedule.

- Controls should be established to ensure that only properly authorized individuals have access to maintain batch job schedules and libraries.

- Controls should be established to ensure that agencies monitor and document abends that occur related to their applications and batch jobs.

- Controls should be established to ensure that reports generated at COT are received and distributed to the appropriate individuals in a timely manner.

APPENDIX B – USER CONTROL CONSIDERATIONS

- Controls should be established at the agencies to ensure that only authorized individuals have access to their programs and data in both the mainframe and client/server environment.

- Controls should be established at the agencies to ensure that data transmissions are complete, accurate, and secure.

- Controls should be established to ensure that the agencies reconcile the number of records sent to COT with the number of records actually received and processed by COT.

- Controls should be established to ensure that the agencies reconcile the number of records received at the agency with the number of records actually sent by COT.

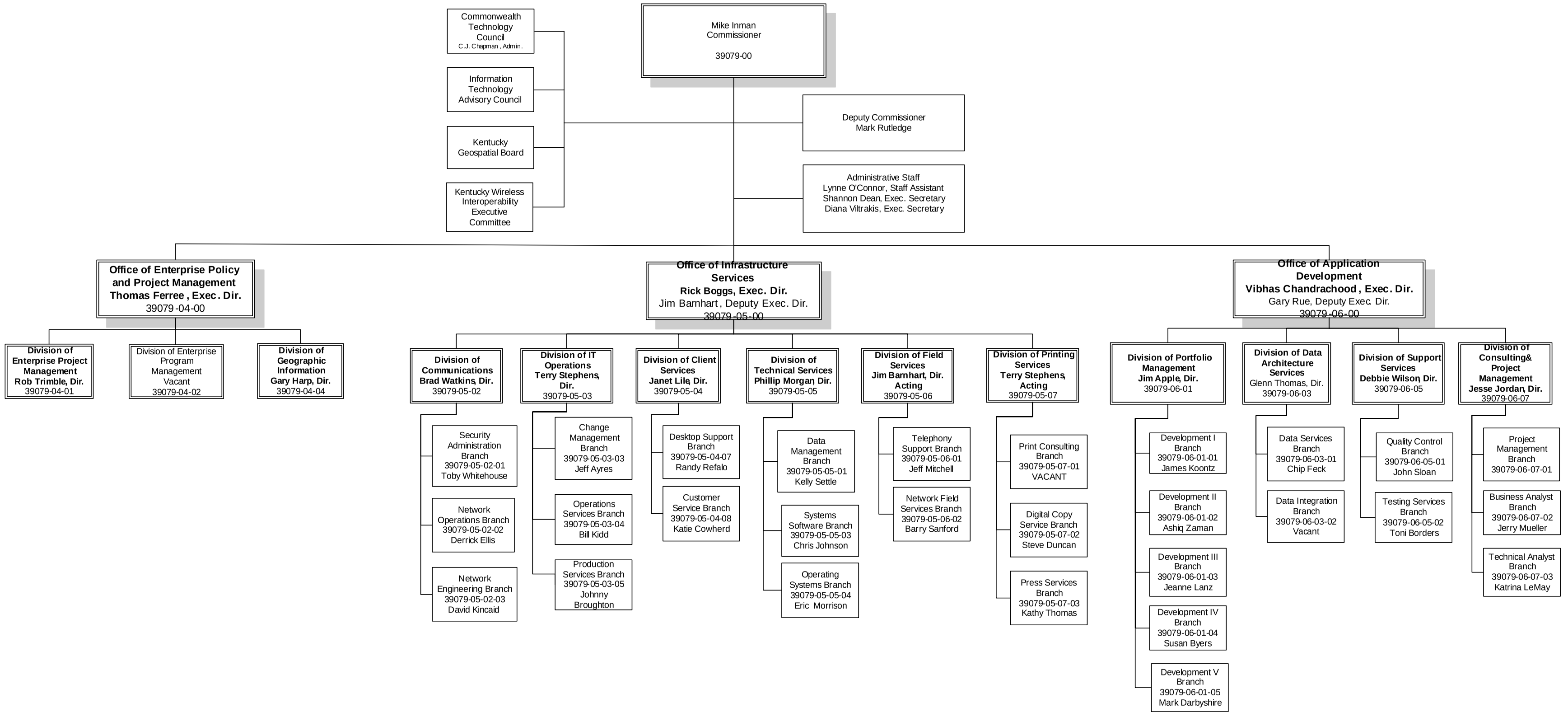
- Controls should be established to ensure that the agencies review the Awareness Reports as they are issued.

- Controls should be established to ensure that the agencies review the Evening Reports.

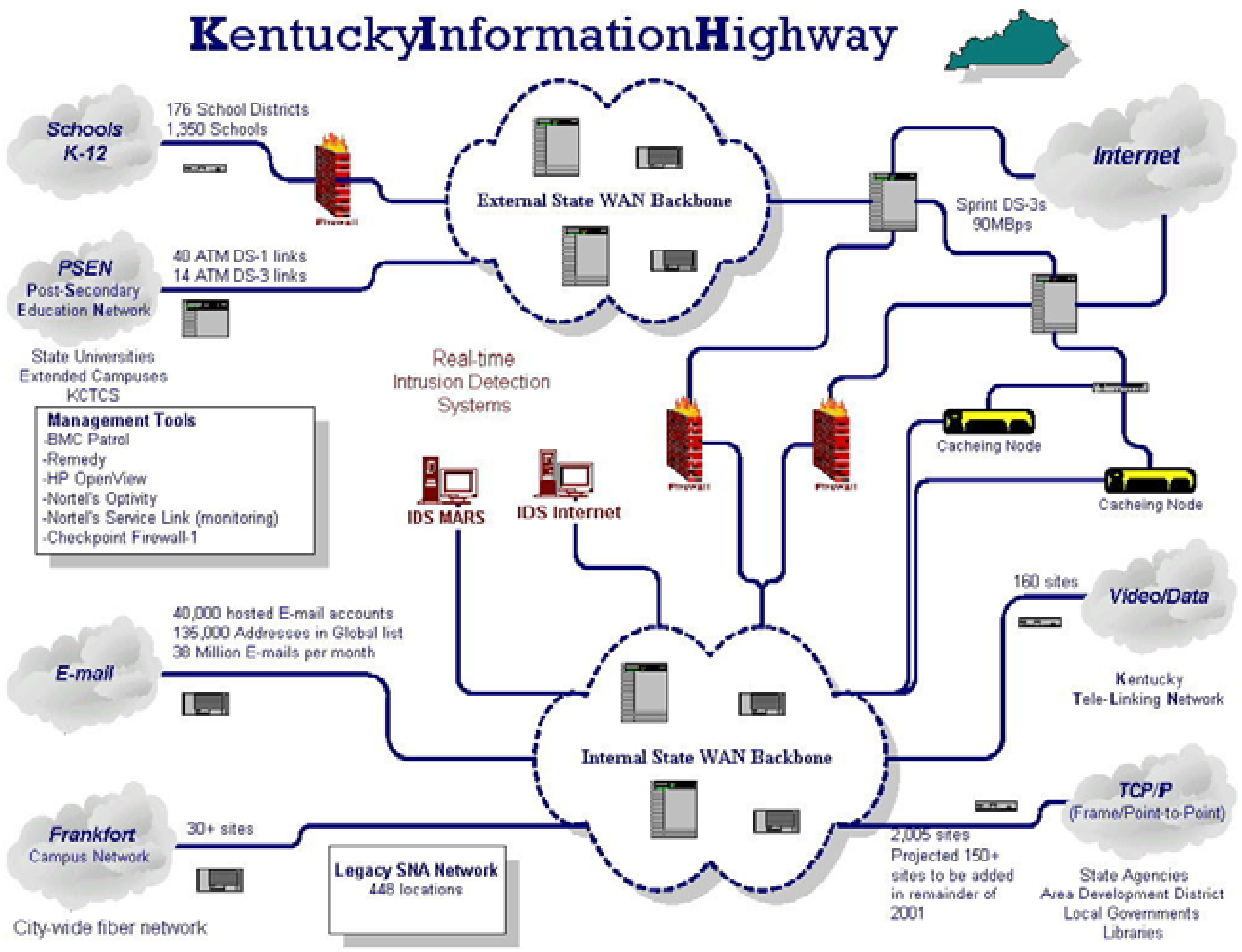
- Controls should be established to ensure that the agencies review the Change Control postings.

APPENDIX C – ORGANIZATIONAL CHART

Commonwealth Office of Technology
Organization
Jan. 31, 2006


Commonwealth Technology Council C.J. Chapman , Admin.
Information Technology Advisory Council
Kentucky Geospatial Board
Kentucky Wireless Interoperability Executive Committee
Mike Inman Commissioner 39079-00
Deputy Commissioner Mark Rutledge
Administrative Staff Lynne O'Connor, Staff Assistant Shannon Dean, Exec. Secretary Diana Viltrakis, Exec. Secretary
Office of Enterprise Policy and Project Management Thomas Ferree , Exec. Dir. 39079 -04-00
Division of Enterprise Project Management Rob Trimble, Dir. 39079-04-01
Division of Enterprise Program Management Vacant 39079-04-02
Division of Geographic Information Gary Harp, Dir. 39079-04-04
Office of Infrastructure Services Rick Boggs, Exec. Dir. Jim Barnhart , Deputy Exec. Dir. 39079 -05-00
Division of Communications Brad Watkins, Dir. 39079-05-02
Security Administration Branch 39079-05-02-01 Toby Whitehouse
Network Operations Branch 39079-05-02-02 Derrick Ellis
Network Engineering Branch 39079-05-02-03 David Kincaid
Division of IT Operations Terry Stephens, Dir. 39079-05-03
Change Management Branch 39079-05-03-03 Jeff Ayres
Operations Services Branch 39079-05-03-04 Bill Kidd
Production Services Branch 39079-05-03-05 Johnny Broughton
Division of Client Services Janet Lile, Dir. 39079-05-04
Desktop Support Branch 39079-05-04-07 Randy Refalo
Customer Service Branch 39079-05-04-08 Katie Cowherd
Division of Technical Services Phillip Morgan, Dir. 39079-05-05
Data Management Branch 39079-05-05-01 Kelly Settle
Systems Software Branch 39079-05-05-03 Chris Johnson
Operating Systems Branch 39079-05-05-04 Eric Morrison
Division of Field Services Jim Barnhart, Dir. Acting 39079-05-06
Telephony Support Branch 39079-05-06-01 Jeff Mitchell
Network Field Services Branch 39079-05-06-02 Barry Sanford
Division of Printing Services Terry Stephens, Acting 39079-05-07
Print Consulting Branch 39079-05-07-01 VACANT
Digital Copy Service Branch 39079-05-07-02 Steve Duncan
Press Services Branch 39079-05-07-03 Kathy Thomas
Office of Application Development Vibhas Chandrachood , Exec. Dir. Gary Rue, Deputy Exec. Dir. 39079 -06-00
Division of Portfolio Management Jim Apple, Dir. 39079-06-01
Development I Branch 39079-06-01-01 James Koontz
Development II Branch 39079-06-01-02 Ashiq Zaman
Development III Branch 39079-06-01-03 Jeanne Lanz
Development IV Branch 39079-06-01-04 Susan Byers
Development V Branch 39079-06-01-05 Mark Darbyshire
Division of Data Architecture Services Glenn Thomas, Dir. 39079-06-03
Data Services Branch 39079-06-03-01 Chip Feck
Data Integration Branch 39079-06-03-02 Vacant
Division of Support Services Debbie Wilson, Dir. 39079-06-05
Quality Control Branch 39079-06-05-01 John Sloan
Testing Services Branch 39079-06-05-02 Toni Borders
Division of Consulting& Project Management Jesse Jordan, Dir. 39079-06-07
Project Management Branch 39079-06-07-01
Business Analyst Branch 39079-06-07-02 Jerry Mueller
Technical Analyst Branch 39079-06-07-03 Katrina LeMay

APPENDIX D – KENTUCKY INFORMATION HIGHWAY


KentuckyInformationHighway
Schools K-12
176 School Districts
1,350 Schools
Firewall
External State WAN Backbone
Internet
Sprint DS-3s
90MBps
PSEN
Post-Secondary Education Network
40 ATM DS-1 links
14 ATM DS-3 links
State Universities
Extended Campuses
KCTCS
Real-time
Intrusion Detection
Systems
Management Tools
-BMC Patrol
-Remedy
-HP OpenView
-Nortel's Optivity
-Nortel's Service Link (monitoring)
-Checkpoint Firewall-1
IDS MARS
IDS Internet
Firewall
Firewall
Cacheing Node
Cacheing Node
160 sites
Video/Data
Kentucky
Tele-Linking Network
E-mail
40,000 hosted E-mail accounts
136,000 Addresses in Global list
38 Million E-mails per month
Internal State WAN Backbone
Frankfort
Campus Network
30+ sites
City-wide fiber network
Legacy SNA Network
448 locations
2,005 sites
Projected 150+
sites to be added
in remainder of
2001
TCP/IP
(Frame/Point-to-Point)
State Agencies
Area Development District
Local Governments
Libraries