

**METROPOLITAN EDUCATIONAL COUNCIL (MEC)  
STATE REGION - ISA, FRANKLIN COUNTY**

**SAS - 70**

**AUGUST 16, 2008 THROUGH JULY 17, 2009**



**Mary Taylor, CPA**  
Auditor of State



---

**TABLE OF CONTENTS**

<b>I</b>	<b>INDEPENDENT ACCOUNTANTS' REPORT</b> .....	<b>1</b>
<b>II</b>	<b>ORGANIZATION'S DESCRIPTION OF CONTROLS</b> .....	<b>3</b>
	CONTROL OBJECTIVES AND RELATED CONTROLS .....	3
	OVERVIEW OF OPERATIONS .....	3
	RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING .....	4
	Control Environment.....	4
	Risk Assessment.....	6
	Monitoring.....	6
	INFORMATION AND COMMUNICATION .....	6
	GENERAL EDP CONTROLS.....	7
	Development and Implementation of New Applications or Systems.....	7
	Changes to Existing Applications and Systems .....	7
	IT Security .....	8
	IT Operations.....	12
	User Control Considerations .....	14
<b>III</b>	<b>INFORMATION PROVIDED BY THE SERVICE AUDITOR</b> .....	<b>15</b>
	GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS.....	16
	Changes to Existing Applications and Systems .....	16
	IT Security .....	17
	IT Operations.....	24
<b>IV</b>	<b>OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION</b> .....	<b>27</b>
	Information Technology Center Profile.....	27

**This Page Intentionally Left Blank**



# Mary Taylor, CPA

Auditor of State

## INDEPENDENT ACCOUNTANTS' REPORT

Governing Board  
Metropolitan Educational Council (MEC)  
2100 CityGate Drive  
Columbus, Ohio 43219

To Members of the Board:

We have examined the accompanying description of controls of the Metropolitan Educational Council (MEC) applicable to the processing of transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS), and Education Management Information System (EMIS). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the MEC'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 internal controls contemplated in the design of the MEC's controls; and (3) such controls had been placed in operation as of July 17, 2009. The MEC uses the services of the Northwest Ohio Computer Association (NWOCA) for systems development and maintenance of the USAS, USPS, SAAS/EIS and EMIS. The accompanying description includes only those controls and related control objectives of the MEC, and does not include controls and related control objectives of NWOCA. Our examination did not extend to controls of NWOCA. The control objectives were specified by the MEC management for the processing of USAS, USPS, SAAS/EIS, and EMIS with the assistance of the Ohio Department of Education. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of the MEC's controls that had been placed in operation as of July 17, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the MEC's controls.

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 Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from August 16, 2008 to July 17, 2009. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user organizations of the MEC 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 Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance the control objectives specified in Section III were achieved during the period from August 16, 2008 to July 17, 2009.

The relative effectiveness and significance of specific controls at the MEC 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 information in Section IV describing the Metropolitan Educational Council is presented by the MEC to provide additional information and is not part of the MEC's description of controls that may be relevant to a user organization's internal control. Such information has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for user organizations and, accordingly, we express no opinion on it.

The description of controls at the MEC is as of July 17, 2009, and information about tests of the operating effectiveness of specified controls covers the period from August 16, 2008 to July 17, 2009. 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 specific controls at the MEC 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 (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of the MEC, its user organizations, and the independent auditors of its user organizations.

A handwritten signature in cursive script that reads "Mary Taylor".

**Mary Taylor, CPA**  
Auditor of State

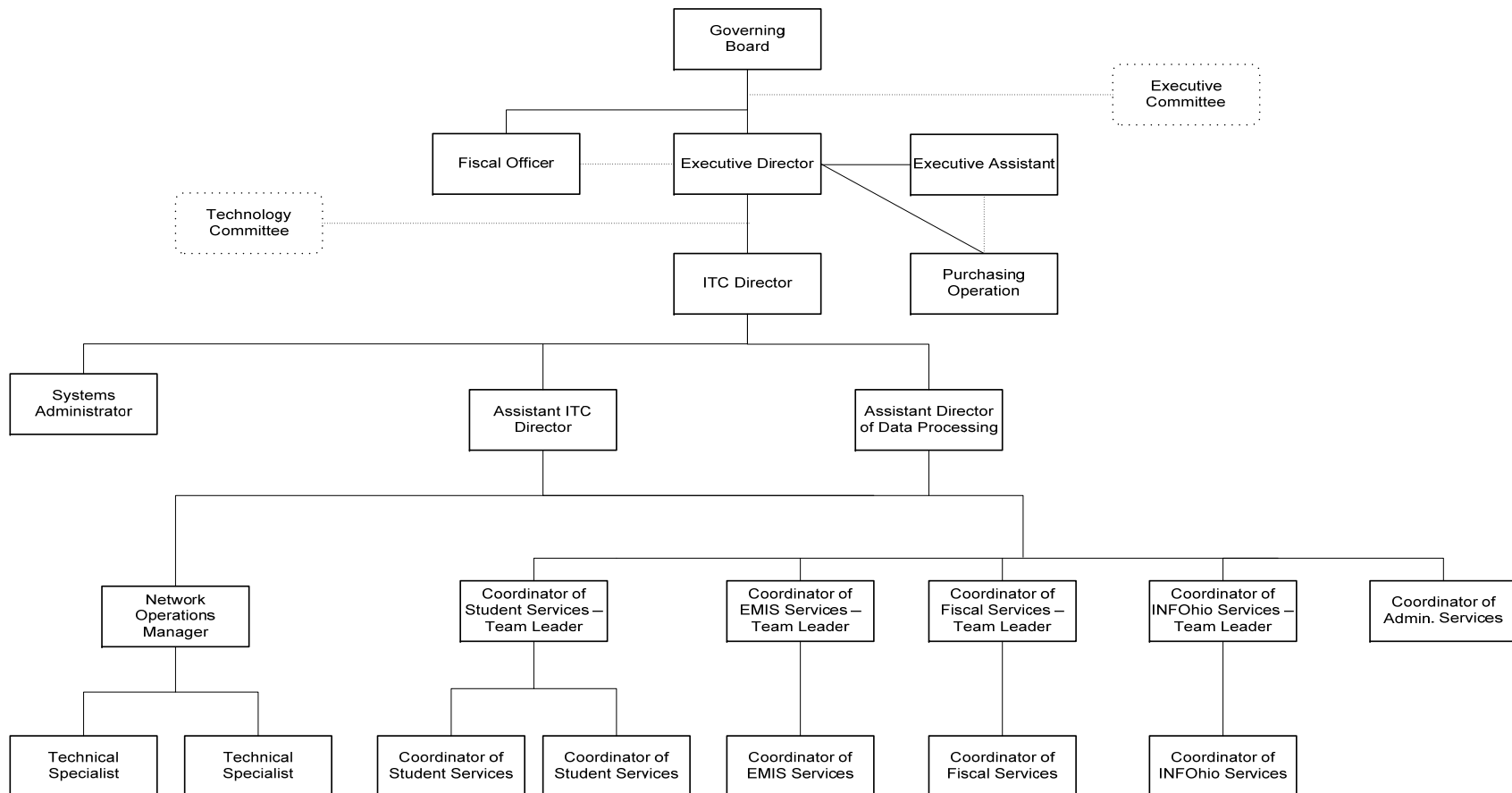
July 17, 2009

## SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

### CONTROL OBJECTIVES AND RELATED CONTROLS

The Metropolitan Educational Council (MEC) control objectives and related controls are included in section III of this report, "Information provided by the Service Auditor," to eliminate the redundancy that would result from listing them here in section II and repeating them in section III. Although the control objectives and related controls are included in section III, they are, nevertheless, an integral part of the MEC's description of controls.

### OVERVIEW OF OPERATIONS



The Metropolitan Educational Council (MEC) is one of 23 governmental computer service organizations serving more than 900 educational entities and 1.4 million students in the state of Ohio. These service organizations, known as Information Technology Centers (ITCs) and their users make up the Ohio Education Computer Network (OECN) authorized pursuant to Section 3301.075 of the Revised Code. Such sites, in conjunction with the Ohio Department of Education (ODE), comprise a statewide delivery system to provide comprehensive, cost-efficient accounting and other administrative and instructional computer services for participating Ohio entities. Funding for this network and for the MEC is derived from the state of Ohio and from user fees.

ITCs provide information technology services to school districts, community (charter) schools, JVS/career & technical, educational service centers (ESCs) and parochial schools; however, not all entities subscribe to the same services. Throughout the remainder of the report, the term “user organization” will be used to describe an entity which uses one or more of the following applications:

- Uniform School Accounting System (USAS).
- Uniform Staff Payroll System (USPS).
- School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS).
- Education Management Information System (EMIS).
- School Options Enrollment System (SOES).

ITCs are organized as either consortia under ORC 3313.92 or Council of Governments (COG) under ORC 167. ORC 3313.92 allows for school districts to create a partnership (a consortia) to resolve mutual needs. One of the members of the consortia is designated as fiscal agent. The fiscal agent provides all accounting, purchasing, and personnel services for the consortia. A “COG” under ORC chapter 167 allows for one or more governmental entities to join together to form a new legal entity. A COG can have its own treasurer, make its own purchases, hire staff, and have debt obligations. The MEC is organized under ORC 167 and has their own treasurer.

## **RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING**

### **Control Environment**

Operations are under the control of the ITC director and the MEC governing board. The governing board is the governing body of the MEC and is composed of individuals from the user organizations. User organizations within Franklin County each appoint a board of education member and a member of the administrative staff to serve on the governing board. One is designated as the official appointee and the other is designated as the alternate. When a majority of the user organizations of any county other than Franklin become members of MEC, said user organization of that county select a single district to represent them on the governing board of MEC. The board meets at least four times per year. The board has also established the executive committee and the technology committee to assist in the operation of the MEC and its programs.

The technology committee is concerned mainly with the operation, management and future planning for MEC. The committee assumes responsibility for and makes recommendations to the governing board in each of the following areas: operation and management; finance; constitution and bylaw; personnel policies; evaluation and planning. The technology committee exercises governing board authority over the operation of the MEC and the delivery of technology services consistent with MEC’s constitution and bylaws.

The MEC employs a staff of 17 individuals and is supported by the following functional areas:

<i>Fiscal Services:</i>	Supports end users in all aspects of the state software applications, including USAS, USPS, SAAS/EIS, and EMIS.
<i>Student Services:</i>	Supports end users in all aspects of the student service applications with a focus on EMIS and assists in the EMIS software development.
<i>Educational Technology:</i>	Provides a variety of educational technology services to subscribing MEC districts including software and Internet access, training, technology planning, technical assistance, and grant writing assistance. Also supports end users in all aspects of the INFOhio program.
<i>Network/Systems Support:</i>	Supports the MEC computer systems and its networked communication system. Also, provides support and training for users.

The MEC is generally limited to recording user organization transactions and processing the related data. User organizations are responsible for authorization and initiation of all transactions. Management reinforces this segregation of duties as a part of its new employees' orientation process, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced MEC employees may alter user data and only at the request of the user organization. When a user organization experiences a problem requiring data to be changed, experienced MEC staff makes the necessary changes to the data in the test environment whenever possible. This reduces the likelihood of processing errors. The user is then walked through the process to change their data in the production system. However, there are times when it is necessary for changes to be made by the MEC staff. In practice, requests are required to be made by treasurers or their designee and are usually received via e-mail. However, MEC does not have a written policy or standard procedure to ensure these requests are handled consistently and documented by all MEC staff.

The MEC follows personnel policies and procedures as outlined in the MEC Personnel Policies and Procedures Manual. When necessary, additional MEC policies have been developed and approved by the governing board to address the concerns of MEC. Detailed job descriptions exist for all positions. The MEC is constantly re-evaluating its need for personnel to provide for the increasing range of services provided. The reporting structure and job descriptions are periodically updated to create a more effective organization. Each MEC employee is evaluated continually by the ITC director and through customer feedback surveys. The executive director is responsible for performing the evaluation of the ITC director.

The MEC's hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the organization require some type of college degree in a computer-related field, and all the MEC staff members are required to attend professional development and other training as a condition of continued employment. Each staff member must attend at least fifteen hours of approved professional development training annually, and at least eighty hours of approved training every four years. In addition, management encourages staff members to obtain additional training by providing a tuition reimbursement program for approved college work, and by paying 100% of incurred costs in attending professional development seminars.

MEC is also subject to ITC Site Reviews by the Technology Solutions Group of the Management Council – Ohio Education Computer Network MCOECN ([mctsg](#)). These site reviews are conducted by a team consisting of an employee of the Ohio Department of Education (ODE), two current and/or former school district administrators, two current and/or former ITC directors, and one additional team member to provide training to subsequent teams. Approximately three to five ITC site reviews are conducted annually. The sites chosen for review are designated by the OECN

Oversight Advisory Committee as approved by ODE. The guidelines and recommended procedures for these reviews are based on the Ohio Administrative Code, which cover the following areas: governance, administration, finance, personnel and staff development, physical facilities, hardware, software, user in-service, and operations. The MEC's ITC site review has not yet been scheduled.

Every five years, the MEC requires their user organizations to sign a Computer Services Agreement. Exhibit A of the Computer Services Agreement outlines the DP Services which includes services, charges and billing, MEC's obligations, and the customer's obligations. In addition, the MEC annually distributes a schedule to all user organizations with all services and their associated costs as set forth by the governing board.

### **Risk Assessment**

The MEC does not have a formal risk management process; however, the governing board actively participates in the oversight of the organization. As a regular part of its activity, the governing board addresses:

- New technology.
- Realignment of the MEC organization to provide better service.
- Personnel issues, including hiring, termination and evaluations.
- Additional services provided to user organizations and other entities.
- Changes in the operating environment as a result of ODE requirements, Auditor of State (AOS) and other accounting pronouncements, and legislative issues.

In addition, the MEC has identified operational risks resulting from the nature of the services provided to the user organizations. These risks are primarily associated with computerized information systems. These risks are monitored as described under "Monitoring" below and in additional detail throughout the General EDP Control section of this report.

### **Monitoring**

The MEC organization is structured so that team leaders report directly to the ITC director. Key management employees have experience with the oversight of the MEC or its user organizations and are familiar with the systems and controls. The MEC ITC director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

Hardware, software, network, database integrity, Internet usage, and computer security reports are monitored on an ongoing basis by departmental management. Some of these reports are automatically run through a scheduler program and sent to management via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily. In addition, the assistant director of data processing and system administrator receive the same reports and monitor them for interrelated and recurring problems.

### **INFORMATION AND COMMUNICATION**

The aspects of the information and communication component of internal control, as they affect the services provided to user organizations are discussed within the General EDP and Financial Application control sections.

---

## GENERAL EDP CONTROLS

### Development and Implementation of New Applications and/or Systems

The MEC staff does not perform system development activities. Instead, the MEC utilizes the software developed and supplied by the State Software Development Team (SSDT), located at the Northwest Ohio Computer Association (NWOCA), another ITC of the OECN. The ODE determines the scope of software development for state-supported systems. Tactical means of accomplishing software development priorities are determined by the Software Advisory Committee (SAC), which consists of members from the Management Council of the OECN (MCOECN), the Ohio Association of School Business Officials (OASBO), the ODE, and the SSDT. The SAC meets four times per year to discuss the status of proposed and ongoing projects.

### Changes to Existing Applications and/or Systems

User organizations participate in the program development/change process via the Software Performance Report/Request (SPR) tracking procedure, which is maintained by the SSDT. The SPR system uses SiteScape Forum, which is used for electronic conferencing, to accept and discuss proposed software enhancements in a public forum. Each major software package (USAS, USPS, SAAS, EMIS) has its own Public and ITC forum which is monitored by the SSDT system analysts. All OECN ITCs and a majority of user organizations have access to forum conferences, providing end-user participation in the program development/change process.

The MEC personnel do not perform program maintenance activities. Instead, they utilize the applications supplied to them by the SSDT. The OECN requires the ITC to keep the version of each application current based on the provider's standard for continued support. Procedures are in place to ensure the SSDT developed applications are used as distributed. The SSDT, at NWOCA, copies zipped files containing the quarterly updates to the ITCs' systems. The source code is not distributed with these files. Release notes are contained within these files and explain the changes, enhancements and problems corrected. User and system manager manuals are also distributed with these releases. The SSDT informs the ITCs that they will support only the latest release of the state software beginning 30 days following the software release date.

The MEC uses a software utility, called OECN\_INSTALL, to unpack these zipped files and install each individual package into its proper OECN directory. The OECN\_INSTALL utility has two options which will either install the new release on the system or install a patch for the current release. This utility ensures that all required components are installed properly and consistently.

Only vendor supplied changes are made to the operating system or system software documentation. The Northern Buckeye Education Council (NBEC), who acts as the fiscal agent for this and other participating ITCs, has entered into a license under the Campuswide Software License Grant Program (CSLG) through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of HP software packages.

The services acquired and/or provided by the NBEC under the agreement include the following:

- Provide for the acquisition and distribution of software media for the participating ITCs for a limited series of HP software packages as approved by the board of trustees of the MCOECN.

- Provide telephone technical support to the participating ITCs' technical staff for a limited series of HP software packages approved by the board of trustees of the MCOECN.
- Track and maintain an accurate listing of all HP hardware and software covered under the agreement.
- Provide periodic training and update sessions covering the policies and regulations governing this program as well as updating the ITCs' technical staff on the latest releases of HP software packages covered under the agreement.

As a participating member of the program of the MCOECN the participating ITCs agree to the following:

- Read, sign, and comply with the rules and regulations of the CSLG Program and the Education Software Library (ESL) Program as operated by the NBEC on behalf of the MCOECN.
- Provide unrestricted privileged access to all computer systems covered under the agreement for the purposes of identifying and/or correcting problems of distributed software.
- Provide HP or MCOECN representatives, upon prior written notice, with physical access to computer facilities at reasonable times during normal business hours to inspect sites and system records for compliance with the terms of the CSLG and ESL Programs.
- Make payments to NBEC for services under the agreement within 30 days of the receipt of an invoice for said services.

Before new releases are installed at the MEC, a backup of the application or operating system affected by the change is prepared to ensure retention of the existing application or operating system in case of an error stemming from the upgrade process.

Documentation for the current version of the operating system and new releases are provided on the HP web site. New releases include documented changes to the operating system and implementation procedures. In addition, the MEC has purchased a copy of the operating system disks from INS, a third-party vendor in partnership with the MCOECN. This is part of the Technology Solutions Group program under the MCOECN (mcoetsg). This program allows the MEC to purchase the operating system software at a reduced cost.

### **IT Security**

The MEC has a computer security and usage policy that outlines the responsibilities of user organization personnel, the MEC personnel, and any individual or group not belonging to the user organization or MEC. Additionally, the MEC uses a banner screen that is displayed when a user logs on to the system. The screen informs the user that use of the system expresses their consent to the security policies of the MEC. The MEC staff members are granted access within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities. Access for new MEC staff is requested by the ITC director, assistant ITC director, or assistant director of data processing. The new employee setup form is used as a checklist for granting access.

Users are granted access upon completion of the account authorization form. Access must be authorized by the user organization management. These authorization forms are sent to MEC to create/update the account and notify the user organization management regarding the newly established account. The authorization forms are maintained by appropriate MEC staff. E-mail requests for user accounts are also accepted by

the MEC. The MEC has only maintained requests for new user or updates to user access for approximately three years.

A listing that indicates user access and privileges within the user organization is sent annually to the respective user organization management to verify the present users on the system were properly authorized.

Access to the Internet has been provided to the user organizations of MEC. Each user organization is responsible for its own Internet acceptable use policies. All documentation pertaining to Internet access and usage policies is maintained by the individual user organizations.

The MEC policies and procedures are partly enforced through the use of system alarms and audits. Security alarm messages are sent to an operator terminal that has been enabled to receive security event messages. Security audit messages are sent to the audit log file; alarms are sent to the operator log file. Access to the operator log and audit log is limited to technology center personnel. Critical events should be reported as both alarms and audits; less critical events can be written to a log file for later examination. The following security alarms and security audits have been enabled to monitor any security violations on the MEC systems:

- AUTHORIZATION: Enables monitoring of changes made to the system UAF or network proxy authorization file in addition to changes to the rights database.
- INSTALL: Provides the ability to audit the use of the install utility which is used to install an image or remove an installed image..
- BREAK-IN: Produces a record of break-in attempts. The DIALUP, LOCAL, REMOTE, NETWORK, DETACHED and SERVER break-in types can be monitored.
- LOGFAILURE: Provides a record of logon failures. The BATCH, DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESS and DETACHED logon failure types can be monitored.

A batch processed command procedure executes each night to extract security violations from the audit log and creates summary and detail reports. These reports, also called Security Monitor Reports, are e-mailed to the systems administrator and are reviewed daily. If an event is deemed suspicious, it is investigated further to determine the exact nature of the event and the corrective action needed.

MEC uses Symantec Anti-Virus software on Microsoft Windows based network servers and desktop workstations to scan all inbound and outbound e-mail. Anti-Virus definitions are automatically updated on a regular basis. Additionally, MEC uses Proof Point Messaging Security Gateway to protect from e-mail based viruses and spam. If a virus is found, the e-mail is quarantined.

Primary logical access control to the HP computers is provided by security provisions of the operating system. This includes access to data, programs and system utilities. When a user logs in to use the system interactively, or when a batch or network job starts, the operating system creates a process which includes the identity of the user. The operating system manages access to the process information using its authorization data and internal security mechanisms.

A proxy login enables a user logged in at a remote node to be logged in automatically to a specific account at the local node, without having to supply access control information. A proxy login differs from an interactive login because an interactive login requires a user to supply a user name and password before the user can perform interactive operations. Proxy records are located in the proxy file. The MEC does not use proxy logins.

The User Identification Codes (UIC) are individually assigned to all technology center personnel employed at the MEC. For organizations that use the MEC system, UICs are assigned at both the group level and user level. Group level UICs are assigned by user organization. With the exception of student information system software accounts, user level UICs are individually assigned. UIC based protection controls access to objects such as files, directories, and volumes.

Certain limited-access accounts require a less restrictive environment than captive accounts. Accounts, under which network objects run, for example, require temporary access to DCL. Such accounts must be set up as restricted accounts, not captive accounts. User accounts should be set with the RESTRICTED flag instead of the CAPTIVE flag if they need to use network applications like MAIL or network proxy accounts. The RESTRICTED flag is used for all user accounts not belonging to the MEC or the system.

The system forces users to periodically change their passwords. All MEC staff have a pre-set password that is different from the one used by the user organizations. The user organization accounts were setup so that their password change interval in accordance with MEC's policy. Passwords are set to expire when a new user account is issued or when an existing user requests a password change. This parameter requires the user to change their password during the first logon procedure. The minimum password length for each user is typically the default for normal users and a different length for all MEC staff.

The operating system has system parameters which, when set appropriately, control and monitor sign-on attempts.

There are parameters in place to control certain aspects of the sign-on procedure, which include the following:

- The terminal name is part of the association string for the terminal mode of break-in detection.
- The user is restricted on the length of time they have to correctly enter a password on a terminal on which the system password is in effect.
- The number of times a user can try to log in over a phone line or network connection. Once the specified number of attempts has been made without success, the user is locked out of the system for a predetermined period of time.
- The length of time allowed between login retry attempts after each login failure.
- The length of time a user terminal, or node, is permitted to attempt a logon before the system assumes that a break-in attempt is occurring and evasive action is taken.
- The period for which evasive action is taken is variable and will grow as further logon failures are detected from the suspect source.
- The number of retry attempts allowed for users attempting to logon before evasive action consists of refusing to allow any logons during a designated period of time.

System parameter standards have been established through the use of HP established defaults. Any changes are recorded in the configuration file for review by the systems administrator.

A timeout program, WATCHER, is used to monitor terminal inactivity and log-off inactive users after a predetermined period of time of non-use. The program is set to run only during non-business hours. The use of this program helps to reduce the risk of an unattended terminal being used to enter unauthorized transactions.

Associated with each object recognized by the operating system may be an Access Control List (ACL). When an access request is made to an object, ACLs are always checked first. An ACL may either grant or deny access to the user requesting it. When an ACL fails to specifically grant access, the system then defaults to UIC-based protection.

The system directory contains security files that control the security parameters for the system. When a user attempts to gain access to an object, such as a file or directory, the system compares the user's UIC to the owner's UIC for that object. In UIC-based protection, the relationship between the user's UIC and the object's UIC determines whether access is granted. Owner relationships are divided into four categories:

**SYSTEM:** Any of the following: (1) Users with a UIC group number between 1 and the MAXSYSGROUP number. (2) Users with system privileges. (3) Users with group privileges whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

**OWNER:** Users with the same UIC as the object's owner.

**GROUP:** Users with the same UIC group number as the object's owner.

**WORLD:** All users, including those in SYSTEM, OWNER, and GROUP.

Through the protection code, each category of users can be allowed or denied read, write, execute, and delete access. The default file protection is for (1) SYSTEM having read, write, execute, and delete capabilities; (2) OWNER having read, write, execute, and delete capabilities; (3) GROUP having read and execute capabilities; and (4) WORLD having no access capabilities.

Certain privileges can override all UIC-based and ACL protection. The operating system analyzes privileges included in the user's authorization record and places the user in one of seven categories depending on which privileges have been granted to the user. Default privileges are those authorized privileges that are automatically granted at login. If an authorized privilege is not a default privilege, it will not automatically be effective at login, and must be enabled or disabled by the user. All user organization users have NORMAL privileges.

The write and delete access capabilities are not activated for WORLD access to the files in the system directory. The UIC associated with each of these files is within the MAXSYSGROUP number. To limit access to security files, the MEC has limited the WORLD access for the user authorization file, which contains account information to identify which users are allowed access to accounts on the system; the proxy file, which contains proxy account information to identify which remote users are allowed access to proxy accounts on the system; and the rights file, which contains names of the reserved system identifiers and identifiers for each user.

A firewall and additional routing devices have been placed between the Internet access provided by the OECN network and the internal network used by the MEC and its user organizations. To allow for MEC IP traffic to flow to the Internet a firewall has been installed at the gateway to the Internet. The firewall has been configured to map the internal network addresses to external IP Internet address.

Access to the OECN software packages is controlled at the ITC level by a security mechanism called the OECN Security Authorization (OSA) utility. Access to specific packages is provided by granting the appropriate operating system identifiers to authorized users. Each application package has a set of unique identifiers that permit access to programs. In addition to the standard identifiers for each package, a pass through identifier can be used to further customize access. OSA is used in conjunction with the OECN menu processor utility thus allowing the users to see only the items they are authorized to execute. UIC-based protections prevent WORLD write or delete access to USAS, USPS, SAAS/EIS, and EMIS application data files.

The OECN\_SYSMAN is an identifier which grants access to all packages. The OECN\_SYSMAN identifier grants the user the same access as OECN\_USPS, OECN\_USAS, etc., for all packages without having to grant each individual identifier. The identifier is defined by state software so it works the same for all ITCs. The identifier grants access to software functions, but does not grant access to data. Only MEC staff has this identifier.

The building is secured by a security system. Motion and sound sensors are located throughout the building and are linked to the system. All outside doors are kept locked. The computer room can be entered from three different doors. One door can be accessed from the outside and the other two from the interior of the building. All three doors are protected by electronic locks. All MEC staff members have access to the computer room.

The following items assist in controlling the computer room to protect it from adverse environmental conditions:

- Sound sensors.
- Motion detectors.
- Raised floor.
- Standard fire extinguisher (inspected yearly)
- Halon fire extinguisher (inspected yearly).
- Liebert 50KVA uninterruptured power supply.
- Liebert environmental systems.
- Emergency power-kill switches for the computer room electricity.
- Diesel powered generator (tested weekly).
- Floor water sensor.

## IT Operations

Traditional computer operations procedures are minimal because users at the user organizations initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All MEC employees have access to technical manuals for the Alpha systems on-site and via the Internet. MEC has a documented operational procedure manual. In addition, users have access to SiteScape Forum, a bulletin board that allows the MEC employees to communicate concerns with user organizations across the state. In addition, user organizations are encouraged to make use of the state wide help desk system to report problems or issues.

Certain routine jobs are initiated for system maintenance and security monitoring. MEC is responsible for operational maintenance tasks, such as system backups, log reports, and other maintenance directed at the whole system. Most daily processes run by the MEC are scheduled through the TIMEBASEd command procedure file. This procedure runs a list of periodic batch jobs scheduled by the systems administrator.

---

Hardware maintenance agreements exist with Service Express, and Networks Group/Juniper. The MEC has a provision within their Service Express hardware maintenance agreement called Protect-All, which covers the replacement of equipment in the event of its total loss. The agreement with SMARTnet and Networks Group/Juniper provides for hardware maintenance of the MEC routers and switches. In addition, all data processing equipment is covered under an insurance policy.

Common user problems that arise daily, such as terminal lockups and program crashes, are usually handled by the MEC service representatives over the phone. MEC utilizes the state wide helpdesk system, CA Unicenter, to document and track problem resolution requests for all service areas.

The MEC uses an HP Storage Area Network (SAN) for data storage. If a disk were to become corrupted, the system could continue functioning without the disk. When a disk fails, the failed disk data is rebuilt through a process known as reconstruction. Reconstruction restores the disk group resiliency to protect against another disk failure. After reconstruction or after a new disk is added to a disk group, the data is redistributed proportionately and reorganized to produce redundant sets to the active disks. A defragmentation program scans the disk volumes daily to improve system performance.

Network performance is monitored through the use of an application called WhatsUp Gold. As the application runs, it displays all network devices and their status. WhatsUp Gold submits a periodic ping to each network device to determine if it is active. If a device is not active, it will be highlighted in red on the application and an e-mail will be sent to the technicians responsible for the device. The technicians will prioritize the problem and schedule corrective actions accordingly.

The MEC has documented procedures for how to back up and restore all system data and programs.

IBM Tivoli Storage Manager (TSM) is used to schedule and maintain server backup and recovery. Daily incremental and monthly full system backups of the Alpha server are scheduled through an OpenVMS script (TIMEBASEd) and pushed to the TSM. Completion of the backups is documented on a log. Incremental backup cartridges are stored in a robotic tape silo. TSM is configured to help ensure that any file or all files can be restored to any date/time within 45 days.

MEC utilizes a number of solutions to protect the system data. Host based volume shadowing mirrors the system data to a second system host located at the disaster recovery site. Additionally, a copy of the data stored in the STORServer/Tivoli backup appliance is copied to the disaster recovery site. A full set of backup tapes is stored in a fireproof safe at a second off-site location. All data required by law to be maintained for a specific duration is maintained by the MEC. Calendar year and fiscal year end information is stored up to 18 years for MEC user organizations.

---

## User Control Considerations

The applications were designed with the assumption that certain controls would be implemented by user organizations. This section describes additional controls that should be in operation at the user organizations to complement the control at the ITC. User auditors should consider whether the following controls have been placed in operation at the user organization:

1. User organizations should have controls over their own web applications, which access their data stored at the MEC.
2. User organization management should have practices to ensure users are aware of the security policies of the MEC and that users take precautions to ensure passwords are not compromised.
3. User organization management should immediately request the MEC to revoke the access privileges of user organization personnel when they leave or are otherwise terminated.
4. User organization personnel should respond to account confirmation requests from the MEC.
5. User organizations should have documented acceptable use policies to define the activities deemed appropriate for use of the Internet. Internet users should be required to accept the terms of the policy before access is provided.
6. Access privileges should only be issued to authorized users who need access to computer resources to perform their job function.
7. PCs and terminals should be protected against damage or misuse by having separate areas, either independent rooms or sections of rooms that restrict access to only authorized individuals.
8. Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.
9. The user organizations should retain source documents for an adequate period to help ensure data can be re-entered in the event that data files are destroyed prior to being backed up and rotated off-site.

The user control considerations presented above do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at the user organization.

---

## **SECTION III - INFORMATION PROVIDED BY THE SERVICE AUDITOR**

*This section is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the MEC's internal control that may be relevant to user organization's internal control, and reduce the assessed level of control risk below the maximum for certain financial statement assertions.*

*The broad objectives of data processing controls should be achieved by a combination of the procedures that are employed in various segments of the transaction processing system, for example procedures performed at the MEC and procedures performed at user organizations that utilize the MEC.*

*For each of the control objectives listed below, only those controls which contribute to the attainment of the related control objective are described and were tested.*

## GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

### Changes to Existing Applications and/or Systems

<b>Changes to Existing Applications and/or Systems - Control Objective:</b> <b>Change Requests</b> - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
In order to maintain continued support of the application software provided by SSDT, ITCs are required to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the USAS, USPS, SAAS/EIS, and EMIS object files at MEC was compared to the CRCs of the object files at NWOCA.	No exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements, and problems corrected. Updated user and system manuals for the applications are also made available to MEC.	Inspected the updated manuals and release notes available online for the most recent release on the SSDT's website.	No exceptions noted.
The MEC participates in the CSLG/ESL program, which provides operating system support, upgrades, and related documentation.	Inspected the CSLG/ESL invoice and proof of payment to confirm MEC has support through the CSLG/ESL program.	No exceptions noted.
Technical documentation for the current version of the operating system is available for reference by MEC personnel.	Inspected the documentation provided with the purchase of the latest operating system release for release notes and installation instructions.  Observed the online documentation at the HP web site, <a href="http://www.hp.com/go/openvms/doc">http://www.hp.com/go/openvms/doc</a> .	No exceptions noted.

**IT Security**

<b>IT Security - Control Objective:</b> <b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The MEC has established policies and procedures regarding computer security and access for its staff and user organizations. Policies are communicated to users.	<p>Inspected the computer network, Internet, e-mail, fax and phone acceptable user policy and MEC information security policy for guidelines regarding computer security and access for the MEC staff to ensure responsibilities and procedures are documented.</p> <p>In addition, inspected the sign-offs for the computer network, internet, e-mail, fax, and phone acceptable use policy to ensure all MEC staff had acknowledged receipt of the policy.</p>	No exceptions noted.
An account authorization form or e-mail is submitted by the appropriate user organization management to MEC before adding a user account on the system.	<p>Using a data analysis tool, compared the current and prior year's user authorization files to identify new user accounts with access to USAS, USPS, EMIS, and/or SAAS/EIS which have not been DISUSERed.</p> <p>Selected 30 of 302 new users and inspected the corresponding account authorization forms or corresponding e-mails for appropriate authorization.</p> <p>Inquired with the assistant director of data processing to confirm the process for authorizing access to the system.</p>	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Annually, the MEC confirms users and access rights by generating and forwarding a listing of user accounts and associated access rights to each user organization. Each user organization confirms user accounts are current and have appropriate identifiers assigned.	I Inquired about the review process with the coordinator of fiscal services – team leader to confirm method and frequency of confirmations by user organizations.  Inspected the initial and follow-up confirmation request and results received from user organizations confirming their review of the user list.	No exceptions noted.
Anti-virus software runs on the MEC PC's and servers to help protect against computer viruses. Definitions are updated periodically and infected items are quarantined. All viruses found are reviewed by the assistant ITC director.	Inspected the anti-virus definition screens to confirm automated procedures update anti-virus definitions.  Inspected an example of the daily virus alerts which can be used to monitor virus attacks/threats to confirm notifications of viruses are received by appropriate personnel.	No exceptions noted.
The tracking of security related events such as break-in attempts and excessive log failures are enabled through the operating system and logged in the system audit journal.	Inspected the security alarms and audits enabled to confirm security related events were appropriately enabled.	No exceptions noted.
A security monitor report, listing security violations from the audit journal and changes to sensitive security files, is generated by the system on a nightly basis for review by the systems administrator.	Inspected the following relating to the security monitor reports to confirm these reports are produced daily and forwarded to the appropriate personnel: <ul style="list-style-type: none"> <li>• An example of a security monitor report and summary.</li> <li>• Security monitor report script.</li> </ul>	No exceptions noted.

<p><b>IT Security - Control Objective:</b>  <b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.</p>		<p><b>Control Objective                  Has Been Met</b></p>
<p><i>Control Procedures:</i></p>	<p><i>Test Descriptions:</i></p>	<p><i>Test Results:</i></p>
<p>The system does not consist of an excessive number of unused or inactive user profiles.</p>	<p>Using a data analysis tool extracted the following information from the user authorization file:</p> <ul style="list-style-type: none"> <li>• User accounts that have never been logged into.</li> <li>• User accounts that have not logged in during the last 180 days.</li> </ul> <p>Inquired with the assistant director of data processing regarding the purpose and appropriateness of accounts extracted.</p>	<p>No relevant exceptions noted.</p>
<p>Password parameters are in place to aid in the authentication of user access. Passwords used by individual profiles agree to password policies established by the MEC and profiles with pre-expired passwords are not excessive on the system.</p>	<p>Using a data analysis tool, extracted password information from the user authorization file. Inspected user account password parameters and compared accounts to policy-defined standards as follows:</p> <ul style="list-style-type: none"> <li>• User accounts with password minimum lengths less than the established guidelines of MEC.</li> <li>• User accounts with password lifetimes greater than the established guidelines of MEC.</li> <li>• User accounts with pre-expired passwords.</li> </ul> <p>Inquired with the assistant director of data processing to confirm the purpose and the appropriateness of the accounts extracted.</p>	<p>No exceptions noted for passwords less than the minimum length.</p> <p>Of 2,380 active user accounts on the system with access to State Software applications, 338 or 14% of accounts exceeded the standard lifetime parameter of 90 days.</p> <p>No relevant exceptions noted for user accounts with pre-expired passwords.</p>

<b>IT Security - Control Objective:</b> <b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameters to confirm parameters were set to control and monitor sign-on attempts.	No exceptions noted.
A program monitors system activity and logs off inactive users during non-business hours. The program is part of the TIMEBASEd command ensuring the program is consistently executed at startup.	Inspected the WATCHER configuration file to confirm inactive accounts are being monitored. In addition, identified protected accounts and confirmed the appropriateness of accounts with the systems administrator.  Inspected the TIMEBASEd scheduler to confirm the WATCHER utility is part of the daily start up procedures.	Accounts are only timed-out after work hours from 5 pm until 6 am.
Access to production data files and programs is restricted to authorized users.	Using a data analysis tool, inspected a listing of fiscal and EMIS executable files for WORLD write or delete access. Inspected user organization data files for WORLD access.	No relevant exceptions noted.
Firewalls and a routing system are used to control Internet traffic and maintain a logical segregation between user organizations.	Inspected the network diagram to confirm components of the network which control Internet access.  Inspected the firewall and router configurations to confirm inbound and outbound IP traffic is restricted through these network components and to confirm the existence of a private internal network.  Inspected a user organization help desk request for a change to the firewall.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Application Level Access Controls</b> - Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.		<b>Control Objective</b> <b>Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
An account authorization form is used to request access to the USAS, USPS, SAAS/EIS and EMIS applications.	Using a data analysis tool compared the current and previous year's user authorization files to identify new users with fiscal or EMIS identifiers that were not disused.  Selected 30 of 302 new users and compared access requested with access granted.	No exceptions noted.
Users are restricted to predefined logical access identifiers that grant varying access privileges based on requests from user management.	Using a data analysis tool summarized the number of accounts with OECN identifiers for evidence of the use of identifiers to segregate access to the applications.	No exceptions noted.
The OECN_SYSMAN identifier is restricted to authorized users.	Using a data analysis tool, extracted accounts from the user authorization file with the OECN_SYSMAN identifier.  Inspected the extracted accounts and confirmed the purpose and appropriateness of the accounts with the assistant director of data processing.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>System Software and Utilities Access Controls</b> - Use of sensitive facilities, such as, master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		<b>Control Objective</b> <b>Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
WORLD access to "key" system and security files is restricted.	Inspected the system file directory listings to confirm there was no WORLD, write and/or delete access.  Inspected file protection masks on the security files to ensure no access was provided at the WORLD level.	No relevant exceptions noted.

<b>IT Security - Control Objective:</b> <b>System Software and Utilities Access Controls</b> - Use of sensitive facilities, such as, master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
System level user identification codes are restricted to authorized personnel.	<p>Identified the maximum system group number for the operating system.</p> <p>Using a data analysis tool, extracted accounts from the user authorization file with a UIC less than the maximum system group number.</p> <p>Inspected the extracted accounts with the assistant director of data processing to confirm accounts were appropriate.</p>	No exceptions noted.
An alternate user authorization file is not permitted to be used and does not exist.	<p>Inspected the value of the user authorization alternate parameter.</p> <p>Inspected the system directory listings to determine if an alternate user authorization file existed.</p>	No exceptions noted.
Remote access to firewall and router configurations used to control Internet access is restricted through password protection.	<p>Inspected the firewall and router configurations to confirm passwords were required for access and remote access is limited.</p> <p>Confirmed through observation, that access is denied with the entry of a null password.</p>	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>System Software and Utilities Access Controls</b> - Use of sensitive facilities, such as, master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		<b>Control Objective</b> <b>Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
System level accounts with elevated privileges are restricted to authorized personnel	Using a data analysis tool extracted the following information from the user authorization file: <ul style="list-style-type: none"> <li>• User accounts will ALL privileges</li> <li>• User accounts have ELEVATED privileges. ELEVATED is defined as those accounts having more than TMPMBX and NETMBX which are the minimum privileges to use the system.</li> </ul> Inquired with the assistant director of data processing regarding the purpose and appropriateness of accounts extracted.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Physical Security</b> - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		<b>Control Objective</b> <b>Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Physical access to the computer room and its contents is restricted to authorized personnel.	Observed use of the key pad entry device and existence of motion detection devices throughout the period of fieldwork to confirm access is restricted to authorized personnel.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, water, humidity, or changes in temperature.	Inspected the computer room to confirm the existence of appropriate environmental controls used to detect and prevent environment hazards.	No exceptions noted.

## IT Operations

<b>IT Operations - Control Objective:</b> <b>System Administration and Maintenance</b> - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The MEC performs routine jobs such as directory updates, backups, security audits, and defragmentations for system maintenance through a scheduling program and the system start-up command.	<p>Inspected the TIMEBASEd schedule for routine maintenance jobs scheduled, such as backups and DEFRAG.</p> <p>Inspected the system start-up command file to confirm the TIMEBASEd scheduler is initiated at startup, as well as routine maintenance jobs such as DEFRAG and security report generation.</p> <p>Inspected the defragment settings and devices through the SHOW/ALL command in the defragmentation program and the TIMEBASEd scheduler for the DEFRAG program's frequency of execution.</p>	No exceptions noted.
MEC has hardware service agreements for support and maintenance of computer and network equipment.	<p>Inspected the hardware maintenance agreements through Service Express for the services provided for the Alpha hardware and the effective dates of service.</p> <p>Inspected the network maintenance agreements through CISCO SMARTnet for services provided for network equipment and the effective dates of service.</p> <p>Inspected invoices and copies of cancelled checks for evidence the agreements were paid throughout the audit period.</p>	No exceptions noted.

<b>IT Operations - Control Objective:</b> <b>System Administration and Maintenance</b> - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
All MEC equipment is covered by insurance.	Inspected the insurance policy, invoices, and computer related coverage restrictions to confirm MEC equipment is insured in the event of a disaster.	No exceptions noted.
WhatsUp Gold software monitors network performance and alerts staff of hardware failures and system problems.	Inspected the WhatsUp Gold Device View, Ping Report and Active Monitor Report for documentation of server status.	No exceptions noted.

<b>IT Operations - Control Objective:</b> <b>Backup</b> - Up-to-date backups of programs and data should be available in emergencies.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Daily incremental and monthly full system backups are automatically performed.	<p>Inspected backup jobs initiated through the TIMEBASEd scheduler to ensure daily incremental and monthly full system backups were scheduled.</p> <p>Inspected a directory listing of backup logs to ensure backups were completed consistently.</p> <p>On 07/13/09, observed the assistant director of data processing perform a restore of a fiscal file from a current backup tape and inspected the file for adequate restoration of data.</p>	No exceptions noted.

<b>IT Operations - Control Objective:</b> <b>Backup</b> - Up-to-date backups of programs and data should be available in emergencies.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Backup tapes are rotated off-site regularly and stored in secure off-site locations.	<p>On 07/14/09, visited the off-site location and compared the tapes within the fireproof safe with the DRPOOL listing to ensure all tapes required for recovery were stored off-site.</p> <p>Inspected the following documentation to ensure files are duplicated at the disaster recovery location:</p> <ul style="list-style-type: none"> <li>• STORServer script report.</li> <li>• STORServer hierarchy schedule.</li> <li>• STORServer completion report.</li> </ul>	No exceptions noted.
The retention and rotation of tapes is managed by the STORServer based on policies.	Inspected the STORServer retention settings to ensure they adhere to the MEC data retention policy.	No exceptions noted.

---

## SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

### INFORMATION TECHNOLOGY CENTER PROFILE OHIO EDUCATION COMPUTER NETWORK

#### SITE DATA

Name:	Metropolitan Educational Council (MEC)
Number:	20
Node Name:	MEC
Chairperson:	Walter Ames Board Member, Whitehall Schools
Fiscal Agent:	MEC
Administrator:	Bret Longberry ITC Director MEC
Address:	2100 Citygate Drive Columbus, OH 43219
Telephone:	614-473-8300
Fax:	614-473-8323
Website:	<a href="http://www.mecdc.org">www.mecdc.org</a>

OTHER SITE STAFF

Jeff Culwell	Assistant director of data processing
Jim Lovsey	Systems administrator
Dayna Duncan	Assistant ITC director
Tim Krile	Network operations manager
Jeff O'Brien	Technical specialist
Justin Price	Technical specialist
Michelle Powers	Coordinator of fiscal services – team leader
Charla Rose	Coordinator of fiscal services
Charla Green	Coordinator of EMIS services – team leader
Deborah LeFever	Coordinator of EMIS services
Cheryl Cahlander	Coordinator of administrative services
Ann Cless	Coordinator of student services – team leader
Diane Flateau	Coordinator of student services
Saundra Richardson	Coordinator of student services
Mary Nemeth	Coordinator of INFOhio/library services – team leader
Ilene King	Coordinator of INFOhio/library services

HARDWARE DATA

## Central Processors and Peripheral Equipment

**CPU Unit 1**

<u>Model Number</u>	<u>Installed</u>	<u>Capacity/Density/Speed</u>
CPU: HP Alpha Server ES45 Model 2	Lines/Ports: 0	Memory Installed: 32 GB
Disk: HP EVA	Units: 24	Total Capacity: 984 GB
Printer: Printronix P5215	Units: 1	Print Speed: 1200 LPM

**CPU Unit 2**

<u>Model Number</u>	<u>Installed</u>	<u>Capacity/Density/Speed</u>
CPU: HP Alpha Server ES45 Model 2	Lines/Ports: 0	Memory Installed: 32 GB
Disk: HP EVA	Units: 24	Total Capacity: 984 GB
Printer: Printronix P5215	Units: 1	Print Speed: 1200 LPM

**CPU Unit 3**

<u>Model Number</u>	<u>Installed</u>	<u>Capacity/Density/Speed</u>
CPU: Compaq Alpha Server 1000A	Lines/Ports: 0	Memory Installed: 256 MB
Disk: RZ1CB	Units: 1	Total Capacity: 4 GB
Disk: RZ1BB	Units: 1	Total Capacity: 2 GB

HARDWARE DATA

## Central Processors and Peripheral Equipment (Continued)

**CPU Unit 4**

<u>Model Number</u>		<u>Installed</u>		<u>Capacity/Density/Speed</u>	
CPU:	Compaq Alpha Server DS20	Lines/Ports:	0	Memory Installed:	512 MB
Disk:	JB0D	Units:	1	Total Capacity:	9.1 GB
Disk:	Internal Raid	Units:	3	Total Capacity:	27.3 GB

**USER ORGANIZATION SITE DATA**

<u>IRN</u>	<u>USER ORGANIZATION</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>	<u>EMIS</u>
008061	Arts and Science Preparatory Academy	Cuyahoga				X
007995	Cleveland Arts and Social Sciences Academy	Cuyahoga				X
008066	Lion of Judah Academy	Cuyahoga				X
000523	Education Alternatives Community School	Cuyahoga				X
000302	Summit Academy – Parma Secondary	Cuyahoga				X
000775	Weems Charter School	Cuyahoga	X			X
132746	Summit Academy – Middletown Elementary	Butler				X
000634	Summit Academy – Middletown Secondary	Butler				X
149310	Amanda-Clearcreek Digital Academy	Fairfield	X	X		X
046839	Amanda-Clearcreek LSD	Fairfield	X	X	X	X
046854	Berne Union LSD	Fairfield	X	X	X	X
046862	Bloom Carroll LSD	Fairfield	X	X	X	X
046839	Fairfield County ESC	Fairfield	X	X	X	X
046870	Fairfield Union LSD	Fairfield	X	X	X	X
044206	Lancaster CSD	Fairfield	X	X	X	X
142984	Lancaster Digital Academy	Fairfield	X			X
000426	Lancaster-Fairfield Alternative School	Fairfield	X			X
046888	Liberty Union – Thurston LSD	Fairfield	X	X	X	X
046896	Pickerington LSD	Fairfield	X	X		
046904	Walnut Township LSD	Fairfield	X	X	X	X
000556	A+ Arts Academy	Franklin	X	X		X
043620	Bexley CSD	Franklin	X	X	X	X
046946	Canal Winchester LSD	Franklin	X	X	X	X
000557	Columbus Arts and Technology Academy	Franklin				X

**USER ORGANIZATION SITE DATA**

<b><u>IRN</u></b>	<b><u>USER ORGANIZATION</u></b>	<b><u>COUNTY</u></b>	<b><u>USAS</u></b>	<b><u>USPS</u></b>	<b><u>SAAS</u></b>	<b><u>EMIS</u></b>
000553	Columbus Humanities Arts and Technology Academy	Franklin				X
000558	Columbus Preparatory Academy	Franklin				X
133439	Cornerstone Academy Community	Franklin				X
143412	Crittenton Community School	Franklin	X	X		X
060988	Department of Youth Services	Franklin				X
047027	Dublin CSD	Franklin	X	X	X	X
051003	Eastland-Fairfield Career & Technical Schools	Franklin	X	X	X	X
000585	FCI Academy	Franklin	X			X
142943	Focus Learning Academy – North Columbus	Franklin				X
142935	Focus Learning Academy – Southeast Columbus	Franklin				X
142927	Focus Learning Academy – Southwest Columbus	Franklin				X
046938	Franklin County ESC	Franklin	X	X	X	X
009165	Gahanna Alternative Community School	Franklin	X			X
046961	Gahanna-Jefferson CSD	Franklin	X	X		X
044073	Grandview Heights CSD	Franklin	X	X	X	X
046979	Groveport Madison LSD	Franklin	X	X	X	X
000197	Hamilton Township Digital Academy	Franklin	X			X
046953	Hamilton Township LSD	Franklin	X	X	X	X
047019	Hilliard CSD	Franklin	X	X	X	X
133660	Horizon Science Academy – Columbus High School	Franklin				X
009197	Horizon Science Academy – Columbus Middle School	Franklin				X
009990	Horizon Science Academy – Elementary School (Northeast Columbus)	Franklin				X
143172	International Academy of Columbus	Franklin	X	X		X
088070	Marburn Academy Elementary	Franklin			X	X

**USER ORGANIZATION SITE DATA**

<u>IRN</u>	<u>USER ORGANIZATION</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>	<u>EMIS</u>
133561	Millennium School	Franklin	X	X	X	X
133397	Montessori Renaissance Experience	Franklin				X
046995	New Albany Plain LSD	Franklin	X	X		
008280	Noble Academy – Columbus	Franklin				X
000679	Oakstone Community School	Franklin	X	X		X
071548	Ohio School for the Blind	Franklin	X			X
071530	Ohio School for the Deaf	Franklin	X			X
000938	Premier Academy of Ohio	Franklin	X	X		X
000743	Pshtecin Public School	Franklin		X		X
047001	Reynoldsburg CSD	Franklin	X	X	X	X
000592	School for Arts Integrated Learning (S.A.I.L.) – New Albany	Franklin	X			
000277	Scholarts Preparatory Academy	Franklin				X
044800	South-Western CSD	Franklin	X	X	X	X
000296	Summit Academy – Columbus Elementary	Franklin				X
000610	Summit Academy – Columbus Middle	Franklin				X
000610	Summit Academy – Columbus Secondary	Franklin				X
044933	Upper Arlington CSD	Franklin	X	X	X	X
000578	Upper Arlington Community High School	Franklin	X			X
000368	Upper Arlington International Baccalaureate HS	Franklin	X			X
143537	Virtual Community School of Ohio	Franklin	X	X		X
045047	Westerville CSD	Franklin	X	X	X	X
000875	Westside Academy	Franklin	X	X		X
045070	Whitehall CSD	Franklin	X	X	X	X
000590	Wickliffe Progressive Community School	Franklin	X			X

**USER ORGANIZATION SITE DATA**

<b><u>IRN</u></b>	<b><u>USER ORGANIZATION</u></b>	<b><u>COUNTY</u></b>	<b><u>USAS</u></b>	<b><u>USPS</u></b>	<b><u>SAAS</u></b>	<b><u>EMIS</u></b>
045138	Worthington CSD	Franklin	X	X	X	X
132985	YouthBuild Columbus Community	Franklin	X			X
000725	Zenith Academy	Franklin				X
132761	Summit Academy – Xenia Elementary	Greene				X
133512	Cincinnati College Preparatory Academy	Hamilton				X
000804	Horizon Science Academy – Cincinnati	Hamilton				X
000306	Summit Academy – Cincinnati Elementary	Hamilton				X
000306	Summit Academy – Cincinnati Secondary	Hamilton				X
007998	Center for Student Achievement	Jackson	X			X
044156	Jackson CSD	Jackson	X	X	X	X
000629	Summit Academy – Painesville Elementary	Lake				X
008064	Academy of Arts and Science	Lorain				X
000574	The Arts Academy	Lorain				X
008068	The Arts Academy – West Cleveland	Lorain				X
133322	Summit Academy – Lorain Elementary	Lorain				X
000609	Summit Academy – Lorain Middle	Lorain				X
000301	Summit Academy – Lorain Secondary	Lorain				X
000304	Summit Academy – Toledo Elementary	Lucas				X
000633	Summit Academy – Toledo Secondary	Lucas				X
063511	Tolles Career & Technical Center	Madison	X	X	X	X
048256	Jefferson LSD	Madison	X	X	X	X
048264	Jonathan Alder LSD	Madison	X	X	X	X
044255	London CSD	Madison	X	X		X
151027	London Digital Academy	Madison	X			X

**USER ORGANIZATION SITE DATA**

<u>IRN</u>	<u>USER ORGANIZATION</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>	<u>EMIS</u>
133314	Summit Academy – Youngstown Elementary	Mahoning				X
000623	Summit Academy – Youngtown Middle	Mahoning				X
000303	Summit Academy – Youngtown Secondary	Mahoning				X
007984	Youngstown Academy of Excellence	Mahoning				X
000808	Horizon Science Academy – Dayton	Montgomery				X
000297	Summit Academy – Dayton Elementary	Montgomery				X
000297	Summit Academy – Dayton Secondary	Montgomery				X
049098	Teays Valley LSD	Pickaway	X	X	X	X
009192	Foundation Academy	Richland				X
008000	Mansfield Preparatory Academy	Richland				X
000311	Bridges Community Academy	Seneca	X	X		X
133306	Summit Academy – Canton Elementary	Stark				X
000300	Summit Academy – Canton Secondary	Stark				X
133587	Summit Academy - Akron Elementary	Summit				X
132779	Summit Academy – Akron Middle	Summit				X
000298	Summit Academy – Akron Secondary	Summit				X
007982	Academy of Arts and Humanities	Trumbull				X
007992	Arts and Sciences Academy	Trumbull				X
000305	Summit Academy – Warren Elementary	Trumbull				X
000616	Summit Academy – Warren Middle	Trumbull				X
050328	Fairbanks LSD	Union	X	X	X	X
050336	North Union LSD	Union	X	X	X	X
<b>TOTALS:</b>			<b>59</b>	<b>45</b>	<b>32</b>	<b>115</b>





**Mary Taylor, CPA**  
Auditor of State

**METROPOLITAN EDUCATIONAL COUNCIL (MEC)**

**FRANKLIN COUNTY**

**CLERK'S CERTIFICATION**

**This is a true and correct copy of the report which is required to be filed in the Office of the Auditor of State pursuant to Section 117.26, Revised Code, and which is filed in Columbus, Ohio.**

*Susan Babbitt*

**CLERK OF THE BUREAU**

**CERTIFIED  
SEPTEMBER 22, 2009**