

The seal of the Auditor of State of Ohio is a large, circular watermark centered on the page. It features a sun rising over a landscape with fields and trees. The text "THE SEAL OF THE AUDITOR OF STATE OF OHIO" is written around the perimeter of the seal.

**NORTHEAST OHIO NETWORK FOR EDUCATIONAL TECHNOLOGY (NEOnet)
STATE REGION - ISA, SUMMIT COUNTY**

SAS - 70

MAY 3, 2008 THROUGH JULY 10, 2009



Mary Taylor, CPA
Auditor of State

TABLE OF CONTENTS

I INDEPENDENT ACCOUNTANTS' REPORT..... 1

II ORGANIZATION'S DESCRIPTION OF CONTROLS 3

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..... 5

 Monitoring..... 6

INFORMATION AND COMMUNICATION 6

GENERAL EDP CONTROLS..... 7

 Development and Implementation of New Applications and Systems 7

 Changes to Existing Applications and Systems 7

 IT Security 8

 IT Operations..... 12

USER CONTROL CONSIDERATIONS..... 14

III INFORMATION PROVIDED BY THE SERVICE AUDITOR..... 15

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING
EFFECTIVENESS..... 16

 Changes to Existing Applications and Systems 16

 IT Security 17

 IT Operations..... 25

IV OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION 27

INFORMATION TECHNOLOGY CENTER PROFILE..... 27

This Page Intentionally Left Blank



Mary Taylor, CPA

Auditor of State

INDEPENDENT ACCOUNTANTS' REPORT

Board of Directors
Northeast Ohio Network for Educational Technology (NEOnet)
420 Washington Avenue
Cuyahoga Falls, Ohio 44221

To Members of the Board:

We have examined the accompanying description of controls of the Northeast Ohio Network for Educational Technology (NEOnet) 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 NEOnet'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 NEOnet's controls; and (3) such controls had been placed in operation as of July 10, 2009. The NEOnet 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 NEOnet, 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 NEOnet 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 NEOnet's controls that had been placed in operation as of July 10, 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 NEOnet'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 May 3, 2008 to July 10, 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 NEOnet 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 May 3, 2008 to July 10, 2009.

The relative effectiveness and significance of specific controls at the NEOnet 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 information technology center is presented by the NEOnet to provide additional information and is not part of the NEOnet'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 NEOnet is as of July 10, 2009, and information about tests of the operating effectiveness of specified controls covers the period from May 3, 2008 to July 10, 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 NEOnet 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 NEOnet, its user organizations, and the independent auditors of its user organizations.

A handwritten signature in black ink that reads "Mary Taylor". The signature is written in a cursive, flowing style.

Mary Taylor, CPA
Auditor of State

July 10, 2009

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The Northeast Ohio Network for Educational Technology (NEOnet) 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 NEOnet's description of controls.

OVERVIEW OF OPERATIONS

NEOnet 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 NEOnet 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 either as consortia under ORC 3313.92 or as a Council of Governments (COG) under ORC 167. ORC 3313.92 allows school districts to create a partnership (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 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. NEOnet is a subsidiary of the Metropolitan Regional Service Council (MRSC) which is a Council of Governments organized under ORC 167. The MRSC employs its own fiscal officer to act as fiscal agent for NEOnet.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the Metropolitan Regional Service Council (MRSC) board of directors. The superintendent from each member user organization is appointed to the legislative body of NEOnet known as the assembly. The assembly and the board of directors are the oversight organizations for NEOnet. The assembly meets at least twice per year to estimate program costs, approve annual appropriations, select officers and members of the board of directors, and approve other matters as determined to require the approval of the assembly. The board of directors is the managerial body of NEOnet and meets at least five times a year. The board consists of the following positions:

- Chair of the assembly.
- Vice chair of the assembly.
- Chair of the program committee.
- Chair of the treasurers operating committee.
- Three “at-large” assembly members.
- Executive director (ex-officio).
- Fiscal officer (ex-officio).

The following committees or sub-committees have been established to address specific needs or goals:

- Treasurers operating committee.
- Program committee / Technology advisory committee.
- Educational operating committee.
- Media specialist committee.
- Audit sub-committee.
- Finance committee.
- Continuous improvement committee.

These committees meet to provide detailed information to the board of directors in regards to each area of expertise.

NEOnet employs a staff of 17 full time individuals, including the executive director, and is supported by the following functional areas:

- *Software Support* – Supports end users in a given area of concentration including the EMIS, fiscal, and student service applications.
- *Media Support* – Supports end users with the library applications.
- *Technical Support* – Supports NEOnet’s computer systems and networked communication system. Provides user training and support.

The managers of each functional area report to the executive director.

Users are responsible for the authorization and initiation of all transactions. Management reinforces this segregation of duties as a part of its new employee orientation process, through on the job training and by restricting employee access to user data. Changes to user data are infrequent.

Only experienced NEOnet employees may alter user data and only at the request of the user organization. Completion of a job record form is required for all changes and the forms are periodically reviewed by the executive director.

The MRSC has established its own personnel policies and procedures which are followed by NEOnet. NEOnet is constantly re-evaluating its need for personnel to support the increasing range of services provided. The reporting structure and job descriptions are periodically updated to create a more effective organization.

NEOnet'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 NEOnet staff members are required to attend professional development and other training as a condition of continued employment. Each staff member must attend at least 15 hours of approved professional development training annually, and at least 80 hours of approved training every four years. Employee evaluations are conducted annually.

NEOnet is also subject to ITC site reviews by the Technology Solutions Group of the Management Council – Ohio Education Computer Network MCOECN ([mc•tsg](#)). 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. NEOnet's ITC site review has not yet been scheduled.

Risk Assessment

NEOnet does not have a formal risk management process; however, NEOnet's board of directors and the various committees and sub-committees actively participate in the oversight of the organization.

As a regular part of its activity, the board of directors and the other bodies address:

- New technology.
- Realignment of the NEOnet 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, AOS and other accounting pronouncements, and legislative issues.
- Operating policies and procedures.

In addition, NEOnet has identified operational risks resulting from the nature of the services provided to their 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 NEOnet organization is structured so staff report to managers who report directly to the executive director. Key staff members have worked at NEOnet or another ITC for many years and are experienced with the systems and controls. The NEOnet executive 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, computer security, and user help desk reports are monitored on an ongoing basis by departmental management. Some of these reports are automatically run through a scheduler program and are sent to management via e-mail. Exceptions to normal processing related to hardware, software, or procedural problems are logged and resolved daily.

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 Control sections.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

The NEOnet staff does not perform system development activities. Instead, NEOnet 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 Systems

End-users 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 utilizes 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/EIS, and EMIS) has its own public and ITC Site forum which is monitored by the SSDT system analysts. All OECN ITCs and user organizations have access to forum conferences, providing end-user participation in the program development/change process.

NEOnet personnel do not perform program maintenance activities. Instead, they use applications supplied 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.

NEOnet 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), acts as the fiscal agent for this and other participating ITCs and 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 to the participant for a limited series of HP software packages as approved by the Board of Trustees of the MCOECN.
- Provide telephone technical support to the participant's 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 NEOnet, 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 OpenVMS 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 MCOECN provides all ITC's with purchasing discounts on hardware and software through the Technology Solutions Group program under the MCOECN ([mc•tsg](#)).

IT Security

NEOnet has a security policy that outlines the responsibilities of user organization personnel, NEOnet personnel, and any individual or group not belonging to the user organization or NEOnet. In addition to the security policy, NEOnet uses banner screens that are displayed before a user logs on to the system. The screen informs the user that unauthorized access of the system is prohibited and individuals using this computer system are subject to having their activities monitored by NEOnet personnel.

The NEOnet staff is 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. The executive director authorizes and creates NEOnet staff access.

Users from the user organizations are granted access upon the receipt of an authorization form. Access to the financial applications requires the authorization of either the superintendent or the treasurer. Authorization forms are sent to NEOnet's coordinator of software services who then creates the account and contacts the user regarding the newly established account. Authorization forms are maintained in the user organization's file. On an annual basis, user organizations are requested to verify their user accounts and identifiers through a positive confirmation process.

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 data processing personnel. Critical events are reported as both alarms and audits; less critical events are written to a log file for later examination. The following security alarms and security audits have been enabled through OpenVMS to monitor security violations on the NEOnet system:

ACL:	Gives file owners the option to selectively alarm certain files and events. Read, write, execute delete, or control modes can be audited.
AUDIT:	Enabled by default to produce a record of when other security alarms were enabled or disabled.
AUTHORIZATION:	Enables monitoring of changes made to the system user authorization file (UAF) or network proxy authorization file in addition to changes to the rights database.
BREAK-IN:	Produces a record of break-in attempts. The DIALUP, LOCAL, REMOTE, NETWORK, and DETACHED 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 coordinator of software services, senior systems analyst, technical specialist, and assistant director technical services manager. They are reviewed daily by the coordinator of software services. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and the corrective action needed.

NEOnet uses several processes to protect its systems from unwanted SPAM e-mails and computer viruses. NEOnet participates in the Iron Port anti-spam project sponsored by the State of Ohio Computer Center (SOCC). This service removes SPAM originating from e-mail servers known to be used by global senders of SPAM and does not pass the SPAM onto NEOnet. At the local level, NEOnet uses two Barracuda servers to scan incoming e-mail from Iron Port for SPAM and viruses. NEOnet also uses a MailMarshal server to scan inbound and outbound e-mail for SPAM and viruses. If a virus is found, the e-mail is quarantined. Due to the volume of virus e-mails, notices are not sent to users and infected e-mail is deleted after three days.

Primary logical access control to the HP computers is provided by security provisions of the OpenVMS operating system. This includes access to data, programs and system utilities. When a user logs in to use OpenVMS interactively, or when a batch or network job starts, OpenVMS creates a process which includes the identity of the user. OpenVMS 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 any 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 any interactive operations. NEOnet uses proxy logins.

The user identification codes (UIC) are individually assigned to all data processing personnel employed at NEOnet. For user organizations that use the NEOnet system, 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 that network objects run under, for example, require temporary access to DCL. Such accounts must be set up as RESTRICTED accounts, not CAPTIVE accounts. User accounts are 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 and CAPTIVE flags are not used for NEOnet staff member accounts because access to the DCL prompt is necessary for them to maintain the system. However all other users, such as teachers, administrative staff, and students, are assigned the RESTRICTED flag.

The system forces users to change their passwords on a periodic basis. Initial passwords are set to expire when a new user identification code is issued or when a user has forgotten his password. This parameter requires the user to change his password during the first logon procedure. Standards for password minimum length and lifetime have been established.

The operating system has system parameters called SYSGEN 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 loses the carrier.
- 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 using HP established defaults.

A timeout program, HITMAN, is used to monitor terminal inactivity and log-off inactive users. The use of this program helps to reduce the risk of an unattended terminal being used to enter unauthorized transactions. Also, timeout programs aid in efficient use of system resources by maintaining connectivity with only active system users.

Associated with each object recognized by OpenVMS 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 the object. 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 SYSGEN parameter for MAXSYSGROUP. (2) Users with system privileges (SYSPRV). (3) Users with group privileges (GRPPRV) 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. OpenVMS analyzes privileges included in the user authorization file (UAF) record for each user 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 users, at the user organization, 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, NEOnet 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.

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 OpenVMS 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 customize access even further. 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 protection prevents WORLD write or delete access to the USAS, USPS, SAAS/EIS, and EMIS application data files.

User organizations have been set up with sub-networks, which have addresses not recognizable to the Internet. This is called a private network. A firewall has been placed between the Internet access provided by the OECN network and the internal network of the user organizations of NEOnet. The firewall equipment denies all outbound traffic requests where it performs the function of a proxy server and acts as a middle man between the Internet and the internal network. NEOnet also makes available an Internet content filter. The filter is an optional service, which screens Internet site requests for "unsuitable" content.

The ITC is located in a segregated area and access is monitored by motion sensitive security devices. The building is secured by a security system and entry doors are locked during off hours, and unlocked during business hours; however, ITC personnel are present at all times. The computer room remains locked at all times and is secured by a combination key pad lock. The combination is known by ITC staff only. Motion detectors, as well as security cameras, are in place throughout the building.

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

- Air conditioning.
- Smoke detectors.
- Fire extinguishers.
- Power conditioner.
- Security camera.
- Equipment is mounted in racks or housed in chassis.
- Backup generator.

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 NEOnet employees have access to operations procedure manuals for the HP systems. In addition, all users, except students, have access to SiteScape Forum, which is a bulletin board that allows NEOnet employees to communicate with users across the state. Users can post questions and/or comments to NEOnet staff.

Data entry errors are mostly corrected by the user and are subject to the normal application controls. User problems, typically related to the student systems, which require NEOnet staff to change data, require the completion of a help desk ticket. These forms are periodically reviewed by the executive director and the coordinator of software services to verify processing was not interrupted. In addition, the user organizations have the option of printing an "AUDIT" report that shows all changes to their data files.

Certain routine jobs are initiated for system maintenance. NEOnet is responsible for operational maintenance tasks, such as system backups, file rebuilds, log reports, and other maintenance directed at the whole system. They use an automated application called DECScheduler to schedule and perform these tasks. DECScheduler is a program that continually submits jobs on the Alpha system. Network devices are also monitored to ensure they are functioning. The senior systems analyst uses a vendor supplied application to monitor the status of all compatible routers and switches. Real time information can be gathered concerning equipment status, utilization, and other factors to determine the "health" of the device.

Common problems, such as terminal lockups and program crashes, are usually handled by NEOnet service representatives over the phone and may not be documented. However, major problems are logged through the help desk log. Any system or network problems are communicated to the executive director.

NEOnet has a hardware maintenance agreement with Service Express. The coverage of the equipment includes a response time of four hours.

The backup of program and data files at NEOnet are scheduled to run automatically. Full system backups are performed daily for the computer system. The tapes are stored in the STORserver located in the computer room at the ITC, which is protected by fire detection equipment and video camera surveillance. Every Tuesday and Friday, the tapes from the previous evening are rotated to an off-site storage facility, which is located 50 miles from NEOnet. The tapes are retained at the facility for four weeks.

All data required by law to be maintained for a specific duration is maintained on-site by NEOnet. Calendar year and fiscal year end information is stored indefinitely for all NEOnet user organizations.

All system and program documentation is stored electronically and is subject to the same backup procedures as the other data files.

In addition, all data processing equipment is covered under an insurance policy.

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:

General EDP Control Procedures

1. User organizations should have controls over their own web applications which access their data stored at the ITC.
2. User organization management should have practices to ensure users are aware of the security policies of their ITC and that users take precautions to ensure passwords are not compromised.
3. User organization management should immediately request the ITC 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 their ITC.
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. 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.
10. User organizations should establish and enforce a formal data retention schedule with their ITC for the various application data files.

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 NEOnet'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 NEOnet and procedures performed at user organizations that utilize NEOnet.

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 Systems

Changes to Existing Applications and Systems - Control Objective: Change Requests - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
In order to maintain continued support of the application software provided by the 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 NEOnet 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.	Inspected the release notes and updated manuals for the most recent releases.	No exceptions noted.
NEOnet participates in the CSLG/ESL program which provides operating system support, software upgrades and software related documentation.	Inspected the CSLG/ESL invoice and proof of payment to confirm NEOnet has support through the CSLG/ESL program.	No exceptions noted.
Documentation for the current version of the OpenVMS operating system are provided on the HP web site.	Inspected the online manuals for the operating system at the HP web site.	No exceptions noted.

IT Security

IT Security - Control Objective: Security Management - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
NEOnet has established a system security policy that outlines user responsibilities regarding computer security and access. The policy is available on NEOnet's web site.	Inspected the system security policy to confirm user responsibilities are documented. Inspected NEOnet's web site to confirm the policy is maintained online.	Control operating as described.
An account authorization form is used to request access to the NEOnet system. Access to the financial applications requires authorization from either the superintendent or treasurer.	Haphazardly selected 30 of 103 new user accounts with audit significant identifiers. Inspected the forms for appropriate authorization signatures.	No exceptions noted.
User access for active accounts is confirmed annually with organization management through a positive confirmation process. NEOnet tracks the status of the confirmations and performs any necessary follow-up communication to facilitate a response from the user organization.	Inspected confirmation documentation for evidence the confirmation process includes the following: <ul style="list-style-type: none"> • Verification forms and user listing sent to the user organizations. • Checklist used to track responses. Inquired with the software specialist student services about follow-up procedures.	No exceptions noted.
Detection control alarms are enabled through OpenVMS to track security related events, such as break-in attempts and excessive login failures. The events are logged to audit journals for monitoring of potential security violations.	Inspected the enabled security alarms and audits.	No exceptions noted.

IT Security - Control Objective: Security Management - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
<p>A command procedure executes each night to extract security violations from the audit log and create summary and detail reports called the security monitor report.</p> <p>The command procedure is generated daily and is e-mailed to the following NEOnet staff:</p> <ul style="list-style-type: none"> • Coordinator of software services • Technical specialist • Senior systems administrator • Assistant director / technical services manager • Assistant director / operations manager. 	<p>Inspected the following information relating to the security monitor report to confirm these reports are produced and available for review daily:</p> <ul style="list-style-type: none"> • DECScheduler job parameters for the security monitor report. • An example security monitor report. • Command procedure which e-mails the report to NEOnet personnel. <p>Independently confirmed the procedure for reviewing the security monitor report with the coordinator of software services and the assistant director / technical services manager.</p>	Control operating as described.
<p>NEOnet's incoming e-mail is filtered through Ironport, two anti-virus and spam filtering servers, and Sophos anti-virus software running on the MailMarshal server which help to protect against computer viruses and spam.</p>	<p>Inspected the following information, relating to the spam firewalls and MailMarshal anti-virus software, to confirm e-mail messages are scanned for spam and viruses:</p> <ul style="list-style-type: none"> • Barracuda spam firewall scanning definitions. • Sophos anti-virus definitions and update properties. • MailMarshal configuration screens. <p>Also, inspected the Internet header text from a sample e-mail which showed the path of the e-mail from IronPort, to the Barracuda server, to the MailMarshal server, and then to the e-mail server.</p>	No exceptions noted.

IT Security - Control Objective: System Level Access Controls - Access to the computer system, programs, and data should be appropriately restricted.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts are specifically defined to prevent blanket access.	Inspected the proxy listing to confirm wild card characters were not used.	No exceptions noted.
Individual user profiles are used to grant access rights and privileges for the system. The use of inactive or disabled profiles is limited.	<p>Extracted information from the user authorization file, to identify:</p> <ul style="list-style-type: none"> • User accounts that have never logged into the system. • Inactive user accounts, defined as those accounts that have not been logged into in 180 days. • User accounts that are DISUSERed. <p>Inspected the results of the extracted information and inquired with the coordinator of software services regarding the appropriateness of the accounts.</p>	<p>From a population of 1,144 active accounts, the following exceptions were noted:</p> <ul style="list-style-type: none"> • There were 221 (19%) accounts that have never been logged into. • There were 257 (22%) accounts that have not been logged into in over 180 days. <p>From a total population of 1430 accounts, the following exception was noted:</p> <p>The number of accounts that have been DISUSERed is 286 (20%).</p> <p>Management gave the following two reasons for these accounts:</p> <p>Accounts that remain on the system that were previously used for e-mail purposes.</p> <p>Accounts on the system used for the Web applications. Users who access the Web application can do so with pre-expired or expired passwords.</p>

IT Security - Control Objective: System Level Access Controls - Access to the computer system, programs, and data should be appropriately restricted.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Access to the OpenVMS system command line (DCL) is restricted to authorized users of the system.	<p>Extracted user accounts from the user authorization file that do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER, or RESTRICTED flags set.</p> <p>Inspected the results of the extracted information and inquired with the coordinator of software services regarding the appropriateness of these accounts.</p>	No exceptions noted.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameters settings.	No exceptions noted.
Passwords are used to authenticate users before granting them access to the system. Passwords used are in agreement with the password policies established by NEOnet.	<p>Extracted information from the user authorization file to identify:</p> <ul style="list-style-type: none"> • User accounts with a password length less than NEOnet standards. • User accounts with a password lifetime greater than NEOnet standards. • User accounts with pre-expired passwords. <p>Inspected the default account to confirm pre-expired parameters were set.</p>	<p>There were 313 (27%) accounts out of a total of 1,144 active accounts that have pre-expired passwords.</p> <p>Management indicated that some of these are accounts on the system used for the Web applications. Users who access the Web application can do so with pre-expired or expired passwords.</p> <p>No other relevant exceptions were noted.</p>
A program, HITMAN, constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed at startup.	<p>Inspected the HITMAN parameters (prime and non-prime) to confirm they were set to automatically logoff inactive users.</p> <p>Inspected the startup file to ensure the HITMAN utility is part of the startup process.</p>	No exceptions noted.
Access to production programs and data files is restricted to authorized users.	Inspected the file protection masks to identify production data files with WORLD access and executable files with WORLD write and/or delete access.	No exceptions noted.

IT Security - Control Objective: System Level Access Controls - Access to the computer system, programs, and data should be appropriately restricted.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user organizations.	<p>Inspected the network diagram to confirm components of the network that control Internet access.</p> <p>Inspected settings in the firewall configuration to confirm that inbound and outbound IP traffic is restricted by the firewall and to confirm the existence of a private internal network.</p>	No exceptions noted.
Firewall requests for new connections and/or modifications to existing connections are submitted to the assistant director / technical services manager via a help desk ticket.	<p>Inspected examples of help desk tickets for firewall change requests maintained by the assistant director / technical services manager. Compared the requests to the corresponding conduit connections.</p> <p>Observed the documentation spreadsheet maintained by the assistant director / technical services manager for evidence that IP addresses assigned are being tracked and for open ports resulting from the request process.</p>	Control operating as described.

IT Security - Control Objective: Application Level Access Controls - 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.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Users are restricted to predefined logical access identifiers that grant varying access privileges based on requests from user management.	Extracted accounts with the OECN identifiers for the USAS, USPS, SAAS/EIS, and EMIS application systems. Inspected the reports to determine whether identifiers were used to segregate access to the applications. Inquired with the coordinator of software services about the process of assigning identifiers.	No exceptions noted.
Users are only granted the level of access authorized by management to the USAS, USPS, SAAS/EIS, and EMIS application systems.	Sampled 30 account authorization forms from a population of 103 new user accounts having OECN financial identifiers. Compared the access requested to the actual access granted.	No exceptions noted.

IT Security - Control Objective: System Software and Utilities Access Controls - Use of master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		Control Objective Has Been Met
<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 for WORLD write or delete access. Inspected the file protection masks on the security files to ensure no access was provided at the WORLD level.	No exceptions noted.

IT Security - Control Objective: System Software and Utilities Access Controls - Use of master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
<p>System level UICs and elevated privileges are restricted to authorized personnel. UICs belonging to the system group are determined by the parameter value for MAXSYSGROUP. UICs less than the MAXSYSGROUP value have system level privileges.</p> <p>Accounts with elevated privileges are defined as those accounts having more than the minimum privileges to use the system.</p>	<p>Inspected the MAXSYSGROUP value.</p> <p>Extracted accounts from the user authorization file to identify:</p> <ul style="list-style-type: none"> • Accounts with a UIC less than the MAXSYSGROUP value. • Accounts with elevated privileges. <p>Inspected the extracted accounts and inquired with the coordinator of software services regarding the appropriateness of the accounts.</p>	No exceptions noted.
<p>The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized ITC personnel.</p>	<p>Extracted accounts from the user authorization file with the OECN_SYSMAN identifier. Inspected the list of accounts.</p> <p>Inquired with the coordinator of software services regarding the appropriateness of the accounts.</p>	No exceptions noted.
<p>Use of an alternate user authorization file is not permitted.</p>	<p>Inspected the value of the user authorization alternate parameter to determine whether an alternate file is permitted.</p> <p>Inspected the system directory listings to determine if an alternate user authorization file existed.</p>	No exceptions noted.
<p>Remote administration to the firewall configuration used to control Internet access is restricted through password protection.</p>	<p>Inspected the firewall configuration to confirm that a password is required and remote access is restricted.</p>	No exceptions noted.

IT Security - Control Objective: Physical Security - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		Control Objective Has Been Met
<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.	Inspected the keypad entry lock and security system to confirm physical access to the computer room is controlled. Observed the presence of security cameras inside and outside the computer room and the live video monitoring system within the computer room.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, water, or changes in temperature.	Inspected the computer room and observed the environmental control devices.	No exceptions noted.

IT Operations

IT Operations - Control Objective: System Administration and Maintenance - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Requests for changes to user organization data are documented on help desk tickets. Screen prints of changes made are attached to the completed forms.	Inquired with the coordinator of software services about the procedures for changing user data. Inspected an audit report (AUDRPT) for a user organization for changes made by NEOnet staff. Verified a help desk ticket was available requesting the change.	No exceptions noted.
Verification and notification of electronic data submission forms are completed by user organizations to certify to the completeness and accuracy of the organization's EMIS data provided to NEOnet.	Inspected the verification forms of all user organizations for one reporting period (October 09K) to confirm the forms were completed.	No exceptions noted.
NEOnet performs certain routine jobs for system maintenance through a scheduling program, DECScheduler.	Inspected the DECScheduler listing of jobs and the OpenVMS system startup file to confirm that DECScheduler was initialized during the startup of the system and routine jobs are scheduled.	No exceptions noted.
A service agreement with Service Express covers technical support and maintenance on the computer hardware.	Inspected the service agreement, support account detail, and payment documentation for evidence of hardware support.	No exceptions noted.
All ITC equipment is covered by insurance.	Inspected the insurance policy and payment documentation for evidence of coverage.	No exceptions noted.
Services on the Alpha are monitored using a software utility, WhatsUp, and technical staff are notified via phone and e-mail when problems occur.	Inspected the list of services monitored on the Alpha and the action policy established for notifying technical staff when problems occur.	No exceptions noted.

IT Operations - Control Objective: Backup - Up-to-date backups of programs and data should be available in emergencies.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Backups of programs and data are performed regularly. The scheduling of the backup procedure is automatically performed each time the backup script is run.	Inspected the DECScheduler and backup command scripts to confirm the backup scripts are scheduled to run each night. Inquired with the coordinator of software services and the assistant director / technical services manager regarding the backup process.	No exceptions noted.
Backup tapes are stored in a secure on-site location and are rotated off-site regularly.	Inspected the STORserver tape library storage of daily backup tapes for evidence of tape maintenance. Inspected a screen print of the "data storage manager software" which indicates the creation and retention of backup tapes as well as whether their location is on-site or off-site. Inspected the signed pickup authorization forms for evidence of off-site rotation of backups by a third-party vendor twice a week. Inspected the contract and payment documentation for off-site rotation of backup tapes.	No exceptions noted.

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name: Northeast Ohio Network for Educational Technology (NEOnet)
Number: 7
Node Name: SCECA0

Chairperson: Wayne Blankenship
Superintendent
Nardon Hills City School District

Fiscal Agent: Metropolitan Regional Service Council (MRSC)

Administrator: Matthew Gdovin
Executive Director
NEOnet

Address: 420 Washington Avenue
Cuyahoga Falls, OH 44221

Telephone: 330-926-3900
FAX: 330-926-3901

Web site: www.neonet.org

OTHER SITE STAFF

Matthew Gdovin	Executive director
Christopher Zolla	Assistant director / technical services manager
Debra Carroll*	Assistant director /operations manager
Paulette Gansel	Coordinator software services
Connie Enders	Fiscal software support specialist
Barbara Couch	Student software support specialist
Denise Marrali	Student software support specialist
Jennifer Cottrill	Student software support specialist
Kathy Peters	Student software support specialist
Nancy Butts	Student software support specialist
Mary Dolis	EMIS software support specialist
Michael Hoffman	Application developer
Tim Tracy	Senior systems administrator
Cyrus Elder	System administrator
Robert Phillips*	Technical specialist
Jim Martin	Media specialist
Jeanne Steele	Media services support specialist

* Positions were terminated as of the end of the audit period.

HARDWARE DATA

Central Processors and Peripheral Equipment

<u>Model Number</u>		<u>Installed</u>		<u>Capacity/Density/Speed</u>	
CPU:	DEC Alpha 4100	Lines/Ports:	N/A	Memory Installed:	8.0 GB
Disk:	RZ1DF-VW	Units:	1	Total Capacity:	9.1 GB
Disk:	RZ1FC-VW	Units:	7	Total Capacity:	254.8 GB
Disk:	RZ1DA-VW	Units:	5	Total Capacity:	45.5 GB
Disk:	RZ1CB-VW	Units:	5	Total Capacity:	21.5 GB
Disk:	RZ29B-VW	Units:	1	Total Capacity:	4.3 GB
Tape Unit:	TSZ07	Units:	1	Max Density:	6250 BPI
Tape Unit:	EXABYTE	Units:	1	Max Density:	8 mm
Printer:	T6101	Units:	1	Print Speed:	600 LPM

USER ORGANIZATION SITE DATA

<u>IRN</u>	<u>USER ORGANIZATION</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS/EIS</u>	<u>EMIS</u>
046557	Cuyahoga Heights Local School District	Cuyahoga	X	X	X	X
044636	Parma City School District	Cuyahoga	X	X		X
046599	Richmond Heights Local School District	Cuyahoga	X	X	X	X
044164	Kent City School District	Portage	X	X	X	X
149286	Kent Digital Academy	Portage	X			X
051391	Maplewood Career Center JVSD	Portage	X	X	X	X
043661	Brunswick City School District	Medina				X
048470	Buckeye Local School District	Medina	X	X	X	X
048488	Cloverleaf Local School District	Medina	X	X	X	X
062109	Medina County Career Center	Medina	X	X	X	X
048454	Medina County Educational Service Center	Medina	X	X		X
149054	Akron Digital Academy	Summit	X			X
043539	Barberton City School District	Summit	X	X	X	X
049981	Copley-Fairlawn City School District	Summit	X	X	X	X
049999	Coventry Local School District	Summit	X	X	X	X
043836	Cuyahoga Falls City School District	Summit	X	X	X	X
147231	Schnee Learning Center (Cuyahoga Falls Digital Academy)	Summit	X			X
050013	Green Local School District	Summit	X	X	X	X
050021	Hudson City School District	Summit				X
050005	Manchester Local School District	Summit	X	X	X	X
050039	Mogadore Local School District	Summit	X	X	X	X
050047	Nordonia Hills City School District	Summit	X	X	X	X
044552	Norton City School District	Summit	X	X	X	X

USER ORGANIZATION SITE DATA

<u>IRN</u>	<u>USER ORGANIZATION</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS/EIS</u>	<u>EMIS</u>
063495	Portage Lakes Career Center	Summit	X	X	X	X
050054	Revere Local School District	Summit	X	X	X	X
050062	Springfield Local School District	Summit	X	X	X	X
044834	Stow-Munroe Falls City School District	Summit	X	X	X	X
049965	Summit County Educational Service Center	Summit	X	X	X	X
044883	Tallmadge City School District	Summit	X	X	X	X
050070	Twinsburg City School District	Summit	X	X	X	X
049973	Woodridge Local School District	Summit	X	X	X	X
TOTALS:			29	26	24	31



Mary Taylor, CPA
Auditor of State

NORTHEAST OHIO NETWORK FOR EDUCATIONAL TECHNOLOGY (NEONET)

SUMMIT 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**