



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

SAS-70

MAY 20, 2000 THROUGH JULY 13, 2001



JIM PETRO
AUDITOR OF STATE

STATE OF OHIO

TABLE OF CONTENTS

I	REPORT OF INDEPENDENT ACCOUNTANTS	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	3
	Control Environment	3
	Risk Assessment	4
	Monitoring	5
	INFORMATION AND COMMUNICATION	5
	GENERAL EDP CONTROLS	6
	Development and Implementation of New Applications and Systems	6
	Changes to Existing Applications or Systems	6
	IT Security	7
	IT Operations	11
III	INFORMATION PROVIDED BY THE SERVICE AUDITOR	13
	GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS	14
	Changes to Existing Applications or Systems	14
	IT Security	15
	IT Operations	23
IV	OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION	27
	DATA ACQUISITION SITE PROFILE	27

This Page Intentionally Left Blank



STATE OF OHIO
OFFICE OF THE AUDITOR

JIM PETRO, AUDITOR OF STATE

88 East Broad Street
P.O. Box 1140
Columbus, Ohio 43216-1140
Telephone 614-466-4514
800-282-0370
Facsimile 614-466-4490
www.auditor.state.oh.us

REPORT OF INDEPENDENT ACCOUNTANTS

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 member school district'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 member school districts 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 13, 2001. 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.

As discussed in the accompanying description, NEOnet has a reciprocal agreement for use of hardware at another Data Acquisition Site. However, a formal Disaster Recovery Plan has not been developed. The deficiency results in policies and procedures not being suitably designed to meet the control objective, "Adequate plans should exist for the recovery of critical resources following an event which disrupts data processing services for an extended period of time."

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 13, 2001. Also, in our opinion, except for the matter described above, 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 member school districts 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 20, 2000 to July 13, 2001. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to member school districts of the NEOnet and to their auditors to be taken into consideration along with information about the internal control at member school districts, when making assessments of control risk for member school districts. 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 20, 2000 to July 13, 2001.

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

The information in Section IV describing the data acquisition site 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 member school districts and, accordingly, we express no opinion on it.

The description of controls at the NEOnet is as of July 13, 2001, and information about tests of the operating effectiveness of specified controls covers the period from May 20, 2000 to July 13, 2001. 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 member school districts, and the independent auditors of its member school districts.

JIM PETRO
Auditor of State

July 13, 2001

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The NEOnet's 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 NEOnet's description of controls.

OVERVIEW OF OPERATIONS

The Northeast Ohio Network for Educational Technology (NEOnet) is a not-for-profit computer service organization owned and operated by eighteen school district's in the Ohio counties of Summit and Portage. The primary function of the NEOnet is to provide information technology services to its member school districts with the major emphasis being placed on accounting, payroll and inventory control services. The NEOnet is located in Cuyahoga Falls, Ohio.

The NEOnet is one of 23 not-for-profit computer service organizations serving more than 600 public school districts and county educational service centers in the State of Ohio. Throughout the remainder of this report, any reference to member school districts will also include the county educational service centers. These service organizations, known as Data Acquisition Sites (DAS) and their member school districts make up the Ohio Educational 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 school districts. Funding for this network and for the NEOnet is derived from the State of Ohio and from user fees.

The laws governing the Ohio Education Computer Network require that a school district serve as fiscal agent for Data Acquisition Sites receiving state funds. Specifically, revised code section 3301.075 requires the NEOnet conform to revised code section 3313.92 in order for the NEOnet to receive Ohio Education Computer Network funds from the State Department of Education. Agreements entered into pursuant to revised code section 3313.92 must be approved by the State Superintendent of Public Instruction, who has interpreted this revised code section to require a board of education to serve as fiscal agent for a Data Acquisition Site receiving funds from the Ohio Education Computer Network. For this reason, the Educational Service Center of Summit County serves as fiscal agent for the NEOnet and performs certain functions to ensure receipt of funds from the Ohio Education Computer Network. Essentially, these functions are to apply for and maintain the Data Acquisition Site permit for the central data processing equipment, and to hold legal title to the central data processing equipment.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the Site Manager and the Board of Directors. The consortium's General Assembly as well as the Board of Directors are the oversight organizations for the NEOnet. One member from each member district is appointed to the assembly and is normally the

district superintendent. 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 the NEOnet and meets five times a year. The board consists of the following positions:

- Superintendent of the Fiscal Agent
- Chair of each Operating committee
- Chair of the Assembly
- Three “at-large” Assembly Members
- Site Manager (ex-officio)
- Treasurer of the Fiscal agent (ex-officio)

The NEOnet employs a staff of 15 individuals and is supported by the following functional areas:

Software Support- Supports end users in a given area of concentration related to either student services applications or the state financial applications.

Technical Support- Supports the NEOnet’s computer systems and its networked communication system. Provides user training and support.

All staff members report to the Site Manager.

The NEOnet is generally limited to recording user organization transactions and processing the related data. Users 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 NEOnet employees may alter user data and only at the request of the member school district. Completion of a Job Record form is required for all changes and the forms are periodically reviewed by the Site Manager.

The NEOnet follows the same personnel policies and procedures as their fiscal agent, the Summit County Educational Service Center. The NEOnet 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.

The 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 the 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 fifteen hours of approved professional development training annually, and at least eighty hours of approved training every four years. Employee evaluations are conducted annually.

Risk Assessment

The NEOnet does not have a formal risk management process; however, the NEOnet Board of Directors actively participates in the oversight of the

organization.

As a regular part of its activity, the Board of Directors addresses:

- new technology
- realignment of the NEOnet organization to provide better service
- personnel issues, including hiring, termination, and evaluations
- additional services provided to member school districts and other entities
- changes in the operating environment as a result of ODE requirements, AOS and other accounting pronouncements and legislative issues

In addition, the NEOnet has identified operational risks resulting from the nature of the services provided to the member school districts. 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 that all staff members report directly to the Site Manager. The NEOnet staff have worked here for many years and are experienced with the systems and controls at the NEOnet. The NEOnet Site Manager 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 sent to management via email. 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 member school districts are discussed within the General EDP control sections.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

There are no systems development activities which are actually performed by NEOnet personnel. The NEOnet utilizes the software which is supplied by the State Software Development Team (SSDT) at the Northwest Ohio Computer Association (NWOCA) which is another DAS of the OECN. The ODE determines the scope of software development for state supported systems. Tactical means of accomplishing the priorities are determined by the SSDT, which consists of staff members from the ODE and the NWOCA. The development team meets on a periodic basis to discuss the status of proposed and ongoing projects.

The majority of the significant application changes are mandated by the ODE. For those changes which are not required by the ODE, a software change impact statement is completed by the SSDT after discussion of the need for the change. Requests for changes to applications originate from three sources: the Compaq/Notes or SiteScape Forum, the help line, or suggestions made by individuals on the SSDT. Requests may be made by users at member school districts, the DAS, or others with access to the forums.

Changes to Existing Applications or Systems

There are no maintenance activities which are actually performed by the NEOnet personnel. The NEOnet utilizes the software which is supplied by the SSDT at the NWOCA. The OECN requires the DAS to keep the version of each software package current based on the provider's standard for continued support.

Procedures are in place to ensure the SSDT developed applications are used as distributed. On a quarterly basis, updates to the state software are downloaded from the SSDT at the NWOCA to the other DAS. Source code is not distributed. Release notes explain the changes, enhancements and problems corrected. User and System Manager manuals are also distributed. The NWOCA informs the other DAS that they will support only the latest release of the state software beginning 30 days following the software release date.

Only vendor supplied changes are made to the operating system or system software documentation. The NBEC, who acts as the fiscal agent for this and other participating DAS, has entered into a license under the Campuswide Software License Grant Program (CSLG) through the Management Council of the Ohio Education Computer Network (MCOECN), for acquiring and/or providing software maintenance services for a limited series of Compaq 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 DAS for a limited series of Compaq software packages as approved by the Board of Trustees of the MCOECN.
- Provide telephone technical support to the participating DAS technical staff for a limited series of Compaq software packages approved by the Board of Trustees of the MCOECN.

- Track and maintain an accurate listing of all Compaq 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 Data Acquisition Sites' technical staff on the latest releases of Compaq software packages covered under the agreement.

As a participating member of the program of the MCOECN the participating DAS 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.
- Read, cooperate, and comply with both the CSLG and ESL Management Plans as adopted and approved by the Executive Committee of the MCOECN.
- Provide any necessary access to all computer systems covered under the agreement for the purposes of identifying and/or correcting problems of distributed software.
- Upon written notice, provide Compaq with physical access to computer facilities at reasonable times during normal business hours for the purpose of inspecting sites and system records for compliance with the terms of the CSLG and ESL Programs.

IT Security

The NEOnet has a security policy that outlines the responsibilities of member school district personnel, the NEOnet personnel, and any individual or group not belonging to the member school district or the NEOnet. In addition to the security policy, the 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 the NEOnet personnel.

The NEOnet staff 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.

Users from the member school districts are granted access upon the receipt of authorization (email or written) from the superintendent, treasurer or assigned Technology Coordinator. Authorization forms are sent to the NEOnet staff and the technical support staff members will create the account and contact the user regarding the newly established account. Authorization forms are maintained in the district's file by the technical support staff member creating the account. Data center personnel access is authorized and created by the Site Manager.

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 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 through OpenVMS to monitor any security violations on both NEOnet systems:

- 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 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.

Primary logical access control to the Compaq 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. Proxy records are located in the NETPROXY.DAT file. The NEOnet utilizes proxy logins.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the NEOnet. For member school districts which use the NEOnet system, UICs are also individually assigned at the request of the member school district. 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 and CAPTIVE flags are not used for NEOnet staff members 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 and CAPTIVE flags.

The system forces users to periodically change their passwords. All administrative, teacher and student accounts have a password lifetime of 90

days. Passwords are set to expire (masking the account with the pre-expired parameter PWDEXPIRE) 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. The minimum password length for each user is typically the default of eight.

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 through the use of Compaq established defaults. Any changes are logged and reviewed by the Site Manager and the Director of Network Services.

A timeout program, HITMAN, is used to monitor terminal inactivity and log-off inactive users after a predetermined period of time of non-use. 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 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 User Identification Code (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 SYSGEN parameter MAXSYSGROUP (default decimal 8, octal 10). (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's UAF 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 member school district users have NORMAL privileges.

The WRITE and DELETE access capabilities are not activated for WORLD access to the files in the SYS\$SYSROOT directory. The UIC associated with each of these files is within the MAXSYSGROUP number.

To limit access to security files, the NEOnet has limited the WORLD access for the SYSUAF.DAT file, which contains account information to identify which users are allowed access to accounts on the system; the NETPROXY.DAT file, which contains proxy account information to identify which remote users are allowed access to proxy accounts on the system; and the RIGHTSLIST.DAT file, which contains names of the reserved system identifiers and identifiers for each user.

Access to the OECN software packages is controlled at the DAS 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 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 protection prevents WORLD WRITE or DELETE access to USAS, USPS, SAAS/EIS and EMIS application data files.

Member school districts have been set up with sub-networks which have addresses not recognizable to the Internet. This is called a private internal network. A Cisco PIX (Private Internet Exchange) firewall and a router have been placed between the Internet access provided by the OECN network and the internal network of the member districts of the NEOnet. The PIX firewall equipment and an additional routing device deny all outbound traffic requests originating from the sub-network. Instead the requests are routed to the PIX firewall where it performs the function of a proxy server and acts as a middle man between the Internet and the internal network. The firewall and routing devices also deny access to all inbound traffic unless the IP traffic originated from the firewall or from inside the network as a result of firewall settings.

NEOnet also makes available an Internet content filter. The filter is an optional service which screens Internet site requests for "unsuitable" content.

The data processing department is located in an enclosed area which is secured by both key locks and a security system. All doors are locked during off hours. During business hours the main door is unlocked, however, data processing 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 the data processing staff and the maintenance personnel. Motion detectors 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,
- A power conditioner.

IT Operations

Traditional computer operations procedures are minimal since users at the member school districts 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 both the VAX and Alpha systems. In addition, all users, except students, have access to SiteScape Forum, which is a bulletin board that allows the NEOnet employees to communicate with users across the state. Users can post questions and/or comments to the NEOnet staff.

User problems that require the NEOnet staff to change data require the completion of a Job Record Form. These forms are periodically reviewed by the Site Manager to verify processing was not interrupted. In addition, the member school districts have the option of printing an "AUDIT" report that shows all activity 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 both the VAX and Alpha Systems.

Common problems that arise daily, such as terminal lockups and program crashes, are usually handled by the NEOnet service representatives over the phone and may not be documented within the Help Desk Log. However, major problems are still logged through the Help Desk Log. Any system

or network problems are communicated to the Site Manager.

NEOnet has a hardware maintenance agreement with Compaq. The coverage of the equipment is based on two service levels, a DECSservice and a Basic Service. A maintenance agreement is also in place for communications equipment utilized by both the member school districts and the NEOnet.

Data integrity is maintained by the software through validity checks on all input.

The NEOnet follows the guidelines of the Ohio Educational Computer Network (OECN) for backing up system data and programs. Full system backups are performed daily for the computer system. The tapes are stored in the computer room at the data center which is protected by fire detection equipment. Every Friday, the previous evening's tape is rotated to a data security storage facility, which is located thirty miles away from NEOnet, and the tape is retained at the facility for three weeks.

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

All system and program documentation is stored electronically and is subject to the same backup procedures as the other data files. The written backup procedures include the frequency of tape backups, the rotation schedule and the retention period.

The NEOnet has entered into a reciprocal disaster recovery agreement with the Stark/Portage Area Computer Consortium, (SPARCC), located in Canton Ohio.

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

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 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 the NEOnet and procedures performed at member school districts that utilize the 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 or Systems

Changes to Existing Applications or 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>
Procedures are in place to ensure that SSDT developed applications are used as distributed. Quarterly updates to the applications are downloaded by NEOnet. Source code is not distributed.	To ensure the USAS, USPS, SAAS, and EMIS software tested at NWOCA is the same version used at NEOnet, a cyclical redundance check (CRC) of the object program files for each application were obtained and compared to the CRCs of the latest ODE version tested at the NWOCA.	The CRCs of the object code for the USAS, USPS, SAAS/EIS and EMIS applications at the NEOnet were the same as the CRCs of the object code from the NWOCA.
The SSDT distributes release notes explaining the changes, enhancements and problems corrected.	Obtained and reviewed the most recent release notes for the state software. Compared and agreed the version numbers on the Release Notes to the version numbers listed on the CRC comparisons.	The SAAS, EMIS, USPS, and USAS release notes all contained changes made, enhancements implemented and problems corrected. The version numbers on the CRC output and the release notes matched.
NEOnet receives upgrades and patches to system software through another DAS (NWOCA) as part of the MCOECN CSLG agreement.	Obtained and reviewed a copy of the NEOnet's CSLG licensing agreement with the NBEC to determine if it is current.	The NEOnet was a participating member of the OECN CSLG program for its system software for the period of July 1, 2000 through June 30, 2001.

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>
The NEOnet has established a security policy to outline management's policies regarding computer security and access.	Obtained and reviewed the Data System Security Policy to determine if user responsibilities are documented. Also discussed the policy with the interim Site - Manager to determine if these policies are communicated to the member school districts.	A Data System Security policy exists and documents data security procedures, data access requirements for school district and computer center personnel, and access by outside users.
Authorization from the appropriate district management is required before setting up a user account on the Alpha.	<p>Obtained and reviewed the new users listing using a security analysis tool to extract information from the security file, SYSUAF. LIS. Selected 20 new users to test the following:</p> <ul style="list-style-type: none"> • Verified only authorized individuals were making the requests. • Compared the requested access rights of the users to their actual user profiles to determine if there were any differences. <p>In addition, reviewed all accounts from the previous year's exception list to determine if the NEOnet followed up on previously identified exceptions.</p>	<p>One of the twenty authorizations forms was not available. For the forms on file, only authorized personnel (treasurers, superintendents, or technology coordinators) requested user access, and users were not granted access rights, other than what was requested.</p> <p>Seven of the eleven accounts from the previous year's exception report were removed from the Alpha. Two of the four accounts remaining did not have authorization forms on file, but were being actively researched for removal.</p>
Banner screens are displayed before a user logs on to the system.	Observed the banner screen to ensure it is displayed upon logon and reviewed the content of the screen message.	The banner screen is displayed upon logon and indicates that the use of the system is restricted to authorized individuals.

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>
Detection control alarms are enabled through OpenVMS to monitor security violations.	Obtained and reviewed the security alarms enabled from the, Senior Software Support Specialist, via the DCL command SHOW AUDIT/ALL.	System security alarms and audits have been enabled for ACL, Authorization, Audit, Breakin and Logfailure.
Member School District User Control Considerations: Determine if district management makes users aware of the confidential nature of passwords and that the users should take precautions to ensure passwords are not compromised. Determine if district management immediately requests the NEOnet revoke the access privileges of district personnel when they leave or are otherwise terminated. Verify if the district has a documented acceptable use policy defining what activities are deemed appropriate for the use of the Internet access provided to the district. Internet users should be required to accept the terms of the policy before access is provided.		
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>
Wild card characters are not used in the NETPROXY listing.	Obtained the PROXY listing from the Senior Software Support Specialist via the SH/PROXY command and reviewed the listing for use of wild card characters.	There were no wildcard characters used in the PROXY listing.

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:
Password values have been enabled to deter unauthorized access through compromised passwords.	A security analysis tool, was used to extract information from the OpenVMS security file, SYSUAF. LIS, to identify the following: <ul style="list-style-type: none"> • User accounts with a password of less than six characters, • User accounts with a password lifetime of greater than ninety days, Reviewed the default account to determine if the pre-expired parameter was set, and reviewed a list of accounts with pre-expired passwords to verify that the parameter is in use.	Accounts are required to be password protected with a password of at least six characters in length. Account password lifetimes for 21 of the 1765 accounts exceeded the 90 day change requirement. These accounts were a combination of the following acceptable policy deviations: <ul style="list-style-type: none"> • Application or operating system support accounts • Accounts used to access the card catalog system, or • Individual accounts used as guest or pass through accounts provided to individuals or other DASs as needed. The pre-expired parameter was set on the default account. From review of the list of pre-expired accounts, it appears that accounts are set up with pre-expired passwords.
Log-in parameters have been set to control and monitor sign-on attempts.	Using the OpenVMS System Generation (SYSGEN) Utility, the Senior Software Support Specialist, printed the OpenVMS Login parameters via the SHOW /LGI command. Parameters were reviewed for appropriateness.	Parameters have been set and controls are in place to address sign on attempts and sign on constraints for break-in detection and evasion. All of these SYSGEN parameters are consistent with the recommended defaults.

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>
HITMAN monitors terminal activity and logs off inactive users.	Reviewed the HITMAN parameters to determine if they were set to automatically logoff inactive users. Reviewed the SYSTARTUP_VMS.COM file to determine if the HITMAN utility is part of the startup procedures.	HITMAN Prime hours are 8:00 am to 5:00 pm, Monday through Friday. HITMAN Non-Prime hours are 5:01 pm to 7:59 am evenings and weekends. First and second warnings are given at thirty and forty-five minutes respectively, with processes being killed at sixty minutes of idle time. Several UICs and system processes, by default, are protected from termination. Additionally, all NEOnet staff members are protected during Prime hours. The only terminal protected for both Prime and Non-Prime hours is the operator's console. From review of the SYSTARTUP_VMS.COM file, HITMAN is part of the daily start up procedure.
Access to production data files and programs is properly restricted.	Obtained and reviewed a directory listing of the executable files for the USAS, USPS, EMIS and SAAS/EIS application programs to verify WORLD Access was limited to READ and/or EXECUTE. Through the use of a command procedure, the data files of all member school districts were reviewed for WORLD WRITE or DELETE access.	Executable files do not have WORLD WRITE or DELETE access. The district data files do not have WORLD access.

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:
The internal network used at the NEOnet uses a 10-dot network, which is an addressing scheme unable to be used over the Internet.	Reviewed an active user listing which identified port/address assignment. Observed settings in the firewall and Cisco router configurations for use of the ten dot network addressing scheme.	Active user listings and configuration file statements indicate that the addressing scheme used is a 10-dot network.
Access to the Internet is controlled with the use of a PIX firewall, and a Cisco router.	Reviewed the network diagram with the Director of Network Services. Observed the existence of the PIX firewall and Cisco router used to control Internet access. Observed settings in the Pix Firewall, and Cisco Router configurations.	Internet traffic is controlled within both devices given the current configuration settings, although an exception was noted in the PIX firewall configuration. The current configuration permits internet traffic to pass through the firewall to the production server, exposing it to a variety of security attacks. These attacks could, if successful, allow for unauthorized access to NEOnet's production computer resources and data, or result in the disabling of the production server.
Member School District User Control Consideration: Determine if User Identification Codes (UICs) are individually assigned to each system user to improve individual accountability of user activity.		

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 the applications necessary to perform their job function.	Discussed the OSA utility with the Senior Software Support Specialist, and reviewed a listing of all accounts with OECSN identifiers for the USAS, USPS, SAAS/EIS and EMIS applications.	Identifiers are assigned at the OpenVMS level to each individual user account per the request of appropriate district personnel. Unusual requests, such as USPS access for a guidance counselor, would be confirmed with the same appropriate district personnel.
The OECSN_SYSMAN identifier is restricted to only authorized users.	Obtained and reviewed a listing of all users having the OECSN_SYSMAN identifier. Discussed the functionality of the identifier with Senior Software Support Specialist.	Accounts that have the identifier fall into one of the following appropriate four groups: <ul style="list-style-type: none"> • Data processing personnel, • System management accounts, • Demonstration accounts or • Application development accounts.
Member School District User Control Consideration: Verify that User Identification Codes (UICs), passwords and associated access privileges are issued only to authorized users who need access to computer resources to perform their job function.		

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 WRITE and DELETE access are absent from the SYS\$SYSROOT directories.	Obtained the file directory listing for the SYS\$SYSTEM and SYS\$MANAGER directories and reviewed the file protection masks for WORLD WRITE or DELETE access.	There were no files having WORLD access equal to WRITE and/or DELETE.

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>
System level UICs are restricted to only authorized personnel.	Through the OpenVMS System Generation (SYSGEN) utility used the SHOW MAXSYSGROUP command to determine the MAXSYSGROUP number. Utilized a security analysis tool to review a listing of all accounts with a UIC less than the MAXSYSGROUP number, and a list of all accounts with elevated privileges (more than NETMBX and TMPMBX).	MAXSYSGROUP is set at eight. Only four accounts have UICs less than MAXSYSGROUP. These group assignments are appropriate because these accounts are necessary system accounts. None of the accounts belong to users. All accounts with elevated privileges are appropriate. The accounts were either employees of the NEOnet, system, or support accounts.
The use of an alternate SYSUAF file is not permitted.	Through the SYSGEN utility using the SHOW UAFALTERNATE command, determined whether or not the parameter's setting allows for the use of an alternate SYSUAF file.	The value of the UAFALTERNATE is '0', which means the operator cannot specify another SYSUAF file other than the default (SYSUAF.DAT) during system startup.
WORLD access is absent from the SYSUAF.DAT, NETPROXY.DAT and RIGHTSLIST.DAT security files.	Obtained the file directory listing for the system directories and reviewed the file protection masks on the SYSUAF.DAT, NETPROXY.DAT and RIGHTSLIST.DAT files.	The security files, SYSUAF.DAT, NETPROXY.DAT and RIGHTSLIST.DAT, have no WORLD access.
Remote administration of the firewall and routers used to control Internet access is restricted.	Reviewed the PIX firewall configuration to determine if passwords are required to access the routing equipment used to control Internet access. Observed the use of passwords to access inquiry and configuration modes on both devices.	Passwords are required to access both the inquiry and configuration modes.

<p>IT Security - Control Objective: Physical Security - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.</p>		<p>Control Objective Has Been Met</p>
<p><i>Control Procedures:</i></p>	<p><i>Test Descriptions:</i></p>	<p><i>Test Results:</i></p>
<p>Physical access to the computer room and its contents is restricted to authorized personnel.</p>	<p>Observed the key pad entry devices and use of the devices throughout the period of fieldwork. Observed the existence of motion detection devices.</p>	<p>Key pad entry devices protect entrance into the computer room. Doors are locked at all times. Motion detectors are located throughout the building in which NEOnet is located. Other equipment was located outside the computer room and is subject to the building's general security controls.</p>
<p>Environmental controls are in place to protect against or detect fire, water, humidity, or changes in temperature.</p>	<p>Toured the computer room and observed the existence of the listed environmental controls.</p>	<p>A Liebert system is used to control temperature and humidity. Fire extinguishers are located in the computer room and data center and were last tested in August of 2000. Elevated flooring is utilized in the computer room.</p>
<p>Member School District User Control Considerations: Determine that terminals are protected against damage or misuse by having separate areas, either independent rooms or sections of rooms that restrict access to only authorized individuals. Verify that communication lines, junctions and modems secured in an area that restricts access to only authorized individuals.</p>		

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>
Procedure manuals for both the VAX and Alpha systems are on-site and accessible.	Verified existence of current VAX and Alpha manuals on-site at the NEOnet. Observed the use of the online reference materials.	The procedural manuals are used as a reference on occasion. On line references are also available.
A Job Record form is completed when changes to member school district files are requested by users.	Obtained and reviewed copies of the Job Record forms. Discussed the process of changing data for member school district with the Senior Software Support Specialist.	A NEOnet employee completes a Job Record form before any requested changes can be made. These forms are periodically reviewed by the Site Manager to verify processing was not adversely affected.
The program DECScheduler is run to schedule and perform routine system maintenance.	Obtained and reviewed the a listing of jobs included under DECScheduler. Discussed the maintenance procedures and the command procedure with the Technical Support Specialists.	DECScheduler is used to execute routine jobs, such as backups, directory updates, and data cleanup, in a batch mode.
Checklists are used to monitor batch processing performed for the EMIS application.	Obtained and reviewed the checklists maintained by the NEOnet for the batch processing performed for EMIS.	EMIS processing is controlled through the use of check lists and monitoring by the NEOnet personnel.

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>
The NEOnet has hardware maintenance agreements with the Compaq Corporation and DataServ to provide service to hardware.	Obtained and reviewed the hardware maintenance agreements in effect during the audit period.	NEOnet has a hardware maintenance agreement with Compaq that is invoiced on a monthly basis. The agreement allows for service calls to be made on both week days and weekends. NEOnet also has a maintenance agreement with DataServe. The maintenance period for both agreements was from July 1, 2000 to June 30, 2001.

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.	Discussed backup procedures with the Technical Support Specialist. Obtained and reviewed the written backup procedures and the DECScheduler list for daily backup jobs.	The NEOnet has documented backup procedures for backing up all system and data files. Full system backups are performed daily, Monday through Friday. Monthly, quarterly, and year end backups are also performed.
Backups tapes are stored at a secure off-site locations.	Toured the off-site storage facility and observed NEOnet's backup tapes to ensure that they are rotated to an off site storage facility. Discussed the off-site storage procedures with the Technical Support Specialist.	Three weeks of backup tapes were present at the off-site storage facility. The facility is environmentally controlled and secure and is not in close proximity to the data center.

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>
Member School District User Control Considerations: Determine if the district retains source documents for an adequate period to ensure data can be re-entered in the event that data files are destroyed prior to being backed up and rotated off-site. Verify the district establishes and enforces a formal data retention schedule with the NEOnet for the various application data files.		
IT Operations - Control Objective: Disaster Recovery - Adequate plans should exist for the recovery of critical computer resources following an event which disrupts data processing services for an extended period of time.		Control Objective Has NOT Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The NEOnet has entered into a reciprocal agreement with SPARCC for use of their computer facilities in the event of a disaster.	Obtained and reviewed the signed copy of the reciprocal agreement.	The NEOnet has a reciprocal agreement with Stark/Portage Area Computer Consortium (SPARCC). The agreement with SPARCC was resigned on June 21, 2001 and remains in effect until either party cancels the agreement. Cancellation requires a 30 day written notice. The agreement outlines the following services in the event a disaster should disable the data processing equipment: <ul style="list-style-type: none"> • Access to the computer facility of the functioning site • Computer time and personnel assistance • Cost for services • Other services as mutually agreed upon

<p>IT Operations - Control Objective: Disaster Recovery - Adequate plans should exist for the recovery of critical computer resources following an event which disrupts data processing services for an extended period of time.</p>		<p>Control Objective Has NOT Been Met</p>
<p><i>Control Procedures:</i></p>	<p><i>Test Descriptions:</i></p>	<p><i>Test Results:</i></p>
<p>All data center equipment is covered by insurance.</p>	<p>Obtained and reviewed the anniversary endorsement statements for the Summit County Educational Service Center for the period from 02/15/00 through 02/15/01, and 02/15/01 through 02/15/02.</p>	<p>Computer equipment is covered under the business personal property insurance maintained by NEOnet's fiscal agent, the Summit County Educational Service Center. The anniversary endorsement statements indicated that coverage was provided for the entire audit period and is in force through 02/15/02.</p>
<p>Member School District User Control Consideration: Verify the district develops, tests and maintains their own contingency procedures to be performed in the event of an extended loss of computer resources. Such procedures should be established based upon the maximum outage tolerances for critical applications.</p>		

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

DATA ACQUISITION SITE PROFILE OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Consortium Name:	Northeast Ohio Network for Educational Technology (NEOnet)
Consortium Number:	7
Node Name:	SCECA0
Consortium Chairperson:	Larry Roberson Superintendent Coventry Local School District
Fiscal Agent District:	Summit County Educational Service Center
DAS Administrator:	Mr. Matthew Gdovin Site Manager NEOnet
Site Manager's Address:	420 Washington Avenue Cuyahoga Falls, OH 44221
Site Manager's Telephone:	330-945-9600 ext. 269
FAX:	330-945-9784
Data Center Address:	420 Washington Avenue Cuyahoga Falls, OH 44221
Data Center Telephone:	330-945-6266

OTHER SITE STAFF

Robert Cochran
Denise Marrali
Paulette Gansel
Barb Couch
Mary Dolis
Neal Strefeler
Bill Manley
Cass Gowins
Jim Fortney
George Kellon
Robert Phillips
Denis Boatright
Robert McNutt
Cyrus Elder

INFOhio Support
Fiscal Operations Support Spec.
Senior Software Support Spec.
Senior Software Support Spec.
Senior Software Support Spec.
Software Support Specialist
Software Support Specialist
Director of Network Services
Technical Support Specialist
Technical Support Specialist

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

<u>Model Number</u>	<u>Installed</u>	<u>Capacity/Density/Speed</u>
CPU: DEC Alpha 4000	1997	Memory Installed: 2.0 GB
Disk: RZ29	Units: 6	Total Capacity: 18.0 GB
Tape Unit: TSZ07	Units: 1	Max Density: 6250 BPI
Tape Unit: EXABYTE	Units: 1	Max Density: 8 mm
Printer: LG06	Units: 1	Print Speed: 600 LPM

CPU Unit 2

<u>Model Number</u>	<u>Installed</u>	<u>Capacity/Density/Speed</u>
CPU: DEC VAX 4705	1995	Memory Installed: 256 Mb
Disk: RZ28	Units: 6	Total Capacity: 12.0 GB

MEMBER SCHOOL DISTRICT SITE DATA

<u>IRN</u>	<u>MEMBER SCHOOL DISTRICT</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>	<u>EMIS</u>
044164	Kent City SD	Portage	X	X	X	X
043539	Barberton City SD	Summit	X	X	X	X
049981	Copley-Fairlawn City SD	Summit	X	X	X	X
049999	Coventry Local SD	Summit	X	X	X	X
043836	Cuyahoga Falls City SD	Summit	X	X	X	X
050013	Green Local SD	Summit	X	X	X	X
050005	Manchester Local SD	Summit	X	X	X	X
050039	Mogadore Local SD	Summit	X	X	X	X
050047	Nordonia Hills City SD	Summit	X	X	X	X
044552	Norton City SD	Summit	X	X	X	X
063495	Portage Lakes JVSD	Summit	X	X	X	X
050054	Revere Local SD	Summit	X	X	X	X
050062	Springfield Local SD	Summit	X	X	X	X
044834	Stow City SD	Summit	X	X	X	X
049965	Summit County Educ Srv Ctr	Summit	X	X	X	X
044883	Tallmage City SD	Summit	X	X	X	X
050070	Twinsburg City SD	Summit	X	X	X	X
049973	Woodridge Local SD	Summit	X	X	X	X
TOTALS:			18	18	18	18



STATE OF OHIO
OFFICE OF THE AUDITOR

JIM PETRO, AUDITOR OF STATE

88 East Broad Street
P.O. Box 1140
Columbus, Ohio 43216-1140
Telephone 614-466-4514
800-282-0370
Facsimile 614-466-4490

NORTHEAST OHIO NETWORK FOR EDUCATIONAL TECHNOLOGY

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
AUGUST 30, 2001**