NORTHEAST OHIO NETWORK FOR EDUCATIONAL TECHNOLOGY (NEOnet)
STATE REGION - ISA, Summit County

SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

APRIL 1, 2013 THROUGH MARCH 31, 2014

Dave Yost • Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

Board of Directors
Northeast Ohio Network for Educational Technology (NEOnet)
700 Graham Road
Cuyahoga Falls, OH 44221

To Members of the Board:

Scope
We have examined NEOnet's accompanying Description of its HP Alpha ES45 system used for processing transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), and School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS) throughout the period April 1, 2013 to March 31, 2014 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of NEOnet's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The NEOnet uses the State Software Development Team (SSDT) located at the Northwest Ohio Computer Association (NWOCA) service organization for systems development and maintenance of the USAS, USPS, and SAAS/EIS application systems. The Description in section 3 includes only the controls and related control objectives of the NEOnet and excludes the control objectives and related controls of the NWOCA. Our examination did not extend to controls of the NWOCA.

Service organization's responsibilities
In section 2, NEOnet has provided an Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. NEOnet is responsible for preparing the Description and for the Assertion, including the completeness, accuracy, and method of presentation of the Description and the Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the Description.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period April 1, 2013 to March 31, 2014.

An examination of a Description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the Description. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in section 3. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The information in section 5 describing the information technology center is presented by the management of NEOnet to provide additional information and is not part of the NEOnet's Description of controls that may be relevant to a user entity'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 entities and, accordingly, we express no opinion on it.

Inherent limitations
Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion
In our opinion, in all material respects, based on the criteria described in NEOnet's Assertion in section 2,

a. the Description fairly presents the system that was designed and implemented throughout the period April 1, 2013 to March 31, 2014.

b. the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2013 to March 31, 2014 and user entities applied the complementary user entity controls contemplated in the design of the NEOnet's controls throughout the period April 1, 2013 to March 31, 2014.

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period April 1, 2013 to March 31, 2014.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Restricted use
This report, including the Description of tests of controls and results thereof in section 4, is intended solely for the information and use of NEOnet, user entities of NEOnet's system during some or all of the period April 1, 2013 to March 31, 2014, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Dave Yost
Auditor of State
Columbus, Ohio

July 11, 2014

This Page Intentionally Left Blank

NEOnet | Northeast Ohio Network for Educational Technology

700 Graham Road
Cuyahoga Falls, Ohio 44221
Phone: 330.926.3900
Fax: 330.926.3901

We have prepared the description of the Northeast Ohio Network for Educational Technology's (NEOnet) *HP Alpha ES45* system (Description) for user entities of the system during some or all of the period April 1, 2013 to March 31, 2014, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a) the Description fairly presents the HP Alpha ES45 (System) made available to user entities of the System during some or all of the period April 1, 2013 to March 31, 2014 for processing their transactions. The NEOnet service organization uses the State Software Development Team (SSDT) located at the Northwest Ohio Computer Association (NWOCA) service organization for systems development and maintenance of the USAS, USPS, and SAAS/EIS application systems. The Description includes only the controls and related control objectives of the NEOnet service organization and excludes the control objectives and related controls of the NWOCA service organization. The criteria we used in making this assertion were that the Description

   i) presents how the System made available to user entities was designed and implemented to process relevant transactions, including

      1) the classes of transactions processed.

      2) the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the System.

      3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the System.

      4) how the System captures and addresses significant events and conditions, other than transactions.

      5) the process used to prepare reports or other information provided to user entities' of the System.

      6) specified control objectives and controls designed to achieve those objectives.

      7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the System.

   ii) does not omit or distort information relevant to the scope of the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and the independent auditors of those user entities, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

b) the Description includes relevant details of changes to the service organization's System during the period from April 1, 2013 to March 31, 2014.

c) the controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period April 1, 2013 to March 31, 2014 to achieve those control objectives and subservice organizations applied the controls contemplated in the design of NEOnet service organization's controls. The criteria we used in making this assertion were that

   i) the risks that threaten the achievement of the control objectives stated in the Description have been identified by the service organization;

   ii) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

   iii) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Matthew Gdovin

Matthew Gdovin
Executive Director

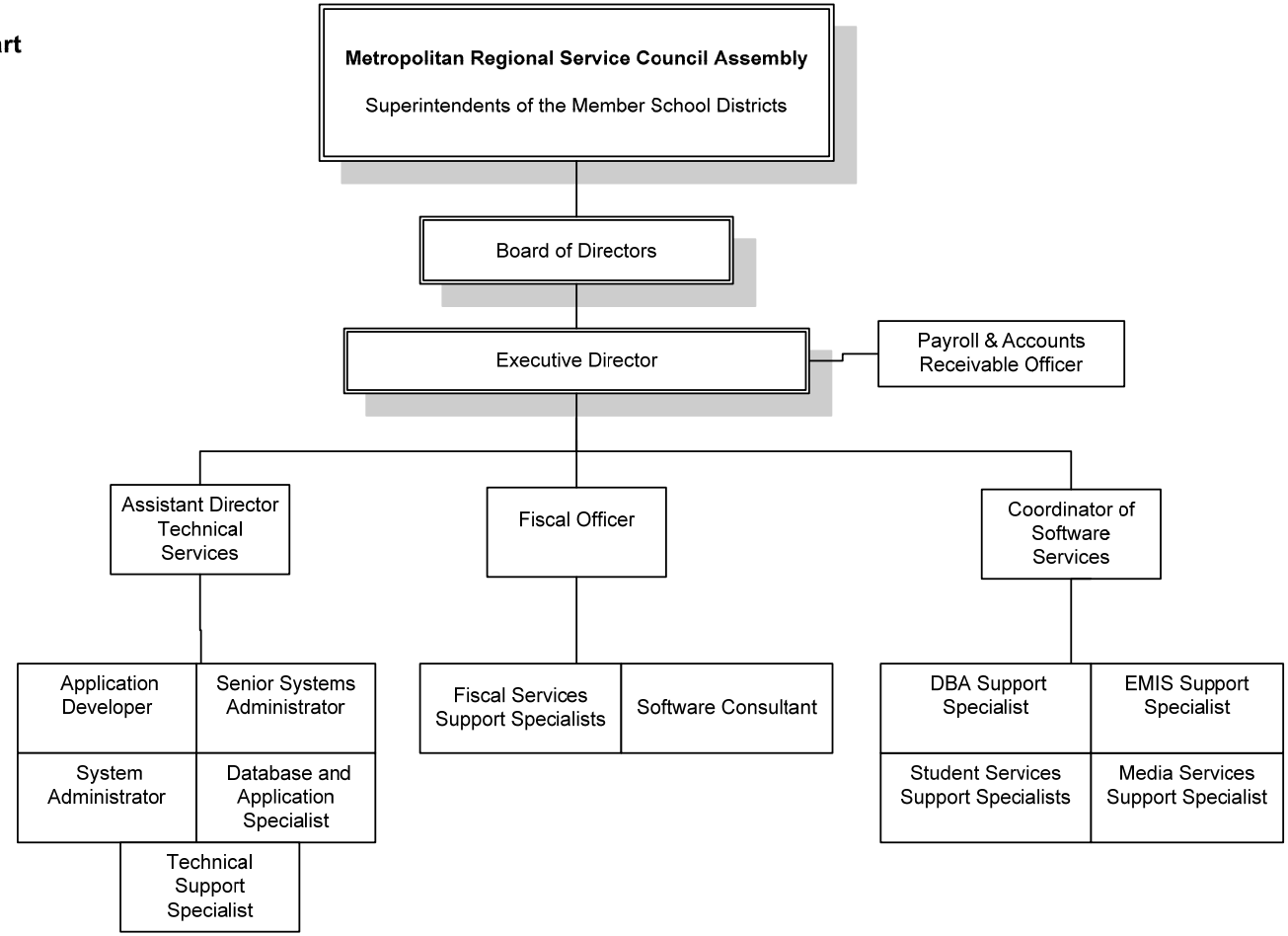
SECTION 3 - DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

The NEOnet's control objectives and related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results", to eliminate the redundancy that would result from listing them here in section 3 and repeating them in section 4. Although the control objectives and related controls are included in section 4, they are, nevertheless, an integral part of NEOnet's description of controls.

OVERVIEW OF OPERATIONS

NEOnet Organizational Chart



NEOnet is one of 22 governmental cooperative shared technology service organizations serving more than 973 educational entities and 1.475 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 entity" 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).

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 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 entity 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 services advisory committee.
- Audit 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 25 individuals, including the executive director, and is supported by the following functional areas:

- *Fiscal Support* – Supports end users with the fiscal applications.
- *Software Support* – Supports end users in a given area of concentration including the EMIS, library and student service 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 entity. Completion of a help desk ticket is required for all changes and the tickets 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 full-time staff member must attend at least 20 hours of approved professional development training annually, and part-time staff member training hours are prorated. 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 was performed on May 14, 2014

Risk Assessment

NEOnet does not have a formal risk management process; however, NEOnet's board of directors and the various 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 other user 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 entities. 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 Computer Control sections 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 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 entities are discussed within the General Computer Control sections.

GENERAL COMPUTER CONTROLS

Development and Implementation of New Applications and Systems

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 as needed to monitor SSDT projects and provide feedback on project priorities.

Changes to Existing Applications and Systems

End users have access to the SSDT website that contains user and technical documentation for the applications. Specific support issues or questions can be communicated to the SSDT via helpdesk software. Solutions are communicated directly to NEOnet staff. Global issues are posted to the SSDT support website.

NEOnet personnel do not perform program maintenance activities. Instead, they utilize the applications supplied to them by the SSDT. The OECN requires the ITC to keep the version of each application current based on the provider's standard for continued support. Procedures are in place to ensure the SSDT developed applications are used as distributed. Upon notification of their availability from SSDT, ITCs obtain quarterly updates by downloading zipped files from the SSDT's download site. The source code is not distributed with these files. Release notes, which explain the changes, enhancements and problems corrected, are provided via the SSDT website. User and system manager manuals are also made available via the SSDT website 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. As a participating member of the MCOECN, an ITC can enter into a cooperative agreement, "Campuswide Software License Grant (CSLG) and Education Software Library (ESL) Program", through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of Hewlett Packard (HP), and other supplier's, software packages as approved by the MCOECN board of trustees.

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

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

- Provide telephone technical support to the 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 and maintain support on one (1) license of Process Software's Multinet TCP/IP stack for each system registered under this program.

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

- Maintain its status as a member in good standing of the MCOECN as a qualification for participating in (or continuing to participate in) this program.
- Read, sign, and comply with the rules and regulations of the CSLG Program as operated by the MCOECN.
- Provide unrestricted privileged access to all computer systems covered under the agreement for the purposes of identifying and/or correcting problems, distributing software, or assuring licensing compliance.
- 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 MCOECN 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 entity personnel, NEOnet personnel, and any individual or group not belonging to the user entity 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 entities 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 fiscal software support specialist who then

creates the account and contacts the user regarding the newly established account. Authorization forms are maintained in the user entity's file. On an annual basis, user entities 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 software consultant, fiscal software support specialist, system administrator and assistant director/technical services manager. They are reviewed daily by the fiscal software support specialist. 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 on to NEOnet. At the local level, NEOnet uses two Barracuda servers to scan incoming e-mail from Iron Port 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. NEOnet also uses a MailMarshal server to scan inbound and outbound e-mail for SPAM.

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 entities 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 enter a correct 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. In addition, a timeout parameter for web sessions is used to log users off the system after a pre-determined period of inactivity.

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 entity, 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 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 the USAS, USPS and SAAS/EIS application data files.

User entities 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 entities of NEOnet. The firewall equipment denies all inbound 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 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 an electronic key system. Electronic keys to the computer room have been given to specific ITC staff authorized by management. 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 entities 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.

Data entry errors are mostly corrected by the user and are subject to the normal application controls. User problems, 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 fiscal software support specialist to verify processing was not interrupted. In addition, the user entities 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 staff over the phone and may not be documented. However, major problems are logged through a help desk ticket. 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 data is stored in the STORserver located at the MCOECN disaster recovery site, which is protected by fire detection equipment and video camera surveillance.

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 for seven years for all NEOnet user entities.

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.

COMPLEMENTARY USER ENTITY CONTROLS

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

General Computer Control Procedures

1. User entities should have controls over their own web applications that access their data stored at the ITC to ensure only thoroughly tested and authorized web applications are implemented.

2. User entity 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 entity management should immediately request the ITC to revoke the access privileges of user entity personnel when they leave or are otherwise terminated.

4. User entity personnel should respond to account confirmation requests from their ITC.

5. User entities 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 entities 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 entities should establish and enforce a formal data retention schedule with their ITC for the various application data files.

The complementary user entity controls presented above do not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at the user entity.

SECTION 4 - INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

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 entity'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 user entities 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 COMPUTER 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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
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 and SAAS/EIS 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
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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
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.	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:*
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.	Selected a sample of 22 user accounts from a population of 1,110 user accounts with audit significant identifiers and inspected the account authorization forms for appropriate authorization signatures.	No exceptions noted.
User access is confirmed annually with entity 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 entity.	Inspected documentation for the 2014 positive confirmation process for evidence of the following: • Verification forms and user listing showing audit significant identifiers. • Checklist used to track responses. Confirmed follow-up procedures with the payroll and accounts receivable officer and the fiscal services support specialist.	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:*
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. The command procedure is scheduled to run daily and is e-mailed to the following NEOnet staff: • Fiscal services software consultant. • Assistant director technical services. • Fiscal services support specialist. • System administrator.	Inspected the following information related to the security monitor report to confirm these reports are produced and available for review daily: • DECScheduler job parameters for the security monitor report. • Example of a security monitor report. • Command procedure used to generate the report. Independently confirmed the process for review of the security monitor report with the system administrator and the fiscal services support specialist.	No exceptions noted.
NEOnet's incoming e-mail is filtered through Ironport, two load balanced anti-virus and spam filtering servers, and anti-spam software running on the MailMarshal server to help protect against computer viruses and spam.	Inspected the following information, related to the spam and anti-virus firewalls and MailMarshal anti-spam software, to confirm e-mail messages are scanned for spam and viruses: • Barracuda spam firewall scanning definitions. • MailMarshal configuration screens and log of updates. Also inspected the Internet header text from an example e-mail to confirm the path of the e-mail from IronPort, to the Barracuda server, to the MailMarshall SMTP protocol server, and then to the e-mail server.	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:*
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. The OECN_RPC logical has been set to prevent users of the web applications from logging in with expired passwords.	Extracted information from the user authorization file to identify: • User accounts with a password length less than NEOnet standards. • User accounts with a password lifetime greater than NEOnet standards. Inspected the default account to confirm pre-expired parameters were set. Inspected the results of the extracted information and inquired with the fiscal services support specialist regarding the appropriateness of the accounts. Inspected the OECN_RPC logical to confirm the VMS process has been set to prevent logins with expired passwords.	Nine of the 1,330 (0.7%) enabled accounts on the system had a password length less than NEOnet's standards. These accounts consisted of the following: • Six system/application accounts. • Two training/demonstration accounts. • One OECN pass through account. There were no user accounts with a password length less than NEOnet's standards. There were 71 out of 1,330 (5%) enabled accounts on the system with a password lifetime greater than NEOnet's standards. These accounts consisted of the following: • Seven system/application accounts. • Forty-three process accounts used by a command procedure. They are not logged into by a user. • Eight OECN pass through accounts. • Two library accounts related to automatic processes. • Two state software support accounts. • Eight accounts used by the districts to validate accounts payable transactions. • One test account. There were no user accounts with a password lifetime greater than NEOnet's standards. No other 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.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameter settings.	No exceptions noted.
A timeout parameter provided through the OECN web access menu system logs off users after a period of inactivity.	Inspected the OECN web terminal log off parameters for the web based application systems to confirm NEOnet is logging off inactive web application users.	No exceptions noted.
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.	Inspected the HITMAN parameters (prime and non-prime) to confirm they were set to automatically logoff inactive users. Inspected the startup file to ensure the HITMAN utility is part of the startup process.	Two system accounts are protected from termination which prevents log off while installations and updates are being performed. Six NEOnet employee accounts are protected from termination while they are running processes. The HITMAN parameter setting for killing processes after a period of inactivity, has been set at an amount greater than suggested by best practices. No other 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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user entities.	Requested the network diagram to confirm components of the network that control Internet access. 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.	No exceptions noted.
NEOnet confirmed user entity firewall access for active IP addresses with user entities through a positive confirmation process. NEOnet tracks the status of the confirmation and performs any necessary follow-up communications to facilitate a response from the user entity.	Inspected the signed network security confirmations to confirm responses were received from all user entities with active IP addresses.	Seven out of 35 (20%) user entities with active IP addresses did not respond to the firewall confirmation request. They include the following: • Breakthrough Schools • Cloverleaf Local SD • Cuyahoga Falls CSD • Kent City SD • St. Augustine Schools • Summit County ESC • Woodridge Local SD No other exceptions noted.

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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Users are restricted to predefined logical access identifiers that grant varying access privileges based on requests from user management.	Extracted a listing of all identifiers from the user authorization file for evidence of the use of identifiers to segregate access to the audit significant applications. Confirmed the process of assigning application identifiers with the fiscal services support specialist.	No exceptions noted.
Users are only granted the level of access authorized by management to the USAS, USPS and SAAS/EIS application systems.	Selected a sample 22 accounts from a population of 1,110 active accounts with identifiers to the audit significant applications. Inspected the account authorization forms or annual confirmation to confirm the identifiers granted were authorized.	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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
WORLD access to “key” security and system 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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
System level UICs 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.	Identified the MAXSYSGROUP value. Extracted accounts from the user authorization file to identify accounts with a UIC less than the MAXSYSGROUP value. Inspected the listing and inquired with the fiscal services support specialist regarding the appropriateness of the accounts.	No exceptions noted.
Accounts on the system with ELEVATED privileges, defined as those accounts having more than the minimum privileges to use the system or participate in groups, is limited to authorized personnel as determined by NEOnet management.	Extracted accounts from the user authorization file to identify accounts with elevated privileges. Inspected the listing and inquired with the fiscal services support specialist regarding the appropriateness of the accounts.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized NEOnet management.	Extracted accounts from the user authorization file with the OECN_SYSMAN identifier. Inspected the listing and inquired with the fiscal services support specialist regarding the appropriateness of the accounts.	No exceptions noted.
Use of an alternate user authorization file is not permitted.	Inspected the value of the user authorization alternate parameter to determine whether an alternate file is permitted. Inspected the system directory listing to determine if an alternate user authorization file existed.	No exceptions noted.
Remote administration to the firewall configuration used to control Internet access is restricted through password protection.	Inspected the firewall configuration to confirm that a password is required and remote access is restricted.	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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Access to manage the virtual servers is restricted to authorized NEOnet personnel as determined by NEOnet management.	Inspected the listing of users with administrative access to VCenter, the virtual server administrative software. Inspected the local VCenter server group listing for membership of the administrator group. Confirmed the appropriateness of access with the technical support specialist.	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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Physical access to the computer room and its contents is restricted to authorized personnel as determined by NEOnet management.	Inspected the electronic keypad and security system to confirm physical access to the computer room is controlled. Observed the presence of security cameras outside the computer room. Inspected the security card access control list to confirm access to the computer room is restricted to authorized personnel. Discussed access to the computer room with the assistant director technical services and technical support specialist.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, water, power fluctuations, 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 that the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Requests for changes to user entity data are documented on help desk tickets.	Confirmed the procedures for changing user data with the fiscal services support specialists. Inspected an audit report (AUDRPT) for a user entity for changes made by NEOnet staff. Verified a help desk ticket was available requesting the change.	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 Gold, 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. Inspected notifications in the technical support specialist's inbox and cell phone.	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***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Backups of programs and data are performed daily.	Inspected the batch queue listing and the command file for the Archive Backup Client (ABC) for Open VMS to confirm the backup job was scheduled to run daily. Inspected an example of the backup notification that is e-mailed to the assistant director/technical services, senior systems administrator, fiscal services support specialist, and system administrator. Inspected follow-up procedures with the fiscal services support specialist.	No exceptions noted.
Backup data is stored at a secure off-site location. On a daily basis, data is pushed, on-line, to an off-site StorServer appliance.	Inspected the backup log to confirm the on-line backup process to the off-site StorServer appliance.	No exceptions noted.

SECTION 5 - 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:	Sam Reynolds Superintendent Manchester Local Schools
Fiscal Agent:	Metropolitan Regional Service Council (MRSC)
Administrator:	Matthew Gdovin Executive Director NEOnet
Address:	700 Graham Road Cuyahoga Falls, OH 44221
Telephone:	330-926-3900
FAX:	330-926-3901
Web site:	https://www.neonet.org

OTHER SITE STAFF

Teresa Bichsel	Fiscal services support specialist
R. Wayne Bowers	Fiscal officer
Savannah Buck	Fiscal services support specialist (started 4/14/2014)
Ben Claussen	Technical support specialist (started 3/5/2014)
Jennifer Cottrill	Coordinator of software services
Mary Dolis	EMIS support specialist
Cyrus Elder	System administrator
Victoria Estes	Fiscal services support specialist (left 3/25/2014)
Kim Fassnacht	Payroll and accounts receivable officer
Michele Fulton	Student services support specialist
Paulette Gansel	Fiscal services software consultant – part time
Benjamin Heller	Technical support specialist
Michael Hoffman	Application developer
Denise Marrali	Student services support specialist
Jim Martin	Business manager
Lisa Nash	Fiscal services support specialist
Kathy Peters	Student services support specialist
Marie Schmidt	Technical support specialist
Jeanne Steele	Media services support specialist
Tim Tracy	Senior systems administrator
Amy Vargo	District payroll specialist (started 7/1/2013)
Catherine Wright	EMIS support specialist
Brendon Yarian	Database and application support specialist
Genne Zimmerly	District EMIS specialist (started 8/15/2013)
Christopher Zolla	Assistant director technical services

HARDWARE DATA

Central Processors and Peripheral Equipment

Model Number		Installed		Capacity/Density/Speed	
CPU:	ES45	Lines/Ports:	N/A	Memory Installed:	16.0 GB
Disk:	DSA0	Units:	1	Total Capacity:	67.82 GB
Disk:	1DKC0	Units:	7	Total Capacity:	135.72 GB
Disk:	1DKC1	Units:	5	Total Capacity:	135.72 GB
Disk:	1DKC2	Units:	5	Total Capacity:	135.72 GB
Disk:	1DKC3	Units:	1	Total Capacity:	135.72 GB

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS/EIS	OTHER*
043794	Cleveland Heights/University Heights City School District	Cuyahoga	X	X		
046557	Cuyahoga Heights Local School District	Cuyahoga	X	X	X	
044305	Maple Heights City School District	Cuyahoga	X	X	X	
044636	Parma City School District	Cuyahoga	X	X		
046599	Richmond Heights Local School District	Cuyahoga	X	X	X	
045492	Mentor City School District	Lake		X		
043661	Brunswick City Schools	Medina				X
048470	Buckeye Local School District	Medina	X	X	X	
048488	Cloverleaf Local School District	Medina	X	X	X	
062109	Medina County Career Center	Medina	X	X	X	
048454	Medina County Educational Service Center	Medina	X	X		
044164	Kent City School District	Portage	X	X	X	
051391	Maplewood Career Center JVSD	Portage	X	X	X	
149054	Akron Digital Academy	Summit	X[(a)]			
043539	Barberton City School District	Summit	X	X	X	
049981	Copley-Fairlawn City School District	Summit	X	X	X	
049999	Coventry Local School District	Summit	X	X	X	
043836	Cuyahoga Falls City School District	Summit	X	X	X	
147231	Schnee Learning Center (Cuyahoga Falls Digital Academy)	Summit	X			
011381	Greater Summit Early Learning Center	Summit	X	X	X	
050013	Green Local School District	Summit	X	X	X	
050021	Hudson City Schools	Summit				X
050005	Manchester Local School District	Summit	X	X	X	
050039	Mogadore Local School District	Summit	X	X	X	

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS/EIS	OTHER*
050047	Nordonia Hills City School District	Summit	X	X	X	
044552	Norton City School District	Summit	X	X	X	
063495	Portage Lakes Career Center	Summit	X	X	X	
050054	Revere Local School District	Summit	X	X	X	
050062	Springfield Local School District	Summit	X	X	X	
044834	Stow-Munroe Falls City School District	Summit	X	X	X	
132779	Summit Academy	Summit			X	
049965	Summit County Educational Service Center	Summit	X	X	X	
044883	Tallmadge City School District	Summit	X	X	X	
050070	Twinsburg City School District	Summit	X	X	X	
049973	Woodridge Local School District	Summit	X	X	X	
TOTALS:			**32**	**30**	**27**	**2**

* OTHER – Applications other than USAS, USPS, and SAAS/EIS, used by the user entities.

[(a)] NEOnet ended service to Akron Digital Academy. All accounts were DISUSERed in June 2013.

This page intentionally left blank.

Dave Yost • 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 9, 2014

88 East Broad Street, Fourth Floor, Columbus, Ohio 43215-3506
Phone: 614-466-4514 or 800-282-0370 Fax: 614-466-4490
www.ohioauditor.gov