LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION/NORTH COAST COUNCIL (LNOCA/NCC)

STATE REGION - ISA, CUYAHOGA COUNTY

SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

APRIL 1, 2011 THROUGH MARCH 31, 2012

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
Lakeshore Northeast Ohio Computer Association/North Coast Council (LNOCA/NCC)
5700 West Canal Road
Valley View, OH 44125

To Members of the Board:

Scope
We have examined LNOCA/NCC's accompanying Description of its Alpha GS80 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, 2011 to March 31, 2012 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 LNOCA/NCC'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 LNOCA/NCC 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 LNOCA/NCC 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, LNOCA/NCC 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. LNOCA/NCC 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, 2011 to March 31, 2012.

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 LNOCA/NCC to provide additional information and is not part of the LNOCA/NCC'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 LNOCA/NCC's Assertion in section 2,

a. the Description fairly presents the system that was designed and implemented throughout the period April 1, 2011 to March 31, 2012.

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, 2011 to March 31, 2012 and user entities applied the complementary user entity controls contemplated in the design of the LNOCA/NCC's controls throughout the period April 1, 2011 to March 31, 2012.

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, 2011 to March 31, 2012.

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 LNOCA/NCC, user entities of LNOCA/NCC's system during some or all of the period April 1, 2011 to March 31, 2012, 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

July 13, 2012

This Page Intentionally Left Blank

NORTH COAST COUNCIL
Connecting You with Technology

We have prepared the description of the Lakeshore Northeast Ohio Computer Association/North Coast Council (LNOCA/NCC) Alpha GS80 system (Description) for user entities of the system during some or all of the period April 1, 2011 to March 31, 2012, 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 Alpha GS80 (System) made available to user entities of the System during some or all of the period April 1, 2011 to March 31, 2012 for processing their transactions. The LNOCA/NCC 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 LNOCA/NCC 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.

5700 West Canal Road ❙ Valley View, Ohio 44125 ❙ 216.520.6900 ❙ Fax 216.520.6969
1885 Lake Avenue ❙ Elyria, Ohio 44035 ❙ 440.324.3185 ❙ Fax 440.324.6140
nccohio.org

b) the Description includes relevant details of changes to the service organization's System during the period from April 1, 2011 to March 31, 2012.

c) the controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period April 1, 2011 to March 31, 2012 to achieve those control objectives and subservice organizations applied the controls contemplated in the design of LNOCA/NCC 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.

John Mitchell
Executive Director
July 13, 2012

SECTION 3 – DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

The LNOCA/NCC'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 the LNOCA/NCC's description of controls.

OVERVIEW OF OPERATIONS

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

ITCs provide information technology services to school districts, community 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. The LNOCA/NCC is organized as a COG under ORC chapter 167 and is a subsidiary of the LNOCA/NCC. The governing board of the Educational Service Center of Cuyahoga County (ESCCC) serves as the fiscal agent for the LNOCA/NCC and performs certain functions that might otherwise be performed by the council.

LNOCA/NCC entered into a Cooperative Service Agreement on August 1, 2011 with the Lake Erie Educational Computer Association (LEECA), a neighboring ITC within the Ohio Education Computer Network. The intent of the agreement is to combine and create one organization with greater operating efficiency and a diversified customer base.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

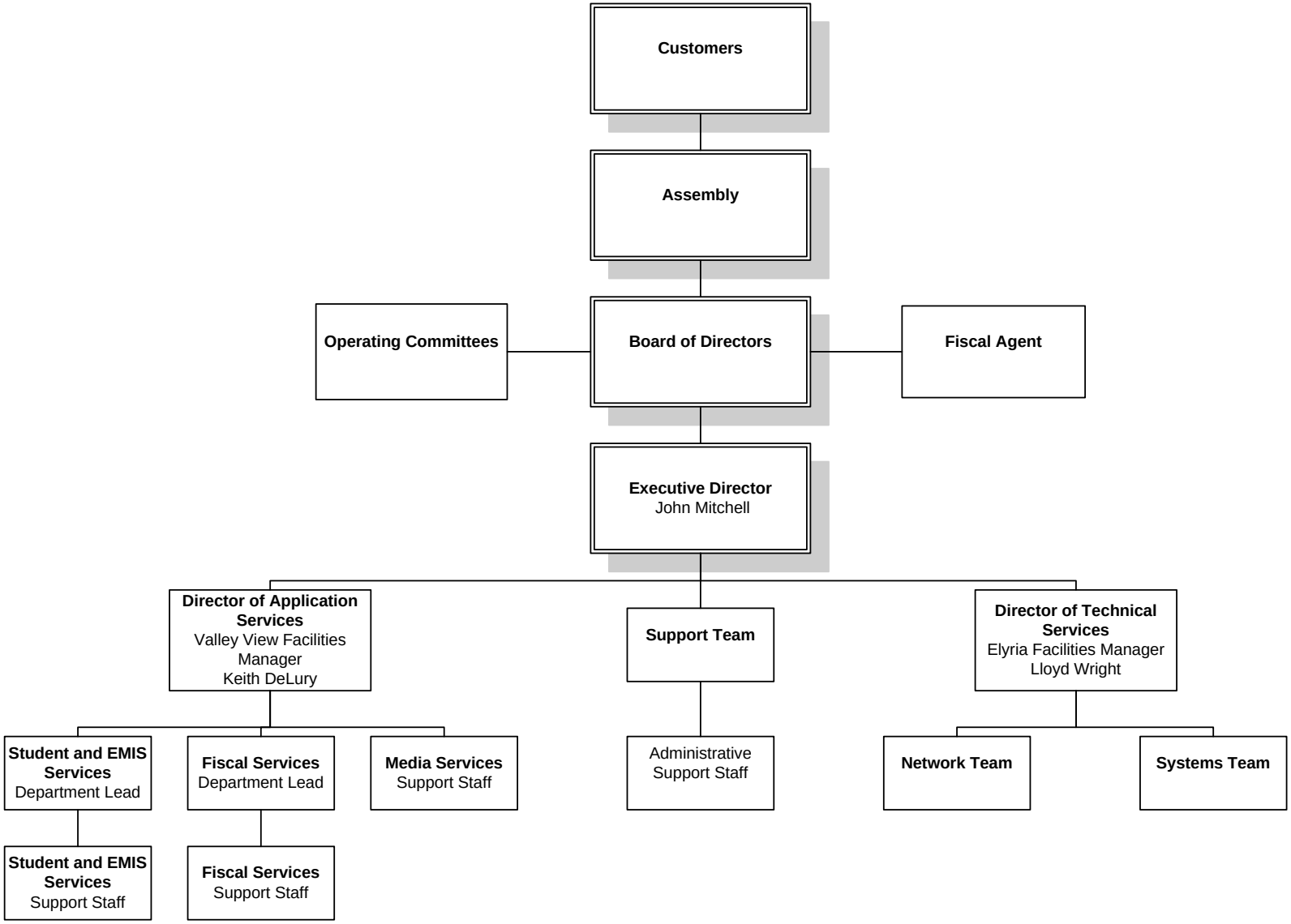
Operations are under the control of the executive director and the board of directors. Each member entity appoints a representative to the legislative body, which is the assembly. The board meets quarterly to estimate program costs, approve annual appropriations, select officers and other members of the board of directors and approve other matters. The board has also established an advisory committee to assist in the operation of the LNOCA/NCC and its programs.

The LNOCA/NCC employs a staff of 16 individuals, including the executive director, and is supported by the following functional areas:

Student Systems:	Supports end users in all aspects of the student service applications with a focus on EMIS.
Fiscal Systems:	Provides training and end user support for the state software applications, including USAS, USPS, and SAAS/EIS.
Library Systems:	Provides a variety of educational technology services and training to subscribing LNOCA/NCC user entities including use of guidance applications, INFOhio, and online resources.
Systems and Network:	Supports the LNOCA/NCC computer systems and its networked communication system. Provides user training and support.
Applications Systems:	Provides technical software support to LNOCA/NCC staff and clients.

The lead support specialists and the support specialists report to the assistant director or the executive director as appropriate. The assistant director reports to the executive director.

The merger to form the North Coast Council (NCC) became effective on July 1, 2012. In anticipation of that merger, LNOCA/NCC implemented the following operational reporting structure of the new North Coast Council.



Users are responsible for the authorization and initiation of all transactions. Management reinforces this segregation of duties through training and by restricting employee access to user data. Changes to user data are infrequent. Only experienced LNOCA/NCC employees may alter user data and only at the request of the user entity. Completion of a LNOCA/NCC intervention form and/or a help desk ticket is required for all changes to user entity data. The forms and tickets are periodically reviewed by the support specialist application systems.

The LNOCA/NCC personnel policies and procedures are available to all employees. When necessary, additional LNOCA/NCC policies have been developed to address concerns of LNOCA/NCC. Detailed job descriptions exist for all positions. The LNOCA/NCC 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 LNOCA/NCC'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 LNOCA/NCC 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 training annually, and training hours for part-time members are pro-rated. Employee evaluations are conducted annually.

LNOCA/NCC 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. LNOCA/NCC's site review was conducted in September 2008.

Risk Assessment

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

- New technology.
- Realignment of the LNOCA/NCC organization to provide better service.
- Personnel issues, including hiring, termination, and evaluations.
- Additional services provided to the user entities 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 LNOCA/NCC has identified operational risks resulting from the nature of the services provided to the 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 EDP Control" section of this report.

Monitoring

The LNOCA/NCC organization is structured so lead support specialists and the support specialists report to the executive or assistant director. The LNOCA/NCC 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 the user entities are discussed within the general EDP control sections.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

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

Changes to Existing Applications and Systems

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

The LNOCA/NCC personnel do not perform program maintenance activities. Instead, they use applications supplied by the SSDT. The OECN requires the ITC to keep the version of each application current based on the provider's standard for continued support. Procedures are in place to ensure the SSDT developed applications are used as distributed. Upon notification of their availability from the 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.

The LNOCA/NCC 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.

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 the LNOCA/NCC, 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 LNOCA/NCC has purchased a copy of the operating system disks from INS, a third-party vendor in partnership with the MCOECN. This is part of the Technology Solutions Group program under the MCOECN (mc•tsg). The LNOCA/NCC is able to purchase the operating system software at a reduced cost under this program.

IT Security

The LNOCA/NCC has a security policy outlining the responsibilities of user entity personnel, the LNOCA/NCC personnel, and any individual or group not belonging to the user entity or the LNOCA/NCC. In addition to the security policy, the LNOCA/NCC uses a banner screen that is 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 the computer system are subject to having their activities monitored by the LNOCA/NCC personnel. The LNOCA/NCC staff members are granted access within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities. Access is established, granted and reviewed by management.

User entity personnel are granted access upon the receipt of a system authorization form from the superintendent and/or treasurer. LNOCA/NCC staff members create, update, or delete the account and e-mail the appropriate user entity designee regarding the request made. At the fall advisory committee meeting or treasurers' meeting, LNOCA/NCC distributes a listing, which lists each user account and the privileges granted

within each user entity. User entities are responsible for reviewing the list, notifying LNOCA/NCC of any account changes, and returning the user verification form.

Access to the Internet has been provided to the user entities of the LNOCA/NCC. LNOCA/NCC has an Internet policy. Requests for an Internet e-mail account must be completed by the user and are sent to the user entity's technology coordinator who sets up the account. Internet account request forms are maintained by the user entity.

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 can be written to a log file for later examination. The following security alarms and/or security audits have been enabled through OpenVMS to monitor any security violations on the LNOCA/NCC 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 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 executive director and are reviewed daily. If an event is deemed suspicious, it is investigated further to determine the exact nature of the event and the corrective action needed.

The LNOCA/NCC uses Sophos anti-virus software, which distributes updates daily to PCs and servers.

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. The LNOCA/NCC does not use proxy logins.

The user identification codes (UIC) are individually assigned to all accounts. 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 object run, 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 LNOCA/NCC 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, and/or CAPTIVE flags.

The system forces users to change their passwords on a periodic basis. Student services accounts were set up so the password change interval corresponds with the school year. These accounts do not affect financially significant functions and are not able to access financial applications. All fiscal services accounts have a shorter password lifetime. Users are instructed to change the initial password provided when a new user identification code is issued or when a user has forgotten his password.

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.

System parameter standards have been established through the use of HP established defaults. Any changes are logged and reviewed by the support specialist application systems.

A timeout program, HITMAN, is used to monitor terminal inactivity and log-off inactive users after a predetermined period of inactivity. In addition, a web session timeout parameter is used to log users off after a pre-determined amount of inactivity. The use of this program helps to reduce the risk

of an unattended terminal being used to enter unauthorized transactions. In addition, timeout programs aid in efficient use of system resources by maintaining connectivity with only active system users.

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

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

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

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

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

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

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

Certain privileges can override all UIC-based and ACL protection. OpenVMS analyzes privileges included in the user authorization file (UAF) record for each user and places the user in one of seven categories depending upon which privileges have been granted to the user. Default privileges are those authorized privileges that are automatically granted at login. If an authorized privilege is not a default privilege, it will not automatically be effective at login and must be enabled or disabled by the user. All user entity personnel have NORMAL privileges.

The write and delete access capabilities are not activated for WORLD access to the files in the system directory. The UIC associated with each of these files is within the MAXSYSGROUP number.

To limit access to security files, the LNOCA/NCC 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 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 internal network. A firewall has been placed between the Internet access provided by the OECN network and the internal network of the user entities of the LNOCA/NCC. The firewall denies all inbound traffic requests unless they originated from the internal network. Instead, the requests are routed through the firewall where it performs the function of a proxy server and acts as an intermediary between the Internet and internal network. Periodically, alterations to the firewall configuration are necessary to allow for the use of specific software or internet services. These changes are requested by user entity technical staff, and are documented in the help desk software. In addition, LNOCA/NCC confirms firewall configuration settings with their user entities annually.

LNOCA/NCC also makes available an Internet content filter. The filter is an optional service that screens Internet site requests for unsuitable content.

The LNOCA/NCC is in a self contained building which is secured by a key lock. All doors are locked during off hours. During daytime hours the main door is unlocked; however, LNOCA/NCC personnel are present at all times. The computer room remains locked at all times and is secured by a lock. The keys are held by the data processing staff.

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

- Raised flooring.
- Power conditioner.
- UPS backup power supply (20 minutes).
- Natural gas generator and a diesel fuel generator.
- Temperature/humidity control.
- Water sensors.
- Heat and smoke detectors.
- Fire extinguishers.

IT Operations

Traditional computer operations procedures are minimal because user entity personnel initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. A general staff procedure manual and department manuals provide directions and guidelines for most of the operational functions performed. The LNOCA/NCC staff also has access to operations procedure manuals for the Alpha system. In addition, all users have access to SiteScape Forum, which is a bulletin board that allows them to communicate with users across the state.

User problems that require the LNOCA/NCC staff to change data require the completion of an intervention form and/or entry of a help desk ticket. These forms and tickets are periodically reviewed by the assistant director. In addition, the user entities have the option of printing an "AUDIT" report that shows most activity changes to their data files.

Data restoration or downloading of data from tapes can be performed by all LNOCA/NCC staff. Any error reports (failure of batch jobs) or system status reports (disk space remaining reports or successful backup reports) are monitored in the morning by reviewing the console log. Common problems that arise daily, such as terminal lockups and program crashes, are usually handled by the LNOCA/NCC service representatives over the phone. Critical problems from the operator log, such as logon failures and system failures, are sent daily via e-mail to the executive director and assistant director. Hardware problems, which cannot be handled by the LNOCA/NCC staff technicians, are referred to Service Express. LNOCA/NCC has a hardware maintenance agreement with Service Express. The agreement provides for on-site service Monday through Friday during the business hours of 8am to 5pm.

Certain routine jobs are initiated for system maintenance. LNOCA/NCC is responsible for operational maintenance tasks, such as system backups, log reports, and other maintenance directed at the whole system. They use an automated application called SUBMITALL to schedule and perform these tasks. SUBMITALL is a command procedure that is run each morning to schedule that day's tasks.

IBM Tivoli Storage Manager (TSM) is used to schedule and maintain server backup and recovery. Daily incremental backups on the Alpha server are performed automatically. Completion of the backups is documented on a log. Incremental backup cartridges are stored in a robotic tape silo. TSM is configured to help ensure that any file or all files can be restored to any date/time within 90 days.

TSM maintains each data file in storage for 45 days if the storage file has been updated. If the data file in storage does not have an update within 45 days, TSM will store the file indefinitely until an update is received. If a storage file is deleted from production, TSM will maintain the file for 90 days.

TSM backup tapes are also rotated offsite. Backup tapes, which contain any changes from the prior backup, are rotated to the offsite facility on a daily basis. These daily tapes, along with the other backup tapes stored off-site, are required to restore the system to the point of the last daily backup. The tapes are rotated to an off-site facility located across the street from LNOCA/NCC.

TSM is used to schedule and maintain server backup and recovery that is uploaded to the State DR site located in Columbus, Ohio on a nightly basis. Daily incremental backups on the Alpha server are performed automatically. Completion of the backups is documented on a log. A DR inventory plan is generated at the completion of each successful back up.

LNOCA/NCC's 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 EDP Control Procedures

1. User entities should have controls over their own web applications which 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 ITC security policies 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. User entity technical staff should respond to requests for confirmation of firewall conduit statements from their ITC.

7. Access privileges should only be issued to authorized users who need access to computer resources to perform their job function.

8. 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.

9. Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.

10. User entities should retain 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.

11. 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 LNOCA/NCC'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 LNOCA/NCC and procedures performed at user entities that utilize the LNOCA/NCC.

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

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Changes to Existing Applications and Systems

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
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 the LNOCA/NCC was compared to the CRCs of the object files at NWOCA.	The CRCs did not match for one file. This file is commonly modified to customize purchase order forms. No other 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 operating system and new releases 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:*
LNOCA/NCC has established a data system security policy addressing responsibilities of user entity personnel, ITC personnel, and individuals or groups not belonging to the user entity or LNOCA/NCC.	Inspected the data system security policy to confirm user responsibilities are documented.	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:*
Authorization from user entity management is required before setting up a user account on the system. Access to financial data requires authorization from the treasurer. All other access requires authorization from the superintendent.	Identified all active accounts having identifiers granting access to the audit significant applications. Selected a sample of 22 accounts from a population of 91 new users. Inspected the user authorization forms to confirm the required signatures were present.	No exceptions noted.
User access is confirmed annually with user entity management through a positive confirmation process. LNOCA/NCC tracks the status of the confirmation and follows-up with a reminder message to facilitate a response from the user entity.	Inspected the September 2011 annual confirmation checklists to confirm all user entities confirmed their access with the LNOCA/NCC.	One user entity, Quest Community School, was in the process of joining LNOCA/NCC at the time of the September 2011 confirmation. Therefore, they were not included in the 2011 confirmation of user accounts. However, they have been included on the most recent confirmation occurring in May 2012. No other exceptions noted.
Detection control alarms are enabled through Open VMS 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 security monitor report is generated daily and is e-mailed to the executive director, assistant director and support specialist application systems.	Inspected the following information relating to the security monitor report to confirm these reports are produced and available for review: • Command procedure used to generate the report. • An example security monitor report. • E-mail directory listing of security monitor reports received by the executive director. Confirmed the procedures for reviewing the security monitor report with the executive director.	No exceptions noted.
Anti-virus software is installed on LNOCA/NCC servers and user terminals. Definitions are updated daily and infected items are quarantined to help prevent and detect computer viruses.	Inspected the Sophos definitions to confirm anti-virus software is actively scanning for viruses. Inspected the following items: • Sophos enterprise console. • Sophos update properties. • On-line access for PCs. • Network computers update schedule. • Virus Scans.	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 parameters are in place to aid in the authentication of user access to the production system. Passwords used by individual profiles are in agreement with the password policies established by the LNOCA/NCC. 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 minimum length less than LNOCA/NCC's standards. • User accounts with a password lifetime greater than LNOCA/NCC's standards. Inspected the above exception reports and inquired with the assistant director to identify exceptions. Obtained and inspected the printout of the OECN_RPC logical from the assistant director to determine whether the VMS process has been set to prevent logins with expired passwords.	There were 105 accounts out of 751 active accounts with a password lifetime greater than LNOCA/NCC's standard. These accounts are system and application accounts whose password cannot expire. There were no user accounts with a password lifetime greater than LNOCA/NCC's standard. No other 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 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 start up file to confirm the HITMAN utility is part of the startup process.	Inactive users are not logged off until after 60 minutes of inactivity. No other exceptions noted.
A timeout parameter provided through the OECN web access menu system logs users off after a period of inactivity.	Inspected the OECN web terminal log off parameters for the audit significant web applications to confirm LNOCA/NCC is automatically logging off inactive web application users.	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:*
Access to production programs and data files is properly restricted.	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.
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user entities.	Inspected the network diagrams to confirm components of the network that control Internet access. Inspected the firewall configuration to confirm a private internal network is used and that Internet traffic is restricted through the firewall.	No exceptions noted.
Network security information (conduit statements) is confirmed with each user entity on an annual basis by LNOCA/NCC. The confirmations are to be signed by the technical coordinator or their designee.	Inspected the file of firewall confirmation sign-offs and compared it to the firewall configuration spreadsheet maintained by the support specialist networks.	The following member user entities have not responded to the firewall confirmation: • Brooklyn City School District • Harvard Avenue Community School • Lakewood City School District No other exceptions noted.
Modifications to the firewall are requested through the help desk software.	Observed requests for modifications to the firewall entered into the help desk software during the audit period. Inspected two examples of the detail included in the help desk ticket for authorization and documentation of access granted.	No exceptions noted.
The LNOCA/NCC does not use proxy logins for remote access.	Inspected the network proxy listing to confirm there were no proxy logins in existence.	No 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 pre-defined logical access identifiers that grant varying access privileges based on request 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 applications. Inquired with the support specialist fiscal systems regarding the OSA utility and the process used to assign application identifiers.	No exceptions noted.
Authorization from appropriate user entity management is required before granting access.	Selected a sample of 22 accounts from a population of 91 new user accounts with identifiers to the audit significant applications. Inspected the account request forms 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” system files is restricted.	Identified system files with WORLD write and/or delete access. Inspected the file protection masks on the security files to confirm WORLD access was absent.	One file was found to have WORLD access equal to write and delete. This file was a backup log file for the STORServer. The file was subsequently moved to another directory with supporting documentation provided. No other 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 as determined by LNOCA/NCC management. 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 listings and inquired with the support specialist application systems regarding the appropriateness of the listed 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 LNOCA/NCC management.	Extracted accounts from the user authorization file to identify accounts with elevated privileges. Inspected the listings and inquired with the support specialist application systems regarding the appropriateness of the listed accounts.	No exceptions noted.
Use of an alternate user authorization file is not permitted.	Inspected the value of the alternate user authorization parameter to determine whether an alternate file is permitted. Inspected the system directory listings to determine if an alternate user authorization file existed.	No exceptions noted.
Remote access to the firewall configuration used to control Internet access is restricted through password protection.	Inspected the firewall configuration to confirm passwords were enabled.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized ITC personnel as determined by LNOCA/NCC management.	Extracted accounts from the user authorization file with the OECN_SYSMAN identifier. Inquired with the assistant director regarding the appropriateness of the listed accounts.	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.	Inspected the key lock and security system to confirm physical access to computer equipment is controlled. Observed employee monitoring of the site during fieldwork.	No exceptions noted
Environmental controls are in place to protect against and/or detect fire, water, humidity, or changes in temperature.	Inspected the computer room 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:*
Internally developed operations instructions and procedures are stored in a central directory, which is available to LNOCA/NCC staff members.	Inspected the LNOCA/NCC procedure binder for existence. Inspected example instructions for content.	No exceptions noted.
The LNOCA/NCC performs certain routine jobs for system maintenance through a scheduling procedure called SUBMITALL.	Inspected the SUBMITALL.dat file for a listing of all jobs scheduled to run on a daily basis. Inspected the SUBMITALL.com file to confirm the SUBMITALL.dat file is initialized daily.	No exceptions noted.
Technical support and maintenance of the computer hardware at LNOCA/NCC is covered by a service agreement with Service Express.	Inspected the Service Express payment documentation for inclusion of the Alpha, period of coverage, and evidence of payment for the audit period.	No exceptions noted.

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:*
A help desk ticket is prepared by LNOCA/NCC staff for requests for changes to user entity data files. The printed help desk tickets are maintained in the user entity's file.	Using a filter in the help desk software, filtered on USAS and USPS for evidence of intervention tickets and support occurring within the audit period. Inspected the hardcopy files for each user entity and confirmed support for changes was on file. Confirmed with the assistant director the roles of the technical and software support staff.	No exceptions noted.
All data center equipment is covered by insurance.	Inspected the insurance policy and payment documentation for evidence of coverage.	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 regularly. Scheduling of the backup procedures is automatically performed each time the backup script is run.	Confirmed the backup file transfer process with the assistant director and the support specialist networks. Inspected the local STORServer backup command script to confirm the local backup script is scheduled to run each night. Inspected the ODE disaster recovery STORServer backup command script and logs to confirm that file transfers to the state disaster recovery site occur nightly.	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:*
Backup tapes are stored in a secure on-site location and are rotated off-site regularly. A second backup file is sent to the mc•tsg disaster recovery site daily.	Inspected the on-site and off-site storage locations for evidence of tape maintenance. Confirmed the backup file transfer process with the assistant director and the support specialist networks. Inspected the State DR STORServer backup command script to confirm the script is scheduled to run each night.	No exceptions noted.

SECTION 5 - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name:	Lakeshore Northeast Ohio Computer Association/North Coast Council (LNOCA/NCC)
Number:	26
Node Name:	LNOCA/NCC
Chairperson:	Dr. Nancy Wingenbach Superintendent Orange City Schools
Fiscal Agent:	Educational Service Center of Cuyahoga County
Administrator:	John Mitchell Executive Director LNOCA/NCC
Address:	5700 West Canal Road Valley View, OH 44125
Telephone:	216-520-6900
FAX:	216-520-6969
Web site:	www.lnoca.org / www.nccohio.org

OTHER SITE STAFF

Sharon Koski	Administrative assistant
Keith DeLury	Assistant director
Jeff Opincar	Support specialist networks
Ricky Bouyer	Support specialist networks
Deb Carroll	Lead support specialist fiscal systems
Joe Kay	Support specialist fiscal systems
Connie Enders	Support specialist fiscal systems
Curtis Vigg	Support specialist application systems
Steven Foster	Support analyst application systems
Marilyn Deyling	Lead support specialist student systems
Jim Holesovsky	Support specialist student systems
Matt Zenobi	Support analyst application systems
Greg Perciak	Support specialist library systems
Lori Singerland	Support specialist library systems
Noreen Lehmann	Support specialist library systems

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	Compaq Alpha Server GS80	Lines/Ports:	N/A	Memory Installed:	6.0 GB
Disk:	RZ29	Units:	10	Total Capacity:	54 GB
Disk:	RA8000	Units:	1	Total Capacity:	306.0 GB
Tape Unit:	9 Track	Units:	1	Max Density:	6250 BPI
Tape Unit:	8 mm	Units:	1	Max Density:	8 mm
Tape Unit:	DAT	Units:	1	Max Density:	20 GB
Tape Unit:	TL891	Units:	1	Max Density:	N/A
Printers:	Tally-MT	Units:	1	Print Speed:	800 LPM

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS/EIS	OTHER*
043562	Bedford City SD	Cuyahoga	X	X		X
043612	Berea City SD	Cuyahoga				X
043646	Brecksville-Broadview Heights City SD	Cuyahoga	X	X		X
043653	Brooklyn City SD	Cuyahoga	X		X	X
043794	Cleveland Heights/University Heights SD	Cuyahoga				X
012010	Cleveland Ohio College Preparatory	Cuyahoga	X			X
050922	Cuyahoga Valley Career Center	Cuyahoga	X	X		X
043901	East Cleveland City SD	Cuyahoga	X	X		X
046532	Educational Service Center of Cuyahoga County	Cuyahoga	X	X		X
008067	Elite Academy of the Arts	Cuyahoga		X		X
044040	Garfield Heights City SD	Cuyahoga	X	X	X	X
008286	Harvard Avenue Community School	Cuyahoga	X	X		X
010005	Horizon Science Academy Cleveland ES	Cuyahoga				X
000838	Horizon Science Denison MS	Cuyahoga				X
010007	Horizon Science Denison ES	Cuyahoga				X
000858	Horizon Science Academy Cleveland MS	Cuyahoga				X
133629	Horizon Science Academy Cleveland	Cuyahoga				X
011533	Horizon Science Academy Lorain	Cuyahoga	X			X
046565	Independence Local SD	Cuyahoga	X	X		X
000942	Lakewood City Academy	Cuyahoga	X	X	X	X
044198	Lakewood City SD	Cuyahoga	X	X	X	X
143461	Marcus Garvey Academy	Cuyahoga				X
044370	Mayfield City SD	Cuyahoga				X

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS/EIS	OTHER*
008278	Noble Academy-Cleveland	Cuyahoga				X
011923	Northeast Ohio College Prep	Cuyahoga	X			X
044545	North Royalton City SD	Cuyahoga	X	X		X
125203	Ohio Schools Council	Cuyahoga	X			
046581	Orange City SD	Cuyahoga	X	X		X
000736	Phoenix Village Academy P2-Hough	Cuyahoga				X
000738	Phoenix Village Academy S1 Warrensville	Cuyahoga				X
050948	Polaris Career Center	Cuyahoga	X	X	X	X
000936	Promise Academy	Cuyahoga	X	X		X
012078	Quest Community School	Cuyahoga	X	X		X
044701	Rocky River City SD	Cuyahoga	X	X		X
044750	Shaker Heights City SD	Cuyahoga	X	X		X
046607	Solon City SD	Cuyahoga				X
044792	South Euclid-Lyndhurst City SD	Cuyahoga	X	X		X
045492	Mentor EVSD	Lake				X
011986	Horizon Academy-Youngstown	Mahoning				X
TOTALS:			**23**	**19**	**5**	**38**

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

Dave Yost • Auditor of State

LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION/NORTH COAST COUNCIL (LNOCA/NCC)

CUYAHOGA 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 21, 2012

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