



**NORTHERN OHIO EDUCATIONAL COMPUTER ASSOCIATION (NOECA)  
STATE REGION - ISA, ERIE COUNTY**

**SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)**

**APRIL 1, 2011 THROUGH MARCH 31, 2012**



**Dave Yost • Auditor of State**



**TABLE OF CONTENTS**

<b>1</b>	<b>INDEPENDENT SERVICE AUDITOR'S REPORT</b> .....	<b>1</b>
<b>2</b>	<b>SERVICE ORGANIZATION'S ASSERTION</b> .....	<b>5</b>
<b>3</b>	<b>DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM</b> .....	<b>7</b>
	CONTROL OBJECTIVES AND RELATED CONTROLS .....	7
	OVERVIEW OF OPERATIONS .....	7
	RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING .....	8
	Control Environment .....	8
	Risk Assessment .....	10
	Monitoring .....	10
	INFORMATION AND COMMUNICATION .....	10
	GENERAL EDP CONTROLS .....	11
	Development and Implementation of New Applications or Systems .....	11
	Changes to Existing Applications or Systems .....	11
	IT Security .....	12
	IT Operations .....	17
	COMPLEMENTARY USER ENTITY CONTROLS .....	18
<b>4</b>	<b>INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS</b> .....	<b>19</b>
	GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS .....	20
	Changes to Existing Applications and/or Systems .....	20
	IT Security .....	21
	IT Operations .....	28
<b>5</b>	<b>OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION (<i>Unaudited</i>)</b> .....	<b>30</b>
	Information Technology Center Profile .....	30

**This Page Intentionally Left Blank**



# Dave Yost • Auditor of State

## **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  
Northern Ohio Educational Computer Association (NOECA)  
219 Howard Dr.  
Sandusky, Ohio 44870-8603

To Members of the Board:

### *Scope*

We have examined NOECA's accompanying Description of its Alpha 8200 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 NOECA'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 NOECA 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 NOECA 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, NOECA 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. NOECA 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 NOECA to provide additional information and is not part of the NOECA'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 NOECA'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 NOECA'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 NOECA, user entities of NOECA'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.

A handwritten signature in black ink that reads "Dave Yost". The signature is written in a cursive style with a large, looping initial "D".

**Dave Yost**  
Auditor of State

June 25, 2012

**This Page Intentionally Left Blank**



## Northern Ohio Educational Computer Association

219 Howard Drive, Sandusky, OH 44870

419.627.1439 Fax 419.627.5608

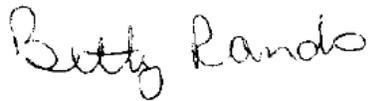
[www.noeca.net](http://www.noeca.net)

We have prepared the description of the Northern Ohio Educational Computer Association (NOECA) HP Alpha Server 8200 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 HP Alpha Server 8200 (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 USAS, USPS, and SAAS/EIS. The NOECA 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 NOECA 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, 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 NOECA 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.

Betty Rando, Director

A handwritten signature in cursive script that reads "Betty Rando".

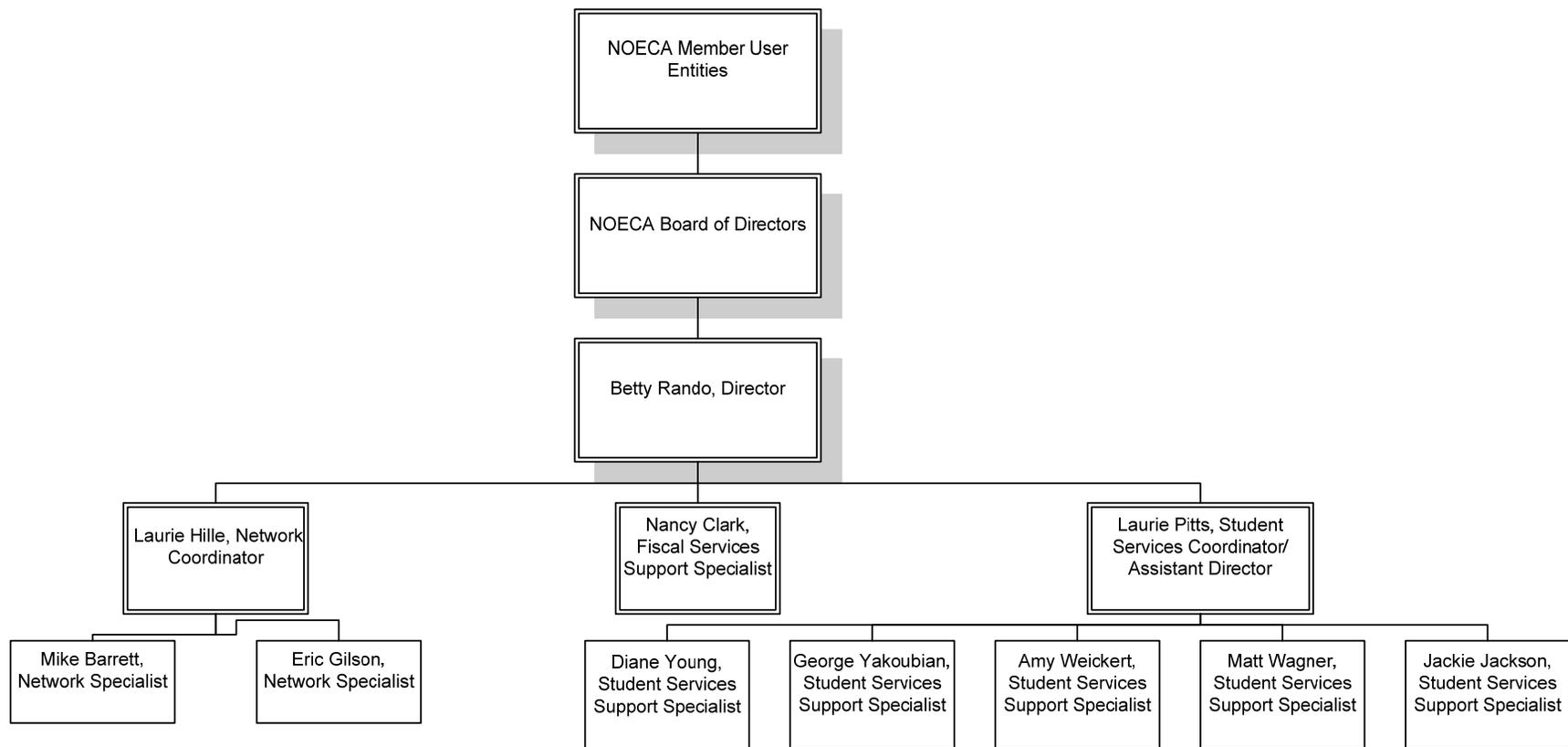
June 25, 2012

## SECTION 3 - DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM

### CONTROL OBJECTIVES AND RELATED CONTROLS

The Northern Ohio Educational Computer Association (NOECA) 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 NOECA's description of controls.

### OVERVIEW OF OPERATIONS



The NOECA 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 NOECA 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 Council of Governments (COG) under ORC 167. ORC 3313.92 allows for school districts to create a partnership (a consortia) to resolve mutual needs. One of the members of the consortia is designated as fiscal agent. The fiscal agent provides all accounting, purchasing, and personnel services for the consortia. A "COG" under ORC chapter 167 allows for one or more governmental entities to join together to form a new legal entity. A COG can have its own treasurer, make its own purchases, hire staff, and have debt obligations. NOECA is organized under section 3313.92 and is thus required to have a board of education serve as its fiscal agent to receive OECN funds from the ODE. For this reason, the North Point Educational Service Center (NPESC), serves as the fiscal agent for NOECA and performs certain functions that might otherwise be performed by NOECA.

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

### ***Control Environment***

Operations are under the control of the director and the NOECA board of directors. The superintendent from each user entity is appointed to the legislative body known as the association assembly. The assembly meets once per year to approve the fee structure, approve the budget and elect members of the board of directors.

The board of directors is the governing body of the NOECA and is composed of two superintendents for each of the counties of Erie, Huron, Ottawa, Sandusky, Seneca and Wood, one superintendent from Crawford County, and the fiscal agent superintendent. The board meets the first Monday of August, November, February and May. The board has also established an operating committee to make recommendations to the board of directors.

The NOECA employs a staff of 16 individuals and is supported by the following functional areas:

<i>Fiscal Services:</i>	Provides end user support and training for the NOECA user entities for the state software applications, including USAS, USPS, and SAAS/EIS.
<i>Student Services:</i>	Supports end users in all aspect of the student service applications, EMIS and Data Analysis for Student Learning (DASL).

<i>INFOhio Services:</i>	Provides support to a statewide project using computer technology to help Ohio schools manage instructional resources located in libraries, classrooms, offices, storerooms and other areas of the school building.
<i>Network Services:</i>	Supports the NOECA computer systems and its networked communication system and provides user training and support.
<i>Video Services:</i>	Provides support for video conference and distance learning.
<i>Technical Support:</i>	Provides contracted services to schools in the area of technical support.

The NOECA follows the same personnel policies and procedures as their fiscal agent, the North Point Educational Service Center. When necessary, additional NOECA policies have been developed to address specific concerns of NOECA. Detailed job descriptions exist for all positions. The NOECA 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. Evaluations are conducted on an annual basis by the director. The chairperson of the NOECA board performs an annual evaluation of the director.

Users are responsible for 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 entity data are infrequent. Only experienced staff may alter user entity data and only at the request of the user entity.

The NOECA 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 or experience in a computer-related field, and all the NOECA 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. All the NOECA staff members are permitted and encouraged to attend professional training as deemed necessary.

The NOECA 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 user entity administrators, two current and/or former ITC Directors, and one additional team member to provide training to subsequent teams. Approximately three to five ITC site reviews are conducted annually. The sites chosen for review are designated by the OECN Oversight Advisory Committee as approved by ODE. The guidelines and recommended procedures for these reviews are based on the Ohio Administrative Code, which cover the following areas: governance, administration, finance, personnel and staff development, physical facilities, hardware, software, user in-service, and operations. The NOECA has not been scheduled for review as of the date of the report.

The NOECA has Service Level Agreements (SLA) with their user entities for certain computer, data processing, and applications services. The user entities agree to pay a fee based upon a fee schedule set forth by the governing board and they agree to abide by the security policies implemented by the NOECA. These SLAs are in effect beginning July 1, 2008, and will be in effect until terminated in writing by either the user entity or the NOECA.

### ***Risk Assessment***

The NOECA 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 of directors:

- Oversee all of NOECA operations.
- Establish policy.
- Make recommendations to the assembly regarding constitutional amendments, budgets, expansions of facilities or services.
- Purchase equipment.
- Appoint operating committee members.

In addition, the NOECA 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 NOECA organization is structured so that department managers report directly to the director and staff report to the department managers. Key management employees have worked at NOECA for many years and are experienced with the systems and controls at the NOECA. The NOECA director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, NOECA uses a variety of "key indicator" reports to monitor the processes involved in processing transactions for user entities.

Hardware, software, network, 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. In addition, the director receives the same reports and monitors them for interrelated and recurring problems.

### **INFORMATION AND COMMUNICATION**

The aspects of the information and communication component of internal control as they affect the services provided to user entities are discussed within the General EDP Controls section.

## **GENERAL EDP CONTROLS**

### **Development and Implementation of New Applications and Systems**

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

### **Changes to Existing Applications and Systems**

End-users participate in the program development/change process via the Software Performance Report/Request (SPR) tracking procedure, which is maintained by the SSDT. The SPR system utilizes SiteScape Forum, which is used for electronic conferencing, to accept and discuss proposed software enhancements in a public forum. Each major software package (USAS, USPS, SAAS/EIS) 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 NOECA 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 they will support only the latest release of the state software beginning 30 days following the software release date.

The NOECA 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 a 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 NOECA, a backup of the application or operating system affected by the change is prepared to ensure retention of the existing application or operating system in case of an error stemming from the upgrade process.

Documentation for the current version of the operating system and new releases are provided on the operating system media and on the HP web site, which is accessible by all ITCs. New releases include documented changes to the operating system and implementation procedures. The NOECA has their own copy of the operating system disks and documentation. This was purchased via the Technology Solutions Group (TSG) program under the MCOECN. This program allows the NOECA to purchase their operating system media at a reduced cost. The current release documentation is maintained by the fiscal services support specialist at NOECA. No new releases were installed during the audit period.

### **IT Security**

The NOECA has a security policy which outlines the responsibilities of user entity personnel, the NOECA personnel, and any individual or group not belonging to the user entity or the NOECA. In addition to the security policy, the NOECA uses a banner screen which is displayed when a user logs onto 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 NOECA personnel.

The NOECA 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.

User entities are granted access upon the written authorization from the superintendent, treasurer and/or building principal. These requests are sent to the NOECA and are reviewed by either the director or the fiscal services support specialist, who will create the account. Data center personnel access is established, granted and reviewed by the director using the system user report listing. Annually, user entity superintendents

and treasurers review the system user authorization report listing for all employees who have access to USAS, USPS, or SAAS/EIS to confirm authorization for continued user access.

Access to the Internet has been provided to the user entities of the NOECA. Access is provided through the OSCNet network and is routed to the NOECA. User entities were provided with model acceptable use policies which could be customized for their user entity. NOECA provides a mail server which allows each user entity to administer their domain.

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 the system to monitor any security violations on the NOECA 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 summary and detail reports. These reports, also called security monitor reports, are e-mailed to the director and the fiscal services support specialist 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 NOECA uses Fortiguard, Security Plus and Symantec anti-virus software to scan inbound and outbound e-mail. A message will pass through varying levels of anti-virus scanning depending on if the traffic is inbound or outbound and if it is going to NOECA or the user entities. All traffic goes through a minimum of two levels of anti-virus. The NOECA updates the anti-virus definitions on an hourly basis and applies software patches as they become available.

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

The User Identification Codes (UIC) are individually assigned to all users. UICs are assigned at the user entity's request. UIC based protection controls access to objects such as files, directories, queues and volumes.

User accounts are set up with the CAPTIVE flag which restricts access to the command line. The CAPTIVE flags are typically not used for administrative accounts (NOECA employees or system accounts) because they require access to the command line.

The system forces users to periodically change their passwords. The DEFAULT account password lifetime and password length fields have been set according to the standards established by NOECA. 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.

Users must provide a valid operating system username and password to authenticate to the USAS and USPS web applications. Once authenticated, users are automatically given only those privileges assigned in each user's default login security profile. The SSDT developed a program called OECN\_RPC (Remote Procedure Call) service which, in conjunction with VXS created by the SSDT, allows users to authenticate through a XML interface using standard operating system authentication policies. If authentication is successful, the RPC service "impersonates" the user by acquiring an operating system security profile of the authenticated user (i.e. default privileges and security identifiers). Once the RPC has acquired the corresponding security profile the operating system process has the same security rights as the authenticated user. The network client then provides a code indicating the user entity data to be used. The RPC service uses the user entity code to define logical definitions to associate the server process with the desired user entity data.

Only default privileges from the user's authorization file record are enabled during a session. The session does not enable any authorized privileges. Therefore, when the service process accesses data files, their default login security profile is used. A user can select predefined OECN software functions that are available to the OECN\_RPC service. (For example, USAS functions for posting a requisition). When the user has finished using the respective web application the logout button is clicked to disconnect. Alternatively, the session may disconnect automatically after the configured inactivity timeout.

The system forces users to periodically change their passwords. The systems manager sets passwords to expire when a new user identification code is issued. New users must log in "interactively" to change their passwords. Notification of password expiration for existing users occurs automatically prior to the password expiration date. The NOECA has established minimum password lengths for all user accounts. When a user logs in to the USAS and/or USPS web applications, the user authorization file is updated to reflect that a non-interactive login has occurred. When a user logs in to the FISCWEB application, the user authorization file is not updated to reflect that a login has occurred.

The operating system has system parameters, which, when set appropriately, control and monitor sign-on attempts. There are parameters in place to control certain aspects of the sign-on procedure, which include the following:

- The terminal name is part of the association string for the terminal mode of break-in detection.
- The user is restricted on the length of time they have to correctly enter a password on a terminal on which the system password is in effect.
- The number of times a user can try to log in over a phone line or network connection. Once the specified number of attempts has been made without success, the connection is terminated.

- The length of time allowed between login retry attempts after each login failure.
- The length of time a user terminal, or node, is permitted to attempt a logon before the system assumes that a break-in attempt is occurring and evasive action is taken.
- The period for which evasive action is taken is variable and will grow as further logon failures are detected from the suspect source.
- The number of retry attempts allowed for users attempting to logon before evasive action consists of refusing to allow any logons during a designated period of time.

System parameter standards have been established through the use of established defaults. Any changes are logged and reviewed by the director and fiscal services support specialist.

A timeout program, HITMAN, is used to monitor terminal inactivity and log-off inactive users after a predetermined period of time of non-use. The use of this program helps to reduce the risk of an unattended terminal being used to enter unauthorized transactions. The web applications also have a time-out feature that was created by the SSdT. This allows the NOECA to modify the time-out parameter to match NOECA policies. Also, timeout programs aid in efficient use of system resources by maintaining connectivity with only active system users.

Associated with each object recognized by the operating system may be an Access Control List (ACL). When an access request is made to an object, ACLs are always checked first. An ACL may either grant or deny access to the user requesting 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 SYSGEN parameter 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 ACL and UIC-based protection. The operating system analyzes privileges included in the user's authorization record and places the user in one of seven categories depending on which privileges have been granted to the user. Default privileges are those

authorized privileges that are automatically granted at login. If an authorized privilege is not a default privilege, it will not automatically be effective at login, and must be enabled or disabled by the user. All user entity users have NORMAL privileges.

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

To limit access to security files, the NOECA 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 operating system identifiers to authorized users. Each application package has a set of unique identifiers that permit access to programs. In addition to the standard identifiers for each package, a pass through identifier can be used to further customize access. OSA is used in conjunction with the OECN menu processor utility thus allowing the users to see only the items they are authorized to execute. UIC-based 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. Firewall equipment and additional routing devices deny all outbound traffic requests originating from the sub-network. In addition, the firewalls and routing devices deny access to all inbound traffic unless the IP address originated from inside the network. Instead, the requests are routed to a proxy server located in each network segment which serves to filter all Internet access. The Internet filter service retrieves requests from the Internet for the typical user. Permission to bypass the proxy server requires management authorization. In addition, an e-mail message is automatically sent to the superintendent and the user each time the proxy server is bypassed. A log of bypasses is maintained for reference purposes. The firewall also prevents all outside connections from accessing inside hosts or servers, unless the IP address originated from inside the network.

The data processing department is located in a secured office building. A key card system restricts access to the NOECA facility. A keypad lock restricts access to the computer room to NOECA personnel.

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

- Smoke and heat sensors.
- The Liebert air conditioning system dedicated to computer room, located in room adjacent to computer room.
- Two back-up air conditioners located in the computer room.
- An FM 200 fire suppression system and a hand held fire extinguisher.
- Raised flooring, with water sensors located beneath.
- Back up UPC with its own environmentally controlled room located adjacent to Liebert air conditioning.
- Back-up generator located outside staff door in back of building.

## 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. The NOECA has access to operations procedure manuals for the Alpha system. In addition, all users, except students, have access to a private SiteScape Forum, a bulletin board that allows the NOECA employees to communicate with users across the state.

User problems that require the NOECA staff to change data require written authorization from the user entity. The NOECA staff will not make changes to a user entity's data unless authorized by the user entity. E-mails authorizing the changes are saved. In addition, the user entities have the option of printing an AUDIT report that shows activity changes to their data files.

Certain routine jobs are initiated for system maintenance. The NOECA is responsible for operational maintenance tasks, such as system backups, directory updates, file rebuilds, data cleanup, and other maintenance directed at the whole system. The NOECA uses automated applications called DECScheduler and Job Access and Management System (JAMS) for scheduling and initiating tasks. The NOECA has lost the ability to update the DECScheduler with new tasks due to the operating system version updates. As a result new tasks are scheduled and initiated through the JAMS. Perfect Disk is an optimization maintenance program scheduled and run through JAMS.

Common problems which arise daily, such as terminal lockups and program crashes are usually handled by the NOECA service representatives over the phone and may not be documented. Complicated problems relating to the network are logged through Computer Associates (CA) Unicenter ServicePlus Service Desk which is the statewide help desk application. The NOECA staff will log the reason for the call, the user entity having the problem, the priority level of the call, the staff member assigned to the call, the date and time of the call, and the status of the call (in-progress, first alert, or closed). The resolution of the problem must be logged before the call can be closed.

The NOECA has maintenance agreements for the computer equipment with Service Express. If NOECA cannot resolve a hardware problem, they will call Service Express and log the call on the service calls log sheet.

In addition, network devices are monitored continuously. A network monitoring software product, "Castle Rock SNMP," monitors network devices using SNMP, or as a last resort, by initiating a "ping" command toward a given device. If the device does not respond to the ping then the software identifies the device as non-functional, changing the color of the device's on-screen icon from green to red. By clicking on the device's icon, the software will show a more detailed problem description. Response to the problem depends on the type of failure.

The NOECA has documented backup procedures. Backup tapes are created on a daily, month end, fiscal and calendar year end basis. A full system backup is completed Monday through Friday. Each morning, the previous night's backup is rotated to Margareta Local Board of Education and the oldest set of tapes (approximately 4 weeks old) is returned to the computer center for use the next evening. Historical year-end and fiscal year-end tapes are maintained at NOECA. A daily reminder is sent to the director and fiscal services support specialist to check if errors occurred during the backup. Nightly backups are also completed each night that send data to the off-site disaster recovery site. Logs of these backups are reviewed by the fiscal services support specialist.

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

### **Complementary User Entity Controls**

These 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 control at the NOECA. User auditors should consider whether the following controls have been placed in operation at the user entity:

1. User entities should have controls over their own web applications which access their data stored at the NOECA to ensure only thoroughly tested and authorized web applications are implemented.
2. User entities should maintain current service level agreements with the NOECA for USAS, USPS, SAAS, and technical support.
3. User entity management should make users aware of the confidential nature of passwords and the precautions necessary to maintain their confidentiality.
4. User entity management should immediately request the NOECA to revoke the access privileges of user entity personnel when they leave or are otherwise terminated.
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. The user entity 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. The user entity should establish and enforce a formal data retention schedule with the NOECA 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 NOECA'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 NOECA and procedures performed at user entities that utilize the NOECA.*

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

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

### Changes to Existing Applications and/or Systems

<b>Changes to Existing Applications and Systems - Control Objective:</b> <b>Change Requests</b> - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
In order to maintain continued support of the application software provided by the SSDT, NOECA is 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 NOECA was compared to the CRCs of the object files at the SSDT.	The POFORM USAS file had a different CRC from that distributed by the SSDT. This file is commonly used to customize purchase orders.  No other exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements and problems corrected. Updated user and system manuals are also made available.	Inspected the release notes and updated manuals for the March 2012 release.	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 documentation at the HP web site.	No exceptions noted.

**IT Security**

<b>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.</b>		<b><i>Control Objective Has Been Met</i></b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The NOECA has established a Data System Security Policy, an Internet Security Policy and a Web Server Acceptable Use Policy that outline user responsibilities regarding computer security and access.	Inspected the NOECA security policies to confirm user responsibilities are documented.	No exceptions noted.
Authorization from the appropriate user entity management is required on the account request form before setting up a user account on the system.	Sampled 14 user accounts from a population of 132 accounts that were added or changed during the audit period. Inspected the account request forms and confirmations for the required authorizations.	One of the fourteen accounts didn't have an authorization form on file.
User entities are required to confirm user accounts annually with a positive confirmation to NOECA. The NOECA tracks the status of the confirmation and performs any necessary follow-up communication to facilitate a response from the user entity.	Inspected the confirmations returned to NOECA for evidence that each user entity signed and returned the confirmation.	No exceptions noted.
Tracking of security related events, such as break-in attempts and excessive login failures is enabled through the operating system. The events are logged to audit journals for monitoring of potential security violations.	Inspected the enabled security audits to confirm security violations are being logged.	No exceptions noted.

<b>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.</b>		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Security violations are extracted, compiled into summary and detailed security reports, and e-mailed to the NOECA staff, for review, daily through command procedures on the system.	<p>Inspected the following information relating to the security monitor reports to confirm these reports are produced and available for review:</p> <ul style="list-style-type: none"> <li>• Scheduler job parameters for the security monitor report.</li> <li>• Command procedure used to generate the report.</li> <li>• Sample security monitor report.</li> </ul> <p>Confirmed, with the director, the security monitor report is received and inspected on a daily basis.</p>	No exceptions noted.
Antivirus software runs on the mail server and primarily scans all inbound and outbound e-mail. Definitions are updated hourly, and infected items are quarantined to help prevent and detect computer viruses.	Inspected the anti-virus update and scan schedules to confirm software and virus definition files are updated hourly and scans are performed.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
<p>Password parameters are in place to aid in the authentication of user access to the production system. Passwords used by individual profiles are in accordance with the password policies established by NOECA.</p>	<p>Extracted information from the user authorization file to identify:</p> <ul style="list-style-type: none"> <li>• User accounts with a password length less than NOECA standards.</li> <li>• User accounts with a password lifetime greater than NOECA standards.</li> </ul> <p>Inspected the above exception reports to identify relevant exceptions. Inquired with the director regarding the appropriateness of the listed accounts.</p>	<p>Sixty of the 676 enabled accounts on the system had a password lifetime greater than NOECA's standard.</p> <ul style="list-style-type: none"> <li>• 1 account is an OECN account and has a password set to 110 days.</li> <li>• 59 accounts have password lifetime set to none. These accounts are used to view fiscal reports via the web or are application or system accounts.</li> </ul> <p>No other exceptions noted.</p>
<p>Password expiration for the web applications is defined at the system or process level.</p>	<p>Inspected the system logical that controls remote access to confirm password expiration is enforced for the web applications.</p>	<p>No exceptions noted.</p>
<p>Use of wild card characters in proxy accounts is restricted to ensure proxy accounts are specifically defined to not allow blanket access.</p>	<p>Inspected the proxy listing to confirm wild card characters were not used.</p>	<p>No exceptions noted.</p>
<p>Access to the operating system command line is restricted to authorized users of the system.</p>	<p>Extracted user accounts from the user authorization file that do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER, or RESTRICTED flags set.</p> <p>Inspected the results of the extracted information and inquired with the director regarding the appropriateness of these accounts.</p>	<p>No exceptions noted.</p>
<p>Log-in parameters have been set to control and monitor sign-on attempts.</p>	<p>Inspected the system log-in parameters to confirm parameters were set to control and monitor sign-on attempts.</p>	<p>No exceptions noted.</p>

<b>IT Security - Control Objective:</b> <b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
System and web application activity are monitored and inactive users are automatically disconnected after a predetermined amount of idle time.	<p>Inspected the HITMAN parameters to confirm they were set to automatically logoff inactive users.</p> <p>Inspected the start up file to confirm the HITMAN utility is part of the startup process.</p> <p>Inspected the configuration for the timeout values on the USAS and USPS web system.</p>	No exceptions noted.
Access to production data files and programs is properly restricted.	Inspected production data files with WORLD access and executable files with WORLD write and/or delete access to confirm they are properly restricted.	No exceptions noted.
A private internal network and firewall are used to control inbound and outbound traffic and maintain a logical segregation between user entities.	<p>Inspected the network diagrams to confirm components of the network which control inbound and outbound traffic.</p> <p>Inspected the firewall configuration to confirm a private internal network is used and that inbound and outbound traffic is restricted to the system through the firewall.</p>	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Application Level Access Controls</b> - Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Users are restricted to predefined logical access identifiers that grant varying access privileges based on requests from user management.	<p>Extracted information from the user authorization file to list accounts assigned with OECN identifiers. Inspected the listing for evidence of the use of identifiers to segregate access to the applications.</p> <p>Inquired with the director regarding the OSA utility and the process used to assign application identifiers.</p> <p>Compared the current user authorization file to prior year's user authorization file and identified 132 new accounts or accounts that have been modified. Sampled 14 user accounts from a population of 132 accounts that were added or changed during the audit period. Inspected the account request forms and compared the access granted to the access authorized per the user authorization form.</p>	<p>One of the fourteen accounts didn't have an authorization form or on file.</p> <p>No other exceptions noted.</p>
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized ITC users.	Extracted accounts from the user authorization file with the OECN_SYSMAN identifier. Inspected the list of accounts to confirm access was restricted to authorized users.	No exception noted.

<b>IT Security - Control Objective:</b> <b>System Software and Utilities Access Controls</b> - Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
WORLD access to "key" system and security files is restricted.	<p>Inspected the file protection masks on the system files to confirm WORLD write and/or delete access was absent.</p> <p>Inspected the file protection masks on the security files to confirm WORLD access was absent.</p>	No exceptions noted.
System level UICs and accounts with elevated privileges are restricted to authorized personnel.	<p>Identified the maximum system group number.</p> <p>Extracted accounts from the user authorization file with a UIC less than the maximum system group number and accounts with elevated privileges.</p> <p>Inspected the listings with the director to confirm only authorized personnel were listed.</p>	No exceptions noted.
An alternate user authorization file is not permitted to be used and does not exist.	<p>Inspected the value of the alternate user authorization file parameter to confirm the parameter's setting does not allow for the use of an alternate user authorization file.</p> <p>Inspected the system directory to confirm an alternate user authorization file does not exist.</p>	No exceptions noted.
Remote administration of the firewall used to control Internet access is restricted.	Inspected the firewall configuration to confirm a username and password is required and remote access is restricted.	No exceptions noted.

<b>IT Security - Control Objective:</b> <b>Physical Security</b> - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Physical access to the computer room and its contents is restricted to authorized personnel.	Inspected the use of keypad entry devices throughout the period of fieldwork.  Inquired with the NOECA staff regarding the periodic changing of access codes.	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**

<b>IT Operations - Control Objective:</b> <b>System Administration and Maintenance</b> - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Certain routine jobs for system maintenance such as directory updates, file rebuilds and data cleanup, are performed by the NOECA through scheduling programs called DECScheduler and JAMS.	Inspected the DECScheduler and JAMS listing of jobs to confirm jobs for system maintenance were scheduled.  Inspected the system startup file to confirm the DECScheduler and JAMS were initialized during the startup of the system.	No exceptions noted.
Castle Rock SNMP is used to monitor the network for hardware failures. If any device is not responding to pings the device will be highlighted.	Observed use of Castle Rock SNMP and confirmed its use for monitoring the network with the network specialist.	No exceptions noted.
A service agreement with Service Express covers maintenance and failures of the computer hardware.	Inspected the Service Express hardware service agreement for services covered and period of coverage.	No exceptions noted.
Requests for changes to user entity data must be authorized by the user entity via e-mail or in writing.	Inspected file folders for all user entities for hard copy documentation of requests on file from April 1, 2011 through March 31, 2012. Confirmed the procedures for changing user data with NOECA staff.	No exceptions noted.
Data center equipment is covered by insurance.	Inspected the insurance policy and payment documentation for evidence of coverage during the audit period.	No exceptions noted.

<b>IT Operations - Control Objective:</b> <b>Backup</b> - Up-to-date backups of programs and data should be available in emergencies.		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Written procedures document instructions for performing backups and for the proper storage of backup tapes at both the onsite and the off-site storage locations.	Inspected the NOECA's written backup procedures for content.	No exceptions noted.

<b>IT Operations - Control Objective:</b> <b>Backup - Up-to-date backups of programs and data should be available in emergencies.</b>		<b>Control Objective Has Been Met</b>
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The NOECA sends backups to the off-site disaster recovery site and runs backups from DECScheduler to tape. Backup logs are sent to NOECA staff to review.	<p>Inspected the DECScheduler with the director to confirm the nightly backups are scheduled. Inspected the listing for backup jobs, run times, status of the backups performed, and notification sent to the director and fiscal services support specialist to confirm nightly backups were completed and monitored for completion.</p> <p>Inspected the backup logs to the MCOECN TSG disaster recovery site with the director to confirm backups are sent each night.</p>	No exceptions noted.
Backups are stored in a secure off-site location.	Inspected the daily tapes maintained at the off-site storage facility to confirm they are rotated to a secure off-site location.	No exceptions noted.

## SECTION 5 - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION (*Unaudited*)

### INFORMATION TECHNOLOGY CENTER PROFILE OHIO EDUCATION COMPUTER NETWORK

#### SITE DATA

Name: Northern Ohio Educational Computer Association (NOECA)  
Number: 1  
Node Name: NOECA

Chairperson: William Lally  
Superintendent  
North Point Educational Service Center

Fiscal Agent: North Point Educational Service Center

Director: Betty Rando  
Director  
NOECA

Address: 219 Howard Drive  
Sandusky, Oh 44870

Telephone: 419-627-1439 Ext. 207  
FAX: 419-627-5608

Web site: [www.noeca.org](http://www.noeca.org)

OTHER SITE STAFF

Nancy Clark	Fiscal services support specialist
Laurie Pitts	Student services coordinator/assistant director
Jackie Jackson	Student services support specialist
Diane Young	Student services support specialist
Lisa Wendt	Library services support specialist
Chris VanFleet	Network specialist
Mike Barrett	Network specialist
Laurie Hille	Network Coordinator
Eric Gilson	Network Specialist
Chris Adams	Technical support specialist
Chad Enderle	Technical support specialist
George Yakoubian	Student services support specialist
Matthew Wagner	Student services support specialist
Russell Abbott	Technical support specialist
Amy Weikert	Student services support specialist

**HARDWARE DATA**

Central Processors and Peripheral Equipment

**CPU Unit 1**

<u>Model Number</u>		<u>Installed</u>		<u>Capacity/Density/Speed</u>	
CPU:	Compaq Alpha Server 8200	Lines/Ports:	N/A	Memory Installed:	5120 MB
Disk:	RZ29B	Units:	10	Total Capacity:	43 GB
Disk:	RZ29D	Units:	1	Total Capacity:	2.1 GB
Disk:	10KUWSE	Units:	15	Total Capacity:	270 GB
Printer:	LG04	Units:	1	Print Speed:	600 LPM

**USER ENTITY SITE DATA**

<u>IRN</u>	<u>USER ENTITY</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>
046508	Buckeye Central Local SD	Crawford	X	X	X
046789	Edison LSD	Erie	X	X	X
051029	EHOVE JVSD	Erie	X	X	X
125690	North Point ESC	Erie	X	X	X
044131	Huron City SD	Erie	X	X	X
046797	Kelleys Island Local SD	Erie	X	X	X
046805	Margaretta Local SD	Erie	X	X	
044743	Sandusky City SD	Erie	X	X	X
043596	Bellevue City SD	Huron	X	X	X
047712	Monroeville Local SD	Huron	X	X	X
044560	Norwalk City SD	Huron	X	X	X
047738	South Central Local SD	Huron	X	X	X
047746	Western Reserve Local SD	Huron	X	X	X
048926	Benton Carroll Salem Local SD	Ottawa	X	X	X
048934	Danbury Local SD	Ottawa	X	X	X
048942	Genoa Area Local SD	Ottawa	X	X	X
048959	Middle Bass Local SD	Ottawa	X		
048967	North Bass Local SD	Ottawa	X		
044651	Port Clinton City SD	Ottawa	X	X	X
048975	Put-in-Bay Local SD	Ottawa	X	X	X
045302	Clyde-Green Springs Ex Vill SD	Sandusky	X	X	X
044016	Fremont City SD	Sandusky	X	X	X
045385	Gibsonburg Ex Vill SD	Sandusky	X	X	X
049569	Lakota Local SD	Sandusky	X	X	X
051458	Vanguard-Sentinel JVSD	Sandusky	X	X	X

**USER ENTITY SITE DATA**

<u>IRN</u>	<u>USER ENTITY</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>
049577	Woodmore Local SD	Sandusky	X	X	X
049692	Bettsville Local SD	Seneca	X	X	X
043992	Fostoria Community School	Seneca	X	X	X
049700	Hopewell-Louden Local SD	Seneca	X	X	X
049718	New Riegel Local SD	Seneca	X	X	X
123257	North Central Ohio ESC	Seneca	X	X	X
049726	Old Fort Local SD	Seneca	X	X	X
049684	Seneca East Local SD	Seneca	X	X	X
045583	Perrysburg Ex Vill SD	Wood	X	X	X
050674	Eastwood Local SD	Wood	X		
050682	Elmwood Local SD	Wood	X	X	X
050716	Northwood Local SD	Wood	X	X	X
008065	Imani Learning Academy	Lucas	X	X	
000125	Polly Fox Academy	Lucas	X	X	
000130	Phoenix Academy	Lucas	X	X	
011511	North Central Academy	Seneca	X		
<b>TOTALS:</b>			<b>41</b>	<b>37</b>	<b>33</b>



# Dave Yost • Auditor of State

**NORTHERN OHIO EDUCATIONAL COMPUTER ASSOCIATION (NOECA)**

**ERIE 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**