NORTHWEST OHIO AREA COMPUTER SERVICES COOPERATIVE (NOACSC)
STATE REGION - ISA, ALLEN COUNTY

SAS - 70

JULY 12, 2008 THROUGH JULY 2, 2009

Mary Taylor, CPA
Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

Mary Taylor, CPA
Auditor of State

INDEPENDENT ACCOUNTANTS' REPORT

Board of Directors
Northwest Ohio Area Computer Services Cooperative (NOACSC)
645 S. Main Street
Lima, Ohio 45804

To Members of the Board:

We have examined the accompanying description of controls of the Northwest Ohio Area Computer Services Cooperative (NOACSC) applicable to the processing of transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS), and Education Management Information System (EMIS). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the NOACSC's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the internal controls contemplated in the design of the NOACSC's controls; and (3) such controls had been placed in operation as of July 2, 2009. The NOACSC uses the services of the Northwest Ohio Computer Association (NWOCA) for systems development and maintenance of the USAS, USPS, SAAS/EIS and EMIS. The accompanying description includes only those controls and related control objectives of the NOACSC, and does not include controls and related control objectives of NWOCA. Our examination did not extend to controls of NWOCA. The control objectives were specified by the NOACSC management for the processing of USAS, USPS, SAAS/EIS, and EMIS with the assistance of the Ohio Department of Education. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of the NOACSC's controls that had been placed in operation as of July 2, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the NOACSC's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from July 12, 2008 to July 2, 2009. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user organizations of the NOACSC and to their auditors to be taken into consideration along with information about the internal control at user organizations, when making assessments of control risk for user organizations.

In our opinion, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance the control objectives specified in Section III were achieved during the period from July 12, 2008 to July 2, 2009.

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

The information in Section IV describing the information technology center is presented by the NOACSC to provide additional information and is not part of the NOACSC's description of controls that may be relevant to a user organization's internal control. Such information has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for user organizations and, accordingly, we express no opinion on it.

The description of controls at the NOACSC is as of July 2, 2009, and information about tests of the operating effectiveness of specified controls covers the period from July 12, 2008 to July 2, 2009. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the NOACSC is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of the NOACSC, its user organizations, and the independent auditors of its user organizations.

Mary Taylor

Mary Taylor, CPA
Auditor of State

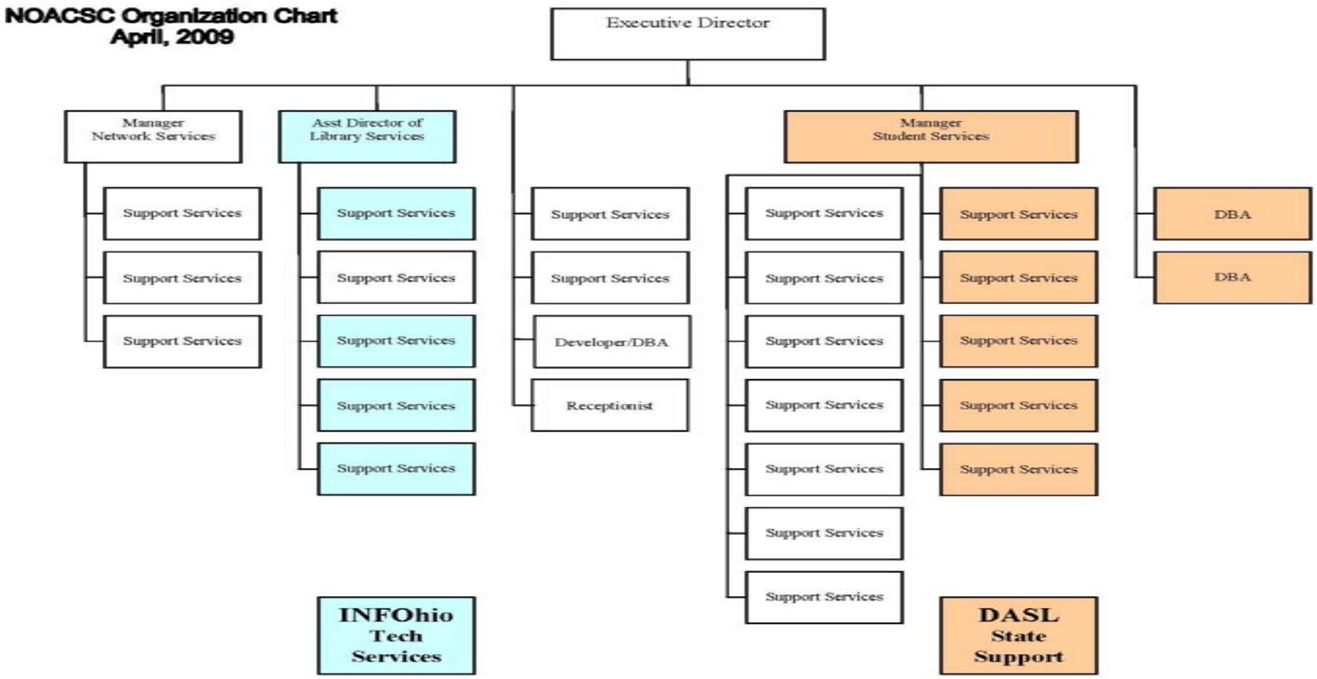
July 2, 2009

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The Northern Ohio Area Computer Services Cooperative (NOACSC) control objectives and related controls are included in section III of this report, “Information provided by the Service Auditor,” to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III. Although the control objectives and related controls are included in Section III, they are, nevertheless, an integral part of the NOACSC’s description of controls.

OVERVIEW OF OPERATIONS


NOACSC Organization Chart
April, 2009

The NOACSC is one of 23 government 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 NOACSC is derived from the state of Ohio and from user fees.

ITCs provide information technology services to school districts, community “charter” schools, JVS/career & technical, educational service centers (ESCs) and parochial schools; however, not all entities subscribe to the same services. Throughout the remainder of the report, the term “user organization” will be used to describe an entity which uses one of more of the following applications:

- Uniform School Accounting System (USAS).
- Uniform Staff Payroll System (USPS).
- School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS).
- Education Management Information System (EMIS).
- School Options Enrollment System (SOES)

ITCs are organized as either 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. NOACSC is organized under section 3313.92 and is thus required to have a board of education serve as its fiscal agent. The Western Buckeye Educational Service Center (ESC) serves as the fiscal agent for the NOACSC.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the governing board. The governing board is composed of two members from each county elected by a majority vote of all charter member user organizations in each county, plus one representative from the fiscal agent. The board meets approximately once a month and at other times as deemed necessary.

The NOACSC employs a staff of 30 individuals and is supported by the following functional areas:

Fiscal Services: Provides end user support and training for the NOACSC user organizations for the state software applications, including USAS, USPS, SAAS/EIS and EMIS.

Technology: Provides a variety of educational technology services to subscribing NOACSC user organizations including software and Internet access, training, technology planning, and technical assistance.

Student Services: Support end users in all aspect of the student service applications, EMIS and Data Analysis for Student Learning (DASL).

Network Support: Provides user training and support for the NOACSC computer system and its networked communication system.

All NOACSC staff ultimately report to the executive director.

The NOACSC is generally limited to recording user organization transactions and processing the related data. Users are responsible for authorization and initiation of all transactions. Management reinforces this segregation of duties as a part of its new employee's orientation process, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced NOACSC employees may alter user data and only at the request of the user organization.

The NOACSC follows personnel policies and procedures adopted by the Governing Board and their fiscal agent, the Western Buckeye ESC. Detailed job descriptions exist for all positions. The NOACSC 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 NOACSC's hiring practices place an emphasis on the hiring and development of skilled information technology professionals. All the NOACSC staff members are required to attend professional development and other training as a condition of continued employment. Each staff member must obtain at least 1.5 continuing educational units (CEU) of approved professional development annually, and at least eight approved CEUs every four years. The NOACSC tracks continuing education requirements for its employees. The NOACSC pays 100% of the incurred costs in attending professional development seminars. Employee evaluations are conducted annually. The board performs an annual evaluation of the executive director.

The NOACSC 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 organization 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 NOACSC has not been scheduled for review as of the date of the report.

The NOACSC has Service Level Agreements (SLA) with their user organizations for certain computer, data processing, and applications services. The user organizations 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 NOACSC. These SLAs are in effect beginning July 1, 2008, and will be in effect until terminated in writing by either the user organization or the NOACSC.

Risk Assessment

The NOACSC does not have a formal risk management process; however, the governing board actively participates in the oversight of the organization.

As a regular part of its activity, the governing board addresses:

- New technology.
- Realignment of the NOACSC organization to provide better service.
- Personnel issues, including hiring, termination, and evaluations.
- Additional services provided to user organizations and other entities.
- Changes in the operating environment as a result of ODE requirements, Auditor of State (AOS) and other accounting pronouncements, and legislative issues.

In addition, the NOACSC has identified operational risks resulting from the nature of the services provided to the user organizations. These risks are primarily associated with computerized information systems. These risks are monitored as described under “Monitoring” below and in additional detail throughout the “General EDP Controls” section of this report.

Monitoring

The NOACSC organization is structured so that each staff member ultimately reports to the executive director. Key employees have worked here for a number of years and are experienced with the systems and controls at the NOACSC. The NOACSC executive director and network services manager monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, NOACSC uses a variety of “key indicator” reports to monitor the processes involved in processing transactions for user organizations.

Hardware, software, network, database integrity, Internet usage, computer security and user help desk reports are monitored on an ongoing basis by departmental management. Some of these reports are automatically run through a scheduler program and sent to management via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily. In addition, the executive director receives the same reports and monitors 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 organizations are discussed within the “General EDP Controls” section.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

The NOACSC staff members do not perform system development activities. Instead, the NOACSC 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 Ohio Department of Education (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 (MC OECN), 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/or Systems

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

The NOACSC personnel do not perform program maintenance activities for USAS, USPS, EMIS, or SAAS. 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. The SSDT, at NWOCA, copies zipped files containing the quarterly updates to the ITCs' systems. The source code is not distributed with these files. Release notes are contained within these files and explain the changes, enhancements and problems corrected. User and system manager manuals are also distributed with these releases. The SSDT informs the ITCs that they will support only the latest release of the state software beginning 30 days following the software release date.

The NOACSC 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 an INSTALL_PACKAGE procedure with several functions that installs full package releases, partial releases or patches on the system. This utility ensures that all required components are installed properly and consistently.

Only vendor supplied changes are made to the operating system or system software documentation. The Northern Buckeye Education Council (NBEC), which acts as the fiscal agent for this and other participating ITCs, has entered into a license under the Campuswide Software License Grant Program (CSLG) through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of HP software packages.

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

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

- Provide telephone technical support to the participating ITCs technical staff for a limited series of HP software packages approved by the executive committee of the MCOECN.

- Track and maintain an accurate listing of all HP hardware and software covered under the agreement.

- Provide periodic training and update sessions covering the policies and regulations governing this program as well as updating the ITCs' technical staff on the latest releases of HP software packages covered under the agreement.

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

- Read, sign, and comply with the rules and regulations of the CSLG Program and the Education Software Library (ESL) Program as operated by the NBEC on behalf of the MCOECN.

- Provide unrestricted access to all computer systems covered under the agreement for the purposes of identifying and/or correcting problems of distributed software.

- Provide HP or MCOECN representatives, upon prior written notice, with physical access to computer facilities at reasonable times during normal business hours to inspect centers and system records for compliance with the terms of the CSLG and ESL Programs.

- Make payments to NBEC for services under the agreement within 30 days of the receipt of an invoice for said services.

The NBEC provides documentation and support for new releases of the operating system. New releases include documented changes to the operating system and implementation procedures. OpenVMS documentation is available on the HP web site, for the current version of the operating system, accessible by all ITCs. In addition, the NOACSC can purchase a copy of the operating system disks from the NBEC via the MCOECN Value-Added Reseller (VAR) program, which offers the operating system software at a reduced rate.

IT Security

The NOACSC has a security policy that outlines the responsibilities of user organization personnel, the NOACSC personnel, and any individual or group not belonging to a user organization or the NOACSC.

The NOACSC staff is granted access within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities. The NOACSC uses the signatures on forms as an acceptance to the security policies of the NOACSC.

Users from the user organizations are granted access upon the receipt of a written "Authorized Account Application" form from the superintendent and/or treasurer. These authorization forms are sent to the executive director, network services manager, or user liaison who will then update the account and e-mail the treasurer regarding the newly established account. The network services manager establishes, grants, and reviews access rights for data center personnel and an authorization form is not used.

Quarterly, the network services manager executes a batch program to identify accounts that have been inactive for the past 120 days. Each user organization is sent an email listing their corresponding inactive accounts. In addition, the email indicates that if the accounts are not logged into the system by a specified date they will be deleted.

The NOACSC policies and procedures are partly enforced through the use of system alarms and audits. The following security alarms and audits have been enabled through OpenVMS to monitor security violations on the NOACSC 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.

In addition, the following security audits have been enabled through OpenVMS to monitor for additional security violations: install, time, sysgen, privilege failure, file access, device access, and volume access.

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 network services manager and reviewed daily. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and the corrective action needed.

The NOACSC utilizes anti-virus software to scan inbound and outbound e-mail. Virus definitions are updated daily, and infected items are deleted.

Primary logical access control to the HP computers is provided by security provisions of the OpenVMS operating system. Individual user profiles are used to grant access rights and privileges for the 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.

The NOACSC does not utilize proxy logins. 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 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.

Associated with each object recognized by OpenVMS may be an Access Control List (ACL). When an access request is made to an object, ACLs are always checked first. An ACL may either grant or deny access to the user requesting it.

Access to the OpenVMS system command line is restricted through the use of login scripts and the CAPTIVE flag. All 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 (NOACSC employees or system accounts) because they require command line access.

The system forces users to periodically change their passwords. All user accounts have a password lifetime set by management. Passwords are set to expire when a new user identification code is issued or when a user has forgotten his password. This parameter requires the user to change his password during the first logon procedure. Standards for minimum password length have been set by management.

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.

System parameter standards have been established through the use of HP established defaults. Any changes are logged and reviewed by the executive director and/or network services manager.

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

When an ACL fails to specifically grant access, the system defaults to User Identification Code (UIC) based protection. The UICs are individually assigned to all data processing personnel employed at the NOACSC. The Group Identification Code (GIC) is assigned to all accounts. For user organizations which use the NOACSC system, multiple user organization users may share an individual UIC; however would have different GICs. Therefore, each account would have a unique GIC, UIC combination. UICs are assigned at the user organization's request. UIC based protection controls access to objects such as files, directories, and volumes.

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

SYSTEM: Any of the following: (1) Users with a UIC group number between 1 and SYSGEN parameter MAXSYSGROUP (default decimal 8, octal 10). (2) Users with system privileges (SYSPRV). (3) Users with group privileges (GRPPRV) whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

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

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

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

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

Through a firewall and switch, user organizations have been set up with sub-networks that have addresses not recognizable to the Internet, known as a private internal network. The firewall and switch also prevent all outside connections from accessing inside hosts or servers, unless the IP address originated from inside the network or the user organization requests certain access to their network from outside (i.e. HTTP, and e-mail, etc.).

The NOACSC staff use an internal wireless access point to provide a convenient means of access to the network. Wireless traffic is encrypted from point to point within the building. Access to the wireless device’s configuration is controlled through password protection.

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, SAAS/EIS, and EMIS application data files.

A powerful identifier OECN_SYSMAN grants all access privileges to all state developed software and is restricted to authorized NOACSC staff. In addition, the BYPASS privilege automatically grants the user the OECN_SYSMAN identifier. The BYPASS privilege is an operating system privilege and functions the same for all ITCs.

To limit access to security files, the NOACSC 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.
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.

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

Remote access to the firewall and various switches is restricted through password protection. Additionally, passwords are encrypted in the devices' configurations.

The data processing department is in an enclosed area, secured by both a key lock and an ADT alarm system. All doors are locked during off hours. During daytime hours, all doors entering the building and to the computer room remain locked at all times. The Northwest Ohio Security System Inc. monitors all building doors and motion detectors 24 hours a day, 7 days a week.

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

- Halon fire extinguishers.
- Heat alarm in the event the temperature exceeds preset level.
- 2 Lenox systems and one Carrier unit are used to monitor temperature and humidity.
- Smoke detectors.
- Raised floor with water sensors.
- Power distribution device to prevent power surges to any of the equipment in the computer room.
- All devices are connected to battery backup systems.
- Entire building utilizes a stand by propane powered generator.

The environmental controls and alarms are attached to the security system, which will alert the security company if something is detected. The security company will then contact the appropriate personnel.

IT Operations

Traditional computer operations procedures are minimal because user organizational personnel initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All NOACSC employees have access to an operations procedures manual, which provides directions and guidelines for most of the operational functions performed. In addition, all users, except students, have access to the SiteScape Forum, which is a bulletin board that allows the NOACSC employees to communicate with users across the state.

The NOACSC staff has privileges that permit them to assist participating user organizations in performing data entry transactions. The privilege is necessary in order to respond to requests to resolve data entry inaccuracies. NOACSC are not allowed to make modifications to user organization data outside the normal application process. Additionally, NOACSC requires approval via e-mail or phone call prior to assisting user organizations. In addition, NOACSC as part of the fiscal year end procedures runs the FISCALCD.COM for USAS and USPS reports. The reports created by this command file are put on the web and also burned to cd's that are given to the user organizations. The user organizations may print out an "AUDIT" report, which shows activity changes to the data file for changes made through the application.

Operations at the NOACSC consist primarily of application installation, system software installation, backup procedures, restart and recovery procedures, and maintenance procedures. The NOACSC also serves as a help-line to the user organizations. The user organization's users call the NOACSC whenever they have a problem with applications or hardware.

NOACSC is responsible for operational maintenance tasks, such as system backups, file rebuilds, log reports, and other maintenance directed at the whole system. They use two automated applications to schedule and perform these tasks.

User organizations are responsible for handling abnormal terminations. If the users cannot solve the problem, they will contact the NOACSC staff. Service Express is contacted for hardware problems that cannot be solved by the NOACSC staff. The NOACSC staff often handles daily problems (e.g., terminal lockups or program crashes) over the phone. If necessary, a staff person will come on-site to resolve the problem.

Network devices at the NOACSC are continuously monitored with the use of an application. The program continuously contacts all network devices. In the event a device does not respond, a network technician is contacted through an automated process to resolve the issue.

Daily full system backups are performed Sunday through Saturday. These backups include the transaction files for each of the user organizations. A stand alone backup that includes all programs, data files, system files, and the operating system, is performed the second Monday of each month. The tape is rotated to the off-site storage facility on Monday morning. The previous Friday's backup tape is returned to the on-site storage location to be reused.

On-site backup tapes are stored in a bank vault next to the computer room within the NOACSC facility. Off-site backup tapes are stored at a board of education building, which is approximately 1.5 miles away. The off-site tapes are located within a locked supply room.

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

USER CONTROL CONSIDERATIONS

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

1. User organizations should have controls over their own web applications which access their data stored at the NOACSC.
2. User organizations should maintain current service level agreements with the NOACSC for USAS, USPS, EMIS, SAAS, and technical support.
3. User organization management should have practices to ensure users are aware of the NOACSC security policies and that the users take precautions to ensure passwords are not compromised.
4. User organization management should immediately request the NOACSC to revoke the access privileges of user organization personnel when they leave or are otherwise terminated.
5. User organizations should have documented acceptable use policies to define the activities deemed appropriate for use of the Internet. Internet users should be required to accept the terms of the policy before access is provided.
6. User organization management should retain signed copies of the authorization form for new user accounts and changes to existing accounts.
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. The user organization 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.
11. The user organization should establish and enforce a formal data retention schedule with the NOACSC for the various application data files.

SECTION III - INFORMATION PROVIDED BY THE SERVICE AUDITOR

This section is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the NOACSC's internal control that may be relevant to user organization's internal control, and reduce the assessed level of control risk below the maximum for certain financial statement assertions.

The broad objectives of data processing controls should be achieved by a combination of the procedures that are employed in various segments of the transaction processing system, for example procedures performed at the NOACSC and procedures performed at user organizations that utilize the NOACSC.

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

Changes to Existing Applications and/or Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Applications developed and maintained by the SSDT at the NWOCA are the same as those distributed to and utilized by NOACSC. The most recent application updates are distributed by the SSDT and NOACSC is required to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the program object files for each application was obtained and compared to the CRCs of the latest SSDT version tested at NWOCA to confirm the USAS, USPS, SAAS, and EMIS software versions tested at NWOCA are the same versions used at NOACSC.	No exceptions noted.
The SSDT distributes release notes and updated manuals to the NOACSC when application updates are released. Updated manuals are also provided on the SSDT web site.	Inspected the release notes and updated manuals for the most recent releases.	No exceptions noted.
The NOACSC participates in the CSLG/ESL program in order to maintain a licensing agreement which provides operating system support, software upgrades, software related documentation, and technical support.	Inspected a copy of the NOACSC's CSLG licensing agreement with the NBEC and payment information to confirm it is current. Inspected online documentation and inquired with the systems manager to determine if the NOACSC is provided with the most current documentation for the operating system.	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 for the most recent version of the operating system.	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:*
The NOACSC requires a standard form for user authorization for all users other than NOACSC staff. The authorization form must be signed by the appropriate management before adding a user account on the Alpha system.	Using an analysis tool identified all accounts on the Alpha which have not been DISUSERed. Haphazardly selected 40 accounts from a population of 1397 and inspected the user authorization forms to confirm the required signatures were present.	No exceptions noted.
Quarterly, the executive director generates and forwards a list of inactive SYSUAF user accounts to each user organization informing them these accounts will be deleted.	Inspected inactive account email messages sent to all user organizations during the audit period. Utilizing an analysis tool, compared the inactive accounts identified in the emails sent to the user organizations to the system user authorization file to confirm if the accounts were deleted from the Alpha if a response was not received.	No exceptions noted.
The tracking of security related events such as break-in attempts and excessive log failures are enabled through OpenVMS. The events are logged to audit journals for monitoring of potential security violations.	Inspected the security alarms and audits to confirm they are enabled.	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 and network services manager. The command procedure is automatically resubmitted to the system daily.	Confirmed security monitoring procedures, including the process for monitoring reports and the frequency of review, with the network services manager. Inspected the following relating to the security monitor reports to confirm these reports are produced daily and forwarded to the appropriate personnel: • Security monitor report. • Command procedure used to generate the report. • Scheduler job parameters for the security monitor report.	No exceptions noted.
Anti-virus software runs on the mail server and file servers to help protect against computer viruses. Definitions are updated daily, and infected items are deleted to help prevent computer viruses.	Inspected, with the network services manager, an ESET log, and PineAPP update log, residing on the mail and file servers to confirm anti-virus definitions are updated daily.	No exceptions noted.

<table>
<tr><td colspan="2"><b>IT Security -</b> <i>Control Objective:</i>
<b>System Level Access Controls -</b> Access to the computer system, programs, and data should be appropriately restricted.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>The system does not consist of an excessive number of unused or inactive user profiles.</td><td>Using an analysis tool, extracted the following information from the user authorization file:
• User accounts that have not been used in at least 180 days.
• User accounts that have not been logged into.
Inspected the results of the extracted information and inquired with the network services manager regarding the appropriateness of the information generated.</td><td>No relevant exceptions noted.</td></tr>
<tr><td>Proxy logins are not utilized by the NOACSC.</td><td>Inspected the proxy listing to confirm NOACSC does not use proxy logins.</td><td>No exceptions noted.</td></tr>
<tr><td>Access to the operating system command line is restricted to authorized users.</td><td>Using a security analysis tool, extracted user accounts that do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER, or RESTRICTED flags set.
Inspected the results of the extracted information and inquired with the network services manager regarding the appropriateness of these accounts.</td><td>No relevant exceptions noted.</td></tr>
</table>

IT Security - *Control Objective:* **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Password parameters are in place to aid in the authentication of user access to the system. Passwords used by individual profiles agree to password policies established by the NOACSC and the number of profiles with pre-expired passwords is limited.	Using an analysis tool, extracted information from the user authorization file to identify: • User accounts with password minimum lengths less than the NOACSC standard. • User accounts with a password lifetime greater than the NOACSC standard. • User accounts with pre-expired passwords. Inspected the above exception reports to identify relevant exceptions. Inquired with the network services manager regarding the appropriateness of the listed accounts.	The following exceptions were noted: Password lifetimes agree to policies established by the NOACSC. However, the password policy allows for password lifetimes longer than industry standards. No additional relevant exceptions were noted.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameter settings. Confirmed settings have not been changed from suggested vendor settings.	No exceptions noted.
A program constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed.	Inspected the HITMAN parameters to confirm they were set to logoff inactive users. In addition, identified protected accounts and confirmed the appropriateness of accounts with the system manager. Inspected the system startup file to confirm the HITMAN utility was part of the startup process.	No exceptions noted.
Access to production data files and programs is restricted to authorized users.	Inspected the directory listing of executable files for the USAS, USPS, EMIS and SAAS/EIS application programs and identified files with WORLD access. Inspected a listing of user organization data files and identified files with WORLD access.	No relevant exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls -** Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A firewall and routers are used to control Internet traffic and maintain a logical segregation between user organizations.	Inspected the network diagram to confirm components of the network that control Internet access. Inspected the firewall configuration to confirm Internet traffic to the Alpha and other devices is restricted through the firewall. In addition, confirmed the existence of a private internal network.	No relevant exceptions noted.
The wireless access point located at and used by NOACSC staff is encrypted to prevent unauthorized access to the system.	Inspected the wireless router configuration to confirm encryption is used.	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 predefined logical access identifiers that grant varying access privileges based on requests from user management.	Using an analysis tool identified all active user accounts with the OECN identifiers for the USAS, USPS, SAAS/EIS, and EMIS application systems. Inspected the reports to determine whether the identifiers were used to segregate access to the applications. Inquired with the fiscal systems specialist regarding the OSA utility and the process used to assign application identifiers. Haphazardly selected 34 user accounts, with an OECN identifier, from a population of 979. Compared the access granted to the access authorized per the user authorization form.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized NOACSC users.	Using an analysis tool, extracted accounts from the user authorization file with the OECN_SYSMAN identifier. Inspected the list of accounts. Inquired with the network services manager regarding the appropriateness of the listed accounts.	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.	Inspected the file directory listing for the system directories and the file protection masks to confirm there was no WORLD write and/or delete access. Inspected the file protection masks on the security files to confirm there was no WORLD write and/or delete access.	No exceptions noted.
System level user identification codes are restricted to only authorized personnel.	Identified the maximum system group number. Used data analysis tools to identify a listing of all accounts with a UIC less than the maximum system group number. Confirmed the appropriateness of identified accounts with the network services manager.	No exceptions noted.
An alternate user authorization file is not permitted to be used and does not exist.	Inspected the value of the alternate user authorization parameter to confirm an alternate file is not permitted. Inspected the system directory listings to confirm an alternate user authorization file did not exist.	No exceptions noted.
Remote administration of the firewall and router configurations used to control Internet access, is restricted.	Inspected the firewall and main switch/router configurations to confirm remote administration was permitted and to confirm passwords are required to access the configuration menus.	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 computer room and inquired with the network services manager regarding personnel access to the room. Inspected the service agreement and payment documentation with Northwest Ohio Security System Inc.	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 with the network services manager to confirm the existence of the environmental controls.	No exceptions noted.

IT Operations

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A service agreement with Service Express covers maintenance and failures on the computer hardware.	Inspected the Service Express agreement for services covered, period of coverage, and the corresponding payment documentation.	No exceptions noted.
NOACSC runs routine system maintenance programs such as cleanup of data files, backup creation, and security log creation. In addition, the programs are included in the scheduler and the scheduler is included in the system startup.	Inspected the startup file and the scheduler procedure listing to confirm routine system maintenance programs are initiated at startup and automatically scheduled to run.	No exceptions noted.
NOACSC staff correct and troubleshoot application issues and problems with equipment for user organizations.	Independently inquired with the network services manager and technicians regarding how problems (e.g., abnormal terminations, program errors, terminal lockout, application software errors, and hardware problems) at the user organizations are resolved.	No exceptions noted.
Application software monitors network performance and alerts staff of hardware failures.	Inspected the system status screen for the network monitoring software. Inquired with the network technicians regarding how the network monitoring software is used to detect and resolve hardware problems.	No exceptions noted.
All data center hardware and software equipment is covered by an insurance policy.	Inspected the property insurance policy and proof of payment for coverage of NOACSC equipment during the audit period.	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:*
Daily full backups of systems and data are performed Sunday through Saturday. All backups are automated and are scheduled. The scheduler is part of the system startup.	Made inquiry regarding backup procedures with the network technician. Inspected the system startup file and scheduler to confirm the scheduler initiates at startup and that backup commands are executed through the scheduler daily. Inspected the backup command procedure and an example of the daily backup log.	No exceptions noted.
Backup tapes are stored in a secure on-site location and rotated to a secure off-site location regularly. Additionally, backup tape listings are used to track the location of backups.	Confirmed backup tape rotation procedures with the secretary/receptionist assigned to rotate backups. Inspected the on-site and off-site storage locations to confirm the backups were stored in secure locations. Inspected the backup tape listing to confirm the backups listed were stored at either the on-site or off-site storage locations.	No exceptions noted.

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

CENTER DATA

Name:	Northwest Ohio Area Computer Services Cooperative (NOACSC)
Number:	5
Node Name:	NOACSC
Chairperson:	Rob Wannemacher Treasurer Wayne Trace Local Schools
Fiscal Agent District:	Western Buckeye ESC
Administrator:	Ray Burden Executive Director NOACSC
Address:	645 South Main Street Lima, OH 45804
Telephone:	419-228-7417
FAX:	419-222-5635
Website:	www.noacsc.org

OTHER CENTER STAFF

David Rowe	Network technician
Jennifer Sudhoff	Local fiscal support
Brenda Core	Local fiscal support
Terri Shutt	Assistant director of library services
Carolyn Winhover	Programmer
Dave Daugherty	Network support
Kevin Hellman	Network services manager
Jean Banks	State INFOhio support
Eric Schumm	Network liaison
Christine Daugherty	Local DASL support
Sheila Rowe	Local EMIS support
Debbie Barbee	Manager student service support
Charles Schmiesing	State INFOhio support
Dan Pottkotter	Local progressbook support
Juanita Markham	State INFOhio support
Bonnie Blachly	Local INFOhio support
Janell Delvesco	Local EMIS support
Lora Lawrence	State DASL database administrator
Mike Ridinger	State INFOhio support
Melissa Drerup	State DASL support
Chris Keller	State DASL support
Denise McDaniel	Local DASL support
Amy Recker	State DASL support
Travis Thomas	State DASL database administrator
Jaime Best	Local progressbook support
Jennifer Schwartz	Secretary/Receptionist
Janice Ditto	State DASL support
Devin Launder	State DASL support
Scott Schaffner	Developer/DBA

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	Compaq Alpha Server 4100 5/600	Lines/Ports:	3	Memory Installed:	6 GB
Disk:	Attached to a SAN	Units:	18	Total Capacity:	Unlimited
CPU:	HP RX2600X Itanium Server	lines/ports:		Memory Installed:	8 GB
Disk:	146GB Drives	Units:	8	Total Capacity:	.9 TB
Tape Unit:	LTO488	Units:	1	Max Density:	200 GB
Printer:	HP4000	Units:	1	Print Speed:	17 PPM
Printer:	HP8150	Units:	2	Print Speed:	32 PPM

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION SITE	COUNTY	USAS	USPS	SAAS	EMIS
043885	Delphos CSD	Allen	X	X	X	X
044222	Lima CSD	Allen	X	X	X	X
045211	Bluffton EVSD	Allen	X	X	X	X
045740	Allen County ESC	Allen	X	X	X	X
045757	Allen East LSD	Allen	X	X	X	X
045765	Bath LSD	Allen	X	X	X	X
045773	Elida LSD	Allen	X	X	X	X
045781	Perry LSD	Allen	X	X	X	X
045799	Shawnee LSD	Allen	X	X	X	X
045807	Spencerville LSD	Allen	X	X	X	X
050773	Apollo JVSD	Allen	X	X	X	X
151175	West Central Learning Academy	Allen	X	X		X
044727	St. Marys CSD	Auglaize	X	X	X	X
044982	Wapakoneta CSD	Auglaize	X	X	X	X
043984	Findlay CSD	Hancock	X	X	X	X
047407	Hancock County ESC	Hancock	X	X	X	X
047415	Arcadia LSD	Hancock	X	X	X	X

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION SITE	COUNTY	USAS	USPS	SAAS	EMIS
047423	Arlington LSD	Hancock	X	X	X	X
047431	Cory-Rawson LSD	Hancock	X	X	X	X
047449	Liberty Benton LSD	Hancock	X	X	X	X
047456	McComb LSD	Hancock	X	X	X	X
047464	Van Buren LSD	Hancock	X	X	X	X
047472	Vanlue LSD	Hancock	X	X	X	X
045187	Ada EVSD	Hardin	X	X	X	X
043729	Celina CSD	Mercer	X	X	X	X
045310	Coldwater EVSD	Mercer	X	X	X	X
048546	Mercer County ESC	Mercer	X	X	X	X
048595	Fort Recovery LSD	Mercer	X	X	X	X
048553	Marion LSD	Mercer	X	X	X	X
048579	Parkway LSD	Mercer	X	X	X	X
048587	St. Henry Conservatory SD	Mercer	X	X	X	X
045575	Paulding EVSD	Paulding	X	X	X	X
048991	Antwerp LSD	Paulding	X	X	X	X
049031	Wayne Trace LSD	Paulding	X	X	X	X
134999	Western Buckeye ESC	Paulding/Van Wert	X	X	X	X

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION SITE	COUNTY	USAS	USPS	SAAS	EMIS
049304	Putnam County ESC	Putnam	X	X	X	X
049312	Col. Grove LSD	Putnam	X	X	X	X
049320	Continental LSD	Putnam	X	X	X	X
049338	Jennings LSD	Putnam	X	X	X	X
049346	Kalida LSD	Putnam	X	X	X	X
049353	Leipsic LSD	Putnam	X	X	X	X
049361	Miller City-New Cleveland LSD	Putnam	X	X	X	X
049379	Ottawa-Glandorf LSD	Putnam	X	X	X	X
049387	Ottoville LSD	Putnam	X	X	X	X
049395	Pandora-Gilboa LSD	Putnam	X	X	X	X
044966	Van Wert CSD	Van Wert	X	X	X	X
050351	Crestview LSD	Van Wert	X	X	X	X
050369	Lincolnview LSD	Van Wert	X	X	X	X
051672	Vantage JVSD	Van Wert	X	X	X	X
050708	North Baltimore LSD	Wood	X		X	X
133363	Quest learning Academy	Allen	X	X		X
000402	Findlay Digital Academy	Hancock	X	X		X
149344	Ohio Virtual Academy	Lucas				X

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION SITE	COUNTY	USAS	USPS	SAAS	EMIS
TOTALS:			**52**	**51**	**49**	**53**

Mary Taylor, CPA
Auditor of State

NORTHWEST OHIO AREA COMPUTER SERVICES COOPERATION (NOACSC)

ALLEN COUNTY

CLERK'S CERTIFICATION

This is a true and correct copy of the report which is required to be filed in the Office of the Auditor of State pursuant to Section 117.26, Revised Code, and which is filed in Columbus, Ohio.

Susan Babbitt

CLERK OF THE BUREAU

CERTIFIED
SEPTEMBER 22, 2009