WESTERN OHIO COMPUTER ORGANIZATION (WOCO)
STATE REGION - ISA, SHELBY COUNTY

SAS - 70

JUNE 14, 2008 THROUGH JUNE 12, 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
Western Ohio Computer Organization (WOCO)
129 E. Court St., 1st Floor
Sidney, Ohio 45365

To Members of the Board:

We have examined the accompanying description of controls of the Western Ohio Computer Organization (WOCO) 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 WOCO'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 WOCO's controls; and (3) such controls had been placed in operation as of June 12, 2009. The WOCO 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 WOCO, 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 WOCO 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 WOCO's controls that had been placed in operation as of June 12, 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 WOCO'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 June 14, 2008 to June 12, 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 WOCO 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.

88 E. Broad St. / Tenth Floor / Columbus, OH 43215-3506
Telephone: (614) 466-3402 (800) 443-9275 Fax: (614) 728-7199
www.auditor.state.oh.us

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 June 14, 2008 to June 12, 2009.

The relative effectiveness and significance of specific controls at the WOCO 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 WOCO to provide additional information and is not part of the WOCO'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 WOCO is as of June 12, 2009, and information about tests of the operating effectiveness of specified controls covers the period from June 14, 2008 to June 12, 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 ITC 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 WOCO, its user organizations, and the independent auditors of its user organizations.

Mary Taylor

Mary Taylor, CPA
Auditor of State

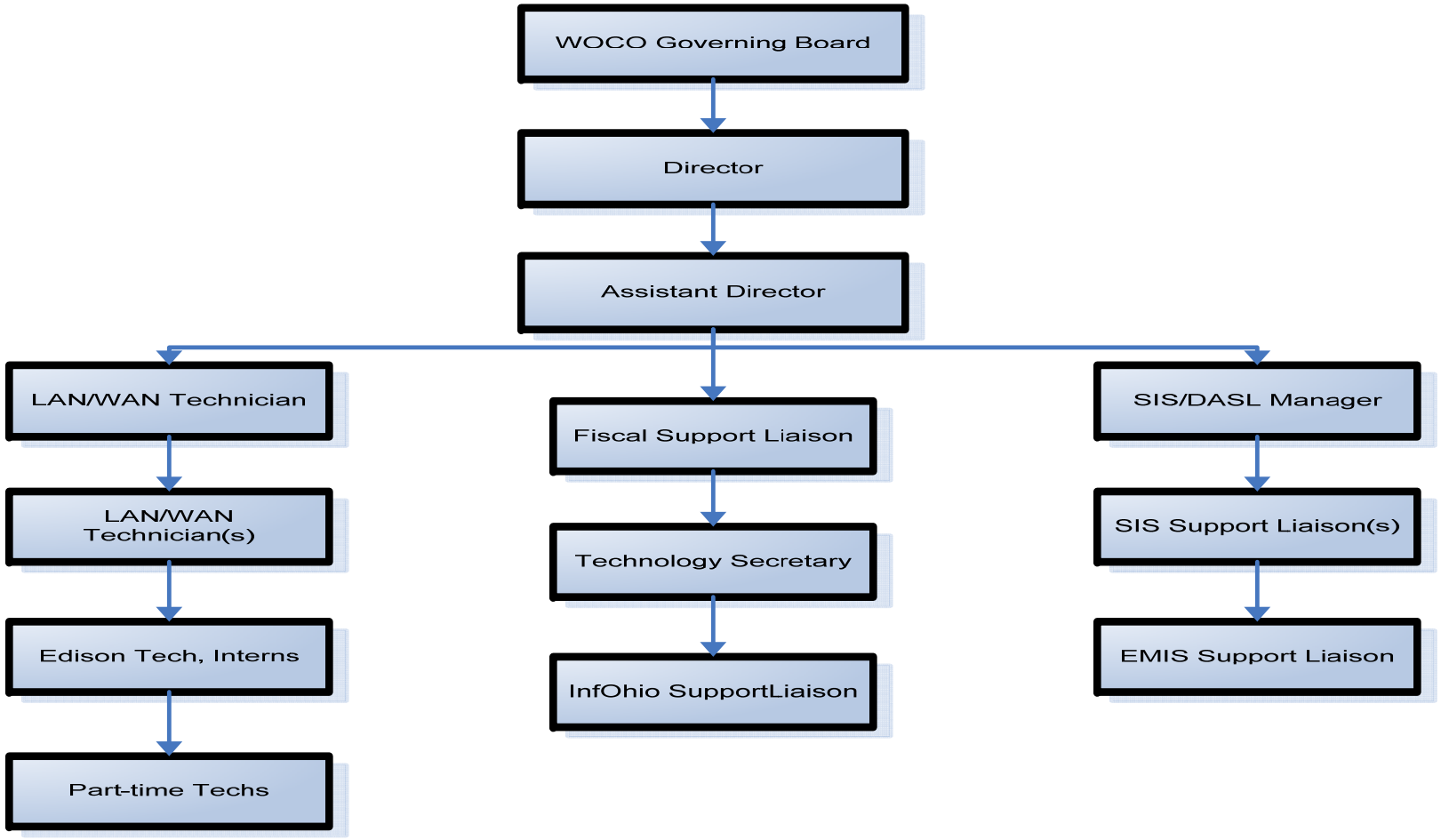
June 12, 2009

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The WOCO's control objectives and related controls are included in section III of this report, "Information provided by the Service Auditor," to eliminate the redundancy that would result from listing them here in section II and repeating them in section III. Although the control objectives and related controls are included in section III, they are, nevertheless, an integral part of the WOCO's description of controls.

OVERVIEW OF OPERATIONS



The WOCO 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 WOCO 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 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).
- 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. WOCO is organized under section 3313.92 and is thus required to have a board of education serve as its fiscal agent. For this reason, the Shelby County Educational Service Center serves as the fiscal agent for the WOCO.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the director and the board of directors. One member from each member user organization is appointed to the legislative body known as the organization assembly and is normally the user organization superintendent. The assembly meets once a year and is responsible for electing the board of directors, approving new cooperative ventures, the annual budget, the basic fee schedule, and amendments to the WOCO's constitution.

The board of directors is the governing body of the WOCO and is composed of the superintendent of the fiscal agent, two superintendents from each of the counties within the WOCO's service area, one representative each from the treasurer and student service users, one non-voting independent user organization representative and a chartered school member representative. The board meets on a bimonthly basis beginning in August of each fiscal year and at other times as deemed necessary. The board has also established several advisory committees to assist in the operation of the WOCO and its programs.

The WOCO employs a staff of 15 positions and is supported by the following functional areas:

Fiscal Services:	Provides support and training to end users for all fiscal services applications. (USAS, USPS, and SAAS/EIS)
Technology:	Provides a variety of educational technology services to subscribing WOCO user organizations including software and Internet access, training, technology planning, and technical assistance.
EMIS Support:	Provides end user support and training for WOCO user organizations for the EMIS state software application.

The managers of each of the functional areas report to the director.

The WOCO 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 orientation process, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced employees may alter user data and only at the request of the user organization.

The WOCO follows the same personnel policies and procedures as their fiscal agent, the Shelby County Educational Service Center. When necessary, additional WOCO policies have been developed and approved by the WOCO board of directors to address concerns of the WOCO. Detailed job descriptions exist for all positions. The WOCO 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 WOCO's hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the organization require some type of college degree in a computer-related field, and all the WOCO staff members are required to attend professional development and other training as a condition of continued employment. Each staff member must attend at least fifteen hours of approved professional development training annually, and at least eighty hours of approved training every four years. In addition, management encourages staff members to obtain additional training by providing a tuition reimbursement program for approved college work, and by paying 100% of incurred costs in attending professional development seminars. Employee evaluations are conducted annually. The board performs an annual evaluation of the director.

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

Risk Assessment

The WOCO does not have a formal risk management process; however, the board of directors comprises representatives from the user organizations who actively participate in the oversight of the WOCO.

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

- New technology.
- Realignment of the WOCO 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 and other accounting pronouncements, and legislative issues.

In addition, the WOCO 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 WOCO organization is structured so that department managers report directly to the director. Key management employees have worked here for many years and are experienced with the systems and controls at the WOCO. The WOCO director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, WOCO 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 technology manager 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/or Systems

The WOCO staff members do not perform system development activities. Instead, the WOCO 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 (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/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, 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 WOCO 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. 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 WOCO 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. 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 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 participating ITC technical staff for a limited series of HP software packages approved by the board of trustees of the MCOECN.

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

- Provide 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 privileged 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.

Before new releases are installed at the WOCO, 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 HP web site. New releases include documented changes to the operating system and implementation procedures. In addition, the MCOECN provides all *ITC*'s with purchasing discounts on hardware and software through the Technology Solutions Group program under the MCOECN (mc•tsg).

IT Security

The WOCO has a computer network and Internet acceptable use policy that outlines the responsibilities of user organization personnel, the WOCO personnel, and any individual or group not belonging to the user organization or the WOCO.

The WOCO utilizes a program called ARP (Account Request Procedure), which is a protected program to create new user accounts. New user accounts for user organization personnel are created by having the treasurer, superintendent, or other authorized individual run the ARP program. User organizations must call the WOCO office to add a user to the authorization list for processing the program. The ARP program prompts the user for the following information: name, title, and programs authorized. Once this information is entered, an e-mail is automatically sent to the WOCO for review prior to creation of the account.

The WOCO 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. Access for staff is established, granted, and reviewed by the director and no authorization form is used.

The WOCO uses a banner screen that is displayed before logging into the system. The screen informs the user that unauthorized access of the

system is prohibited and individuals using this computer system consent to the security policies of the WOCO and are subject to having their activities monitored by the WOCO personnel.

A list of users and their corresponding access rights within the user organization. is generated and sent quarterly via an automated script to the respective superintendents to verify the present users on the system were properly authorized. The superintendent also confirms the access rights of each account.

Security alarm messages are sent to an operator terminal that has been enabled to receive security event messages. Security audit messages are sent to the audit log file; alarms are sent to the operator log file. Access to the operator log and audit log is limited to data processing personnel. Critical events should be reported as both alarms and audits; less critical events can be written to a log file for later examination. The following security alarms and security audits have been enabled through the operating system to monitor security violations on the WOCO system:

ACL:	Gives file owners the option to selectively alarm certain files and events. READ, WRITE, EXECUTE, DELETE, or CONTROL modes can be audited.
AUDIT:	Enabled by default to produce a record of when other security alarms were enabled or disabled.
AUTHORIZATION:	Enables monitoring of changes made to the system user authorization file 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 operator log, creates a summary report and a detail report which contain information on unsuccessful logon attempts and any use of the authorize command. The command procedure is owned by the system account and only users with system privileges can access the command procedure. The security monitor report, is e-mailed to the director and technology manager daily for review. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and the corrective action needed.

Access to the Internet has been provided to the user organizations of the WOCO. Access is provided through the OSCNet network and is routed to the WOCO. The WOCO utilizes Sophos Anti-Virus software on the Alpha and Mail Marshal servers to scan all inbound and outbound e-mail. If a virus is found, the e-mail is quarantined and the recipient and support staff are sent e-mails informing them of the infected e-mail.

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 operating 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 WOCO utilizes 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 any access control information. A proxy login differs from an interactive login because an interactive login requires a user to supply a user name and password before the user can perform any interactive operations. Proxy records are located in the proxy file.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the WOCO and to all user organization users who use the WOCO system. UICs are assigned at the user organization's request. UIC based protection controls access to objects such as files, directories, and volumes.

Certain limited access accounts require a less restrictive environment than captive accounts. Accounts, under which network objects run, for example, require temporary access to the command line. Such accounts must be set up as restricted accounts, not captive accounts. User accounts should be set with the RESTRICTED flag instead of the CAPTIVE flag if they need to use network applications like MAIL or network proxy accounts. The RESTRICTED and CAPTIVE flags are typically not used for administrative accounts (treasurers and their staff) because access to the command line prompt is necessary for them to manipulate print queues. However, all other users are assigned the RESTRICTED and CAPTIVE flags.

The system forces users to periodically change their passwords. An account password lifetime standard has been established by management. Most UIC accounts have a password lifetime set at the standard; however there are a few accounts that have password lifetimes greater than the standard. These accounts are system accounts and Ohio Career Information System (OCIS) accounts which have a separate parameter.

The WOCO sets passwords 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. The minimum password length for each user is typically the default or another value established by the password minimum qualifier.

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

- The terminal name is part of the association string for the terminal mode of break-in detection.
- The user is restricted on the length of time they have to correctly enter a password on a terminal on which the system password is in effect.
- The number of times a user can try to log in over a phone line or network connection. Once the specified number of attempts has been made without success, the user loses the carrier.
- The length of time allowed between login retry attempts after each login failure.
- The length of time a user terminal, or node, is permitted to attempt a logon before the system assumes that a break-in attempt is occurring and evasive action is taken.
- The period for which evasive action is taken is variable and will grow as further logon failures are detected from the suspect source.

- The number of retry attempts allowed for users attempting to logon before evasive action consists of refusing to allow any logons during a designated period of time.

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

Associated with each object recognized by the operating system may be an Access Control List (ACL). When an access request is made to an object, ACLs are always checked first. Access to the operating system command line is restricted through the use of login scripts. The WOCO has a master login command which when executed puts the user into the state's menu system which prevents the user from leaving its controlled environment. Any attempt to leave the menu logs the user off of the system. WOCO assigns each of their employees an individual UIC. A unique group UIC number is assigned to each user organization and each user in the user organization is assigned a number under that group.

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

The WOCO 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 configuration is controlled through password protection.

Access to the OECN software packages is controlled at the ITC level 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. The powerful identifier OECN_SYSMAN grants all access privileges to all state developed software and is restricted to authorized WOCO staff. In addition, the BYPASS privilege automatically grants the user with access similar to the OECN_SYSMAN identifier. The BYPASS privilege is an operating system privilege and functions the same for all ITCs.

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 WOCO 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.

Certain privileges can override all UIC-based and ACL protection. The operating system 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.

The WOCO computer room is located in a Shelby County building in Sidney. The door to the computer room always remains locked. The main doors to the building are locked during non-business hours. The WOCO offices are located in another building nearby in Sidney. There are two entrances into the WOCO offices. One door always remains locked while the other is locked when the WOCO offices are not in use.

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

- Halon fire extinguishers.
- Leibert system to monitor temperature and humidity.
- Raised flooring.
- Power distribution device to prevent power surges to any of the equipment in the computer room.
- Un-Interruptible Power Supplies ensure the system will continue to operate in the event the power fails.
- Smoke detectors.

IT Operations

Traditional computer operations procedures are minimal since users at the user organizations initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. The WOCO staff has privileges that permit them to assist participating user organizations in performing data entry transactions. This is necessary so staff can respond to participating user organizations' requests and assist in resolving data entry errors. User organizations are responsible for changes to their own data. Occasionally WOCO will assist the user organizations with data changes upon receipt of an e-mail. User organizations are encouraged to review the "AUDIT" report, which shows all activity changes to their data files.

Certain routine jobs are initiated for system maintenance. WOCO is responsible for operational maintenance tasks, such as system backups, cleanup of .txt files, cleanup of disks, creation of the security log, and other maintenance directed at the whole system. They use an automated application called SCHEDULER which schedules and performs these tasks. SCHEDULER is a program that continually submits jobs on the Alpha system.

The WOCO staff have privileges that permit them to assist participating user organizations in performing data entry transactions. The privilege is necessary in order to respond to participating user organization personnel requests in resolving data entry inaccuracies. User organizations request help in resolving data entry inaccuracies/errors via CA Unicenter's help desk by posting a ticket. Any invalid transactions should be discovered by the user organization in their balancing procedures. In addition, the districts may print out an "AUDIT" report which shows all activity changes to the data file if the change was made to the application.

The WOCO utilize software to monitor network performance and hardware failures. The application pings the network hardware continuously to see each if each device responds. If a device fails to respond, the software indicates a failure and an email is sent to the LAN/WAN technician for resolution.

Common problems that arise daily, such as terminal lockups and program crashes, are usually handled by the WOCO service representatives over the phone. Critical problem aspects from the console log, such as system failures, are reviewed periodically by the director.

WOCO has a hardware maintenance agreement with HP for its computer equipment and with DataServ for the communications connections for the user organizations.

The WOCO Operations manual documents backup procedures for backing up system programs, data, and related documentation. Full system backups are performed daily for the computer system. All system and program documentation is stored electronically and is subject to the same back-up procedures as the other data files. All data required by law to be maintained for a specific duration is maintained by the WOCO. Calendar year and fiscal year-end information is stored indefinitely for all the WOCO user organizations.

On-site backup tapes are stored in the WOCO computer room. Off-site backup tapes are stored at the WOCO offices located across the street from the computer room. The off-site tapes are located within a fire-proof cabinet outside the director's office.

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:

General EDP Control Procedures

1. User organizations should have controls over their own web applications which access their data stored at the WOCO.

2. User organizations should maintain current service level agreements with the WOCO for USAS, USPS, EMIS, SAAS, and technical support.

3. User organization management should have practices to ensure users are aware of the WOCO security policies and that the users take precautions to ensure passwords are not compromised.

4. User organization management should immediately request the WOCO to revoke the access privileges of user organization personnel when they leave or are otherwise terminated.

5. User organization personnel should respond to account confirmation requests from their WOCO.

6. 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.

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 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 their WOCO for the various application data files.

The user control considerations presented above do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at the user organization.

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 WOCO'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 WOCO and procedures performed at user organizations that utilize the WOCO.

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

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Changes to Existing Applications or Systems

Changes to Existing Applications or Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
In order to maintain continued support of the application software provided by SSDT, ITCs are required to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the object program files for each application was obtained and compared to the CRCs of the latest SSDT version tested at NWOCA to ensure the USAS, USPS, SAAS, and EMIS software versions tested at NWOCA are the same versions used at WOCO. Inquired with the director to confirm procedures for installation of new releases	No relevant 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 most recent release. Confirmed with the systems manager that installation procedures, explanation of changes, enhancements, and/or corrections are documented and communicated to the WOCO. Inspected the SSDT web-site for availability of updated manuals.	No exceptions noted.

Changes to Existing Applications or Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The WOCO 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 WOCO'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 WOCO is provided with the most current documentation for 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:*
Authorization from the appropriate user organization management via an Account Request Procedure (ARP) request is required before setting up a user account on the Alpha.	Utilized a data analysis tool to identify the population of 86 new user accounts. Obtained and inspected the Account Request Procedure (ARP)'s for 25 of 86 new user accounts to confirm proper authorization by the treasurer and/or superintendent.	No exceptions noted.
Quarterly, a list of users and their access is sent to the user organizations for confirmation of authorization.	Confirmed the authorization procedures with the director. Inspected the procedure that generates the listing of inactive accounts to all user organizations. Inspected the confirmation checklist to confirm user organizations are replying to the confirmations being sent out.	Madison-Champaign ESC and Ohio Hi-Point Career Center did not respond to the confirmations sent to the user organizations.
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 security alarms and audits enabled to confirm the security related events were appropriately 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 reports are automatically e-mailed for review by WOCO staff. The security monitor report is scheduled to run daily.	With the director, confirmed security monitoring procedures, including the process for monitoring reports and the frequency of review. Inspected the following information relating to the security monitor report to confirm these reports are produced and available for review daily: • Example of a security monitor report. • Security monitor command procedure utilized to generate the report. • Scheduler for command procedure utilized to generate the report and email notification.	No exceptions noted.
Anti-virus software runs on the Alpha and Mail Marshal servers. Definitions are updated automatically and infected items are quarantined to help prevent and detect computer viruses.	Inspected the anti-virus update schedule to confirm software and virus definition files are updated hourly. Inspected payment documentation to the vendor for anti-virus services and updates.	No exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The user profiles on the system do not consist of an excessive number of inactive profiles.	Using an analysis tool, extracted information from the user authorization file to identify: • User accounts that have not been used in 180 days. • User accounts that have never been logged into. Inquired with the director regarding the purpose and appropriateness of accounts extracted.	No relevant exceptions noted.
Wild card characters are not used to define NETPROXY accounts.	Inspected the proxy listing for wild card characters.	No exceptions noted.
Log-in scripts are used to restrict user access to the command prompt.	Inspected the login scripts (login procedure) with the director to confirm the use of “captive scripts” for user accounts.	No exceptions noted.
Password parameters are in place to aid in the authentication of user access to the Alpha. Passwords used by individual profiles agree to password policies established by the WOCO and profiles with pre-expired passwords are not excessive on the system.	Utilized an analysis tool to identify the following within the system user authorization file: • User accounts with password minimum lengths shorter than the established guidelines of WOCO. • User accounts with password lifetimes longer than the established guidelines of WOCO. • User accounts with pre-expired passwords. Inspected the listed accounts with the director.	No relevant exceptions noted
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the login parameter settings.	No exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A program, HITMAN, constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed at startup.	Inspected the HITMAN parameters. In addition, identified protected accounts and confirmed the appropriateness of accounts with the system manager. Inspected the system startup file to confirm the HITMAN program was part of the startup procedures.	No exceptions noted.
Access to production data files and programs is properly restricted.	Using an analysis tool, identified and inspected production data files with WORLD access and executables files with WORLD write and/or delete access.	No relevant exceptions noted.
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user organizations.	Inspected network diagram to confirm components of the network which control Internet access. Inspected the firewall configuration for inbound and outbound control lists, for existence of a private internal network, and to confirm well known ports are controlled. Made inquiry with the LAN/WAN technician regarding routers to confirm all Internet traffic is routed to the firewall.	No relevant exceptions noted.
The wireless access point located at WOCO and used by WOCO staff is encrypted to prevent unauthorized access to the system	Made inquiry regarding the use of wireless networking to determine the extent of the wireless component of the network. Inspected the control utility screen to confirm the use of encryption.	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 a data analysis tool, extracted information from the users authorization file listing all identifiers for evidence of the use identifiers to segregate access to the applications. Inquired with the assistant director regarding the OSA utility and the process used to assign application identifiers. Using a data analysis tool, extracted accounts with the OECN identifiers for the USAS, USPS, SAAS/EIS, and EMIS application systems. From a selection of 25 new accounts, compared the identifiers authorized by management to those identifiers granted on the system.	No exceptions noted.
The OECN_SYSMAN identifier grants all access privileges for all state developed applications and is restricted to authorized users.	Obtained a listing of the accounts having the OECN_SYSMAN identifier. Inspected the list of accounts to confirm the identifier had not been provided to user organization staff members. Confirmed the functionality of the identifier with the assistant director.	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 system file directory listings for WORLD write and/or delete access. Inspected the file protection masks on the security files.	No exceptions noted.
System level UICs and accounts with elevated privileges are restricted to authorized personnel. UICs belonging to the system group are determined by the parameter value for MAXSYSGROUP. UICs less than the MAXSYSGROUP value have system level privileges. Accounts with elevated privileges are defined as those accounts having more than the minimum privileges to use the system.	Identified the maximum system group value. Using an analysis tool, extracted accounts from the user authorization file to identify: • Accounts with a UIC less than the MAXSYSGROUP value. • Accounts with elevated privileges. Inspected the listed accounts and inquired with the director as to the appropriateness of the listed accounts.	No exceptions noted.
An alternate user authorization file does not exist and is not permitted.	Inspected the value of the alternate user authorization parameter to determine whether an alternate file is permitted. Inspected the system directory listings to determine if an alternate user authorization file existed.	No exceptions noted.
Remote access to firewall and router configurations used to control Internet access is restricted to authorized personnel and is password protected.	Inspected the firewall configurations to confirm passwords are required to access the configuration menus and to confirm remote administration is allowed. Confirmed with the LAN/WAN Technician that passwords are changed periodically.	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.	Toured the computer room and made inquiry regarding personnel access with the LAN/WAN technician.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, humidity, or changes in temperature.	Toured the computer room with the LAN/WAN technician, and observed 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 HP covers maintenance and failures on the computer hardware.	Inspected the hardware maintenance agreements and payment information for service levels, effective period, and payment.	No exceptions noted.
WOCO 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.
The application software, Solarwinds, monitors network performance and alerts staff of hardware failures.	Made inquiry with the LAN/WAN technician regarding detection and resolution of failed hardware problems and use of the network monitoring software. Inspected e-mails received by the LAN/WAN technician to confirm notification of hardware failures.	No exceptions noted.
A service agreement with DataServ, Inc. covers maintenance and failures on the network hardware and software.	Made inquiry with the director regarding the process of monitoring network hardware and software errors. Inspected the network maintenance agreement and payment information for service level, effective period, and payment.	No exceptions noted.
Data center equipment is covered by insurance.	Inspected the insurance policy and payment documentation for evidence of coverage.	No exceptions noted.

IT Operations - *Control Objective:* **Backup** - Up-to-date backups of programs and data should be available in emergencies.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Daily image backups of systems and data are performed Monday through Thursday for selected drives and directories. Friday image backups are performed for all drives and directories. Backups are automated and scheduled. The scheduler is part of the system startup.	Inspected the system startup procedure to confirm the scheduler was included in the startup. Inspected the scheduler procedures to confirm the "daily_backup" and "full_backup" jobs and the frequency of execution. Made inquiry with the director regarding the review of backup logs for successful completion. Inspected an example of the daily and full backup logs, and backup command procedure for successful completion of backups.	No exceptions noted.
Backup tapes are stored in a secure on-site location and rotated to a secure off-site location regularly.	Made inquiry with the technical secretary/assistant regarding duration for retaining backup tapes and the backup tape rotation schedule. Observed backup tape rotation to the off-site storage location. Inspected the on-site and off-site storage locations for proper tape rotation.	No exceptions noted.

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

CENTER DATA

Name:	Western Ohio Computer Organization (WOCO)
Number:	7
Node Name:	WOCOA
Chairperson:	Larry Ludlow Superintendent Ft. Loramie Local SD
Fiscal Agent User Organization:	Shelby County Educational Service Center
Administrator:	Lewis ”Sonny” Ivey (SONNY) Director WOCO
Address:	129 East Court Street, 1st Floor Sidney, OH 45365
Telephone:	937-498-2161
FAX:	937-497-7233
Web Site:	www.woco-k12.org

OTHER CENTER STAFF

Charlie Rhyan	Assistant director
Donn Walls	Technology manager
John Demotte	LAN/WAN technician
Steve Bostic	LAN/WAN technician
Marcy Roll	SIS/EMIS support liaison
Stacy Gratz	Fiscal support liaison
Bridgett Wick	Technical secretary/assistant
Julie Ellis	SIS support liaison/Computer technician
Mike Wagner	Computer technician
Mary Copeland	SIS/EMIS/liaison
Pam Mohler	EMIS support liaison
Tom Hill	Part-time computer technician
Andy Kemmer	SIS/EMIS support liaison
Tom Walter	LAN/WAN technician

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit

Model Number		Installed		Capacity/Density/Speed	
CPU:	Compaq Alpha Server 8200	Lines/Ports:	N/A	Memory Installed:	3 GB
Disk:	RAID MA8000	Units:	6	Total Capacity:	108 MB
Disk:	R229B	Units:	1	Total Capacity:	2 MB
Disk:	R21EF	Units:	3	Total Capacity:	48MB
Tape Unit:	TSZ07	Units:	1	Max Density:	6250 BPI
Tape Unit:	TZ87	Units:	1	Max Density:	6400 BPI
Printer:	LG06	Units:	1	Print Speed:	600 LPM

USER ORGANIZATION CENTER DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
045930	Auglaize County EXC	Auglaize	X	X	X	X
045948	Minster Local SD	Auglaize	X	X	X	X
045955	New Bremen Local SD	Auglaize	X	X	X	X
045963	New Knoxville Local SD	Auglaize	X	X	X	X
045971	Waynesfield-Goshen Local SD	Auglaize	X	X	X	X
046193	Graham Local SD	Champaign	X	X	X	X
046185	Madison-Champaign ESC	Champaign	X	X	X	X
045484	Mechanicsburg Exempted Village SD	Champaign	X	X	X	X
046201	Triad Local SD	Champaign	X	X	X	X
046219	West Liberty-Salem Local SD	Champaign	X	X	X	X
044941	Urbana City SD	Champaign	X	X	X	X
047480	Hardin County ESC	Hardin	X	X	X	X
047498	Hardin Northern Local SD	Hardin	X	X	X	X
044172	Kenton City Schools	Hardin	X	X		X
047506	Ridgemont Local SD	Hardin	X	X	X	X
047514	Riverdale Local SD	Hardin	X	X	X	X
047522	Upper Scioto Valley Local SD	Hardin	X	X	X	X
048058	Logan County ESC	Logan	X	X	X	X
048074	Benjamin Logan Local SD	Logan	X	X	X	X
048082	Indian Lake Local SD	Logan	X	X	X	X
048090	Riverside Local SD	Logan	X	X	X	X

USER ORGANIZATION CENTER DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
051334	Ohio Hi-Point Career Center	Logan	X	X	X	X
062125	Upper Valley Career Center	Miami	X	X	X	X
049742	Shelby County ESC	Shelby	X	X	X	X
049759	Anna Local SD	Shelby	X	X	X	X
049767	Botkins Local SD	Shelby	X	X	X	X
049775	Fairlawn Local SD	Shelby	X	X	X	X
049783	Fort Loramie Local SD	Shelby	X	X	X	X
049791	Hardin-Houston Local SD	Shelby	X	X	X	X
049809	Jackson Center Local SD	Shelby	X	X	X	X
049817	Russia Local SD	Shelby	X	X	X	X
000288	Auglaize County Education Academy	Auglaize	X			X
000287	Auglaize County Spec. Needs School	Auglaize	X			X
151084	Graham Academy	Champaign	X			X
149062	Urbana Academy	Champaign	X			X
043588	Bellefontaine City Schools	Logan				X
044784	Sidney City Schools	Shelby	X	X		X
TOTALS:			**36**	**32**	**30**	**37**

Mary Taylor, CPA
Auditor of State

WESTERN OHIO COMPUTER ORGANIZATION (WOCO)

SHELBY 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 27, 2009

88 E. Broad St. / Fourth Floor / Columbus, OH 43215-3506
Telephone: (614) 466-4514 (800) 282-0370 Fax: (614) 466-4490
www.auditor.state.oh.us