TRI-RIVERS EDUCATIONAL COMPUTER ASSOCIATION (TRECA)
STATE REGION - ISA, MARION COUNTY

SAS - 70

AUGUST 4, 2007 THROUGH AUGUST 1, 2008

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
Tri-Rivers Educational Computer Association (TRECA)
100 Executive Drive
Marion, Ohio 43302

To Members of the Board:

We have examined the accompanying description of controls of the Tri-Rivers Educational Computer Association (TRECA) 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 TRECA'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 TRECA's controls; and (3) such controls had been placed in operation as of August 1, 2008. The TRECA 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 TRECA, 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 TRECA 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 TRECA's controls that had been placed in operation as of August 1, 2008. 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 TRECA'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 August 4, 2007 to August 1, 2008. 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 TRECA 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 August 4, 2007 to August 1, 2008.

The relative effectiveness and significance of specific controls at the TRECA 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 TRECA to provide additional information and is not part of the TRECA'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 TRECA is as of August 1, 2008, and information about tests of the operating effectiveness of specified controls covers the period from August 4, 2007 to August 1, 2008. 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 TRECA 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 TRECA, its user organizations, and the independent auditors of its user organizations.

Mary Taylor

Mary Taylor, CPA
Auditor of State

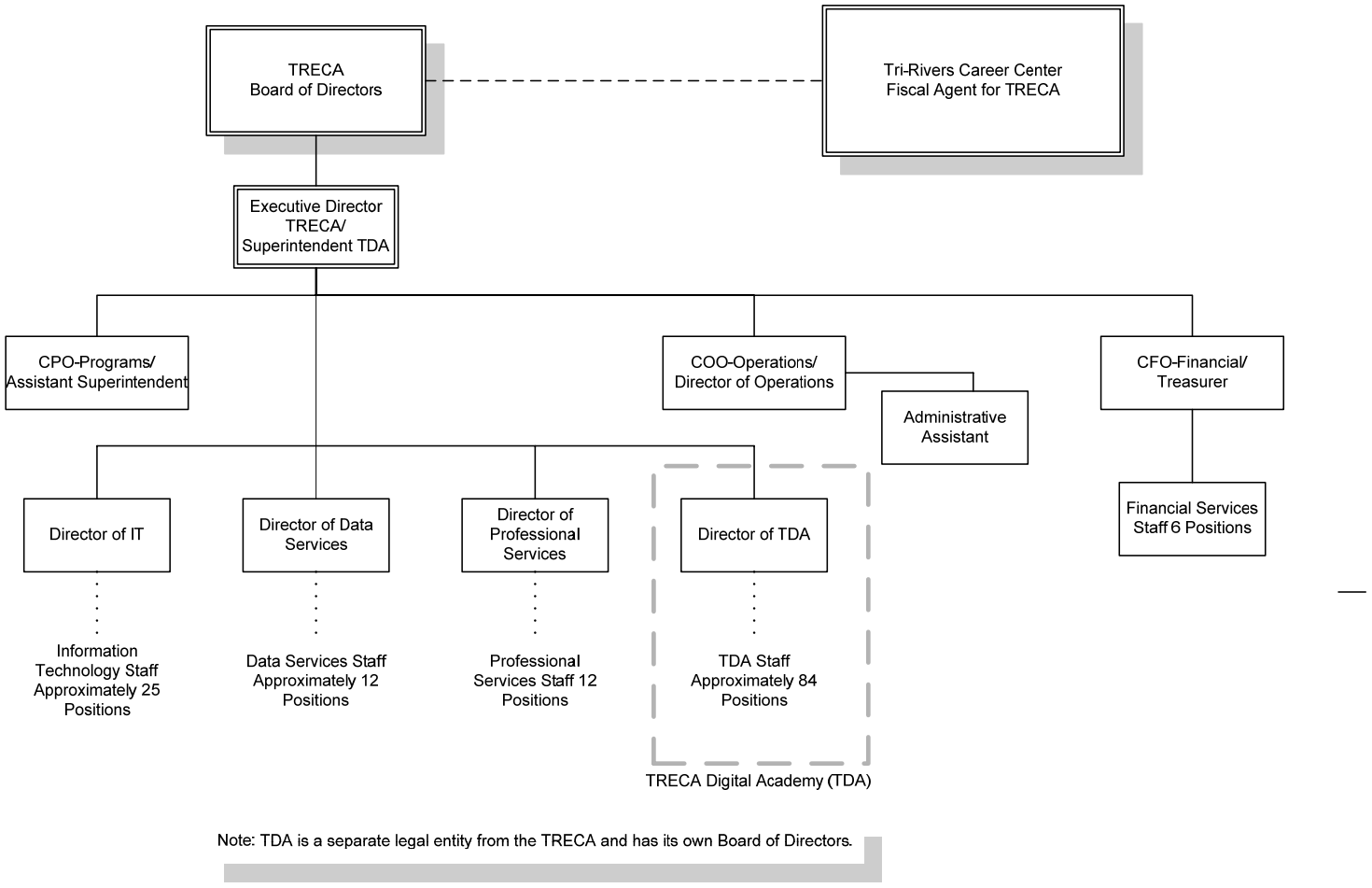
August 1, 2008

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The TRECA'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 TRECA's description of controls.

OVERVIEW OF OPERATIONS



The TRECA is one of 23 not-for-profit computer service organizations serving more than 740 educational entities and 1.2 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 TRECA 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).
- Community School Average Daily Membership (CSADM).

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. The TRECA is organized under Chapter 167.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the TRECA board of directors. A general assembly, consisting of one delegate from each voting member user organizations, acts as the deliberative and advisory body of the COG. The general assembly will meet at least twice per year to make recommendations to the board of directors about estimated program costs, annual budgets, selection of officers, and any other matters referred to them by the Board.

The board of directors is the governing body of the TRECA and is responsible for transacting all business and administering all programs. The board of directors consists of nine voting members made up of seven superintendents from the eleven member counties, a superintendent from one of the user organizations and the superintendent from the fiscal agent. The board of directors meets monthly.

The TRECA employs a staff of approximately 63 individuals, not including the TRECA Digital Academy, and is supported by the following functional areas:

Treasurer & Business Manager: Works with the board of directors in all budget aspects for TRECA.

Information Technology: Supports the TRECA computer systems and its networked communication system; along with providing user training and support.

Data and Research: Comprises the following functional areas:

Data and Research: Provides the TRECA user organizations with support for data storage and researching of problems with data records. Additionally, provides data storage on CD for those user organizations requesting it.

State Software-Fiscal Support: Provides end-user support to user organizations with support for fiscal concerns using state software applications, including USAS, USPS, SAAS/EIS, and EMIS.

Professional Development: Provides a variety of educational technology services to subscribing TRECA user organizations including software and Internet access, training, technology planning, technical assistance, and grant writing assistance.

Student Services: Facilitates the implementation and operation of the student services of the TRECA including EMIS and provides user training and support.

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

The TRECA 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 TRECA employees may alter user data and only at the request of the user organization.

The TRECA has established personnel policies and procedures. When necessary, additional TRECA policies have been developed and approved by the board of directors to address concerns of TRECA. The TRECA is in the process of rewriting all job descriptions; consequently, revised job descriptions exist for the majority of positions. The TRECA is constantly re-evaluating its need for personnel to provide for the increasing range of services provided and to foster efficiency within its organization. The reporting structure and job descriptions are periodically updated to create a more effective organization.

The TRECA 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 TRECA 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 approved professional development continuing educational units (CEU) annually and at least eight approved CEUs 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 65% of incurred costs in attending additional professional development seminars. Employee evaluations are conducted annually. The board of directors performs an annual evaluation of the executive director.

Risk Assessment

Although the TRECA does not have a formal risk management process, the board of directors is comprised of representatives from the member user organizations who actively participate in the oversight of the TRECA. As a regular part of its activity, the board addresses:

- New technology.
- Realignment of the TRECA 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 TRECA has identified operational risks resulting from the nature of the services provided to the member 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 TRECA organization is structured so that managers of each department report directly to the executive director. Key management employees have worked for TRECA for many years and are experienced with the systems and controls at the TRECA. The TRECA executive director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, the TRECA uses a variety of "key indicator" reports to monitor the processes involved in processing transactions for user organizations.

Hardware, software, network performance, 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.

The TRECA monitors its quality of service to user organizations through user organization satisfaction meetings. The professional development director and IT director hold these meetings annually for each user organization.

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" sections.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

The TRECA staff does not perform system development activities. Instead, the TRECA 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 Ohio Educational Computer Network (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

Application enhancements and modifications are initiated through the Software Performance Report/Request (SPR) tracking procedure, which is maintained by the SSDT. The SPR system utilizes SiteScape Forum, layered products for electronic conferencing, which are used to accept and discuss proposed software enhancements in a public forum. The forum is divided into Public and ITC. Each major software package (USAS, USPS, SAAS, EMIS) has its own Public and ITC forum which is monitored by the SSDT system analysts. Public is used by user organization personnel and the ITC forum is used by the ITC personnel. ITC and a majority of user organization personnel have access to forum conferences, providing end-user participation in the program development/change process.

The TRECA 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 ITC's 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 distributed with these releases. The SSDT informs the ITC that they will support only the latest release of the state software beginning 30 days following the software release date.

The TRECA 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 ITC's 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 ITC's 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 sites 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.

Documentation for the current version of the OpenVMS operating system and new releases are provided on the HP web site. New releases include documented changes to the operating system and implementation procedures. In addition, the TRECA has purchased a copy of the operating system disks from INS, a third-party vendor in partnership with the MCOECN. This is part of the Technology Solutions Group program under the MCOECN (mc•tsg). The TRECA is able to purchase the operating system software at a reduced cost under this program.

IT Security

The TRECA staff is required to complete a written "Authorized Account Application Form" to gain access to the system. The TRECA 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 is established, granted and reviewed by the systems manager or the systems assistant.

Users from the user organizations are granted access upon the receipt of a written "Authorized Account Application Form." The form must be authorized by the appropriate user organization management before a user account may be created or updated. Either the systems manager or a designee will create, update, or delete the account and e-mail the appropriate user organization designee regarding the request made. The TRECA maintains a file of all requests made by the individual user organizations.

Through an automated procedure user account activity is monitored on a monthly basis. Accounts on the system that have not been logged into for over 180 days are automatically disabled and reviewed by the systems manager monthly. If the account is determined to be old and unused it is deleted from the system.

Annually, the systems manager sends an e-mail to each user organization listing all corresponding accounts and access rights and requests the user organizations to confirm the appropriateness of the accounts. If a user organization does not respond, the systems manager sends a follow-up e-mail until a response is received.

The TRECA has security policies and procedures in place outlining the responsibilities of user organization personnel, the TRECA personnel and any individual or group not belonging to either the user organizations or the TRECA. In addition, the TRECA utilizes a banner screen that is displayed before a user logs in and after a user successfully logs on to the system. The screen informs the user that by connecting to the system they expressly consent to the security policies of the TRECA.

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 and alarms to the operator log file. Access to the audit log and the operator log is limited to data processing personnel. The following detection control audits and/or alarms have been enabled through OpenVMS to monitor any security violations:

ACL:	Gives file owners the option to selectively alarm certain files and events. READ, WRITE, EXECUTE, DELETE or CONTROL modes can be audited.
AUDIT:	Enabled by default to produce a record of when other security alarms were enabled or disabled.
AUTHORIZATION:	Enables monitoring of changes made to the system user authorization file, UAF, or network proxy authorization file in addition to auditing 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.
FILE ACCESS:	Audit file protection violations: READ, WRITE, EXECUTE and DELETE violations 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.
MOUNT:	Produces a record of MOUNT or DISMOUNT requests.

The security monitor report is e-mailed daily to the systems manager for review. The security monitor procedure monitors the system audits file entries for the previous day and uses e-mail to send a report to the systems manager. The systems manager reviews the security monitor report to determine if any suspicious events have occurred. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and the corrective action needed. The systems manager maintains these reports in his e-mail directory for about one month. In addition, the reports are archived and are available since the implementation of the system.

The TRECA utilizes Sophos anti-virus software on an external e-mail gateway to scan all inbound and outbound e-mail. Virus definitions are updated daily. Additionally, infected e-mail is quarantined.

Security provisions of the operating system provide primary logical access control to the HP computers. 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. The system manages access to the process information using its authorization data and internal security mechanisms.

The TRECA 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.

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

Each user is subject to a minimum password length established by management. The system forces users to periodically change their passwords. The systems manager uses a unique password scheme for all new users. This method of assigning passwords does not require using pre-expired passwords.

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.

System parameter standards have been established through the use of HP established defaults. Any changes are logged and reviewed by the systems 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 then defaults to User Identification Code (UIC) based protection. The system uses UIC based protection to control access to objects such as files, directories and volumes. TRECA 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 member number under that group.

The system directory contains security files that control the security parameters on the system. When a user attempts to gain access to an object, such as a file or directory, the system compares the 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, OWNER, GROUP and WORLD.

Through the protection code, each category of user 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. UIC-based protection prevents WORLD, WRITE or DELETE access to USAS, USPS, SAAS/EIS and EMIS application production and data files.

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.)

Access to the OECN software packages is controlled at the ITC level by granting the appropriate 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 that grants access privileges to all state developed software is restricted to authorized TRECA staff.

To limit access to security files, the TRECA 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 main switch is restricted through password protection. Additionally, remote access is automatically denied for users physically outside the firewall.

The main doors to the building are secured when the building is not in use. The computer room is located within the TRECA offices. Access to the computer room requires a keyless entry code which is known only to key TRECA staff. The doors leading to the TRECA offices are secured during non-business hours and the computer room is locked at all times.

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

.

- UPS backup power supply.
- Smoke detector.
- Fire extinguisher.
- Temperature control system.

IT Operations

Traditional computer operations procedures are minimal because users at the user organizations initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All TRECA employees have access to a procedures manual, which provides directions and guidelines for most of the operational functions performed. They also have access to operations procedure manuals for the system. In addition, all users, except students, have access to SiteScape Forum, which is a bulletin board that allows the TRECA employees to communicate with users across the state. Users can post questions and/or comments to the TRECA staff.

TRECA 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' personnel requests in resolving data entry errors. Errors are discovered by the user organizations in their balancing procedures. In addition, the user organizations may view or print out an "AUDIT" report that shows all activity changes to the data file made through the application. Changes made directly to the data file are not reflected in the "AUDIT" report. TRECA requires user organizations to formally request changes to data files outside the application. These requests are maintained to track changes made to the data outside the application.

TRECA has a hardware maintenance agreement with HP which is in effect during standard office hours. Problems related to the HP systems are logged by the employee responding to the call. Problems with communication lines are communicated via e-mail to the vendor.

Certain routine batch jobs can be initiated at the TRECA for system maintenance. The TRECA is responsible for some operational maintenance tasks, such as: system backups, file rebuilds, database integrity testing, log reports, and other maintenance directed at the system as a whole. The TRECA helps to prevent database failure or corruption through the use of a program called REORG that is run through the Scheduler. Scheduler is a program that continually submits jobs on the system.

Common problems that arise daily, such as terminal lockups and program crashes are usually handled by the TRECA service representatives over the phone and may not be documented if the problem was minor. Some problems are logged through e-mail that is sent to service representatives. Critical problems such as login failures, system failures, or break-in attempts are reviewed daily by the systems manager.

The TRECA utilizes Servers Alive software to monitor their network systems. While running, Servers Alive shows all the routers for the system on screen. If the Servers Alive does not receive a response from a certain device, the device will be highlighted in red on the screen. The level of the problem will determine the action taken by the TRECA staff. If the problem is major, such as a malfunctioning router, the TRECA will contact the user organization to resolve the matter quickly as possible. For minor problems, such as a switch device, the TRECA will prioritize and schedule maintenance.

The TRECA has a formal backup policy in place. Full system backups of all user directories are performed weekly. Full system backups of all data and programs are performed daily and weekly, with tapes being rotated off-site Monday through Friday. About eight weeks of backup tapes are maintained in the backup rotation. A tape library log is maintained to track the tapes.

TRECA stores on-site back-up tapes in a fireproof safe located within the data center. The TRECA rotates its backup tapes to a safe deposit box at a local bank. At year-end, all user files and programs are backed up and stored. All year-end backups are kept for five years, with the most recent being stored off-site. Older year-end backups are kept in the on-site, fireproof safe. All data processing equipment is covered under an insurance policy.

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

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

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Changes to Existing Applications and Systems

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
In order to maintain continued support of the application software provided by 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 confirm the USAS, USPS, SAAS, and EMIS software versions tested at NWOCA are the same versions used at TRECA.	No relevant exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements, and problems corrected. Updated user and system manuals for the applications are also made available.	Inspected the release notes for the most recent application releases. Inspected the SSDT web-site for availability of updated manuals.	No exceptions noted.
The TRECA participates in the CSLG/ESL program, which provides software upgrades and related documentation.	Inspected a checklist maintained by the NWOCA to track receipt and payment of the CSLG/ESL agreements for each ITC.	No exceptions noted.
In order to maintain continued support of their application software provided by the SSDT, the TRECA is required to install new releases of the operating system.	Observed the online documentation at the HP web site, http://www.hp.com/go/openvms/doc/. Also, inspected the install instructions and OpenVMS 8.3 documentation that came with the upgrade.	No exceptions noted.
User Control Consideration(s): User organizations should maintain current service level agreements with the TRECA for USAS, USPS, EMIS, SAAS, and technical support.		

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 TRECA requires a standard form for user authorization. The authorization form must be signed by the appropriate user organization management before adding a user account on the system. In addition, the authorization form lists the level of access requested.	Utilized a third-party audit software package to identify the population of accounts during the audit period. Selected 60 of 1,795 accounts. Inspected the associated Authorized Account Authorization Form's and/or confirmation for each selected item to confirm proper authorization by the treasurer and/or superintendent. In addition compared the access level granted per the request form with the actual access level granted per the system user authorization file.	15 of 60 forms or 25% did not exist 6 of the 45 forms located had different access to the ALPHA than requested per the form.
Annually, the TRECA system manager generates and sends a listing, per user organization, of user accounts and associated access rights. In addition, each month the TRECA system manager generates a listing of unused accounts. The system manager reviews these listings and deletes all unnecessary accounts.	Made inquiry with the system manager regarding the confirmation procedures. Inspected the script that is run monthly by the system manager to generate an Unused Account Listing of accounts which have not been logged into for greater than one year.	The TRECA did not send a confirmation to the user organizations during the audit period. No other exceptions noted.
The tracking of security related events such as break-in attempts and excessive login failures are enabled through OpenVMS for the system. The events are logged to audit journals to monitor potential security violations.	Inspected the security alarms and audits enabled. Made inquiry with the system manager regarding the review of audit journals to confirm the journals were reviewed.	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:*
Security violations are extracted, compiled into summary and detailed security reports, and emailed to the systems manager nightly through OpenVMS command procedures on the system. Daily, the reports are reviewed for login failures, break-in attempts, and changes to the user authorization file. The command procedures are automatically resubmitted to the system daily.	Inspected the security report and operator log. Inquired with the system manager of software applications and support regarding the report review process.	No exceptions noted.
Anti-virus software runs on the external email gateway to help protect against computer viruses. Definitions are updated hourly, and infected items are quarantined to help prevent and detect computer viruses.	Inspected the definitions in the anti-virus update log and anti-virus settings to confirm the TRECA systems were protected from viruses.	No exceptions noted.

User Control Considerations:

User organization management should make users aware of the confidential nature of passwords and the precautions necessary to maintain their confidentiality.

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

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

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.

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 accounts.	Utilized a third-party audit software package to identify the following within the system user authorization file: • User accounts that have not been used in at least 180 days. • User accounts that have never logged in. Inspected the listed accounts and inquired with the systems manager as to the purpose and appropriateness of the accounts.	No relevant exceptions noted.
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts are specifically defined to not allow blanket access.	Inspected the results of the SHOW/PROXY command for the use of wild card characters.	No exceptions noted.
Access to the system command line (DCL) is restricted to authorized users.	Utilized a third-party audit software package to identify user accounts which do not have the Audit, Captive, Disctly, Disuser or Restricted flags set within the system user authorization file. Inspected the listed accounts and confirmed the appropriateness of accounts with the system manager.	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:*
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 TRECA. The number of profiles with pre-expired passwords is limited.	Using a security analysis tool, extracted information from the user authorization file to identify: • User accounts with a password minimum length less than TRECA's standard. • User accounts with a password lifetime greater than TRECA's standard. • User accounts with pre-expired passwords. Inspected the above exception reports to identify relevant exceptions. Also inspected the default account parameters.	No relevant exceptions noted.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameter settings.	No exceptions noted.
A program 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 whether the HITMAN program was part of the startup procedures.	No exceptions noted.
Access to production data files and programs is restricted to authorized users.	Using a security analysis tool, identified and inspected production data files with WORLD access and executable files with WORLD write and/or delete 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 layer 3 switch are used to control Internet traffic and maintain a logical segregation between user organizations.	Made inquiry with the systems manager regarding the network diagram to confirm components of the network which control Internet access. Inspected the firewall and main switch configurations to confirm: • All Internet traffic was switched to/from the firewall. • Inbound and outbound IP traffic is restricted through the firewall. • Inspected the firewall configuration for inbound and outbound control lists and for existence of a private internal network.	No exceptions noted.
Individual user profiles are used to grant access rights and privileges for the system. The user profiles on the system do not consist of an excessive number of elevated privileges accounts.	Utilized a third-party audit software package to identify the following within the system user authorization file: • User accounts with group privileges. • User accounts with devour privileges. • User accounts with system privileges. • User accounts with objects privileges. • User accounts with all privileges.	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.	Inspected reports listing all accounts with OECN identifiers for evidence of the use of identifiers to segregate access to the applications.	No exceptions noted.
The OECN_SYSMAN identifier grants all access privileges for all state developed applications and is restricted to authorized users.	Inspected a listing of user accounts assigned the OECN_SYSMAN identifier. Made inquiry with the system manager regarding the appropriateness of accounts assigned the OECN_SYSMAN identifier.	No exceptions noted.
User Control Consideration: User Identification Codes (UICs), passwords and associated access privileges should only be issued to authorized users who need access to computer resources to perform their job function.		

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.

IT Security - *Control Objective:* **System Software and Utilities Access Controls** - Use of master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
System level user identification codes are restricted to only authorized personnel.	Identified the maximum system group number through the System Generation (SYSGEN) Utility Utilized a third-party audit software package to identify a listing of all accounts with a UIC less than the maximum system group number. Inquired with the systems manager as to the appropriateness of identified accounts.	No exceptions noted.
Use of an alternate user authorization file is not permitted.	Inspected the value of the alternate user authorization file parameter to confirm an alternate file is not permitted. Inspected the system directory listings for existence of an alternate user authorization file.	No exceptions noted.
Remote access to firewall and router configurations used to control Internet access are restricted through password protection.	Inspected the firewall and main switch configurations to confirm remote administration was permitted and 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 using keypad entry devices. Key pad entry device access codes are change periodically.	Observed use of the key pad entry devices throughout the period of fieldwork to confirm access is restricted to authorized personnel. Inquired with the systems manager about the periodic changing of the key pad entry device access codes to confirm key codes are periodically changed.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, water, or changes in temperature.	Inspected the TRECA data center with the systems manager to confirm the existence of appropriate environmental controls used to detect and prevent environmental issues.	No exceptions noted.
User Control Considerations: 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. Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.		

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:*
TRECA maintains a hardware service agreement with HP to cover hardware maintenance and failures.	Inspected the HP hardware service agreements and purchase orders for an effective date, service level, unit/monthly price, and period of coverage.	No exceptions noted.

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:*
Routine system maintenance programs, such as purging of e-mail, reorganizing of application files, and analyzing files, are run to help prevent file failure and data corruption. In addition, the programs are included in the scheduler and the scheduler is included in the system startup.	Inspected the system startup procedures for the scheduler to confirm the scheduler is initiated at system startup. Inspected the scheduled programs in the scheduler to confirm routine system maintenance programs are automatically scheduled to execute. Additionally, confirmed the jobs were successful and if an error did occur, an email was sent to inform the appropriate TRECA personnel.	No exceptions noted.
The software "Servers Alive" monitors network performance and alerts staff of hardware failures.	Inspected a system status screen for Servers Alive to confirm network monitoring information is provided by the application. Inquired with the systems manager regarding network monitoring and confirmed how errors noted through Servers Alive are resolved.	No exceptions noted.
Data center hardware and software is covered by an insurance policy.	Inspected the property insurance policy and proof of payment to confirm TRECA equipment is insured in the event of a disaster.	No exceptions noted.
Requests for changes to user organization data must be authorized by the user organization via e-mail or in writing.	Inspected all user organizations for documentation of requests on file for the 2008 fiscal year. Inquired with TRECA staff regarding the procedures for changing user data.	No relevant 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:*
Incremental backups of programs and data are performed nightly Monday through Thursday. Additionally, full backups of systems and data are performed weekly on Fridays. All backups are automated and are scheduled. The scheduler is part of the system startup.	Confirmed backup procedures with the systems manager and systems assistant. Inspected the scheduler and startup procedures to confirm backups are executed regularly.	No exceptions noted.
Backup tapes are stored in a secure on-site location and rotated to a secure off-site location regularly.	Confirmed backup tape rotation, policy and retention procedures with the systems assistant. Observed the backup tape rotation to the off-site storage location. Toured the off-site storage location and inspected the sign in sheet for the safe deposit box. Inspected the backup tape listing and compared the listing to backup tapes stored at the on-site and off-site locations.	No exceptions noted.
User Control Considerations: 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. The user organization should establish and enforce a formal data retention schedule with their ITC for the various application data files.		

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

CENTER DATA

Name:	Tri-Rivers Educational Computer Association (TRECA)
Number:	16
Node Name:	TRECA
Chairperson:	Douglas Ute Superintendent Elgin Local Schools
Fiscal Agent District:	Tri-Rivers Career Center
Administrator:	Michael Carder Executive Director TRECA
Address:	100 Executive Drive Marion, OH 43302
Telephone:	740-389-4798
FAX:	740-389-4517
Web site:	www.treca.org

OTHER SITE STAFF

Sherry Albright	Assistant database administrator
Mark Ames	IT director
Scott Armstrong	Treasurer
Kevin Becker	Database developer
Shelly Beidelscheis	Fiscal services secretary
Judy Benner	INFOhio liaison
David Cartwright	Student services liaison
Bob Casey	Director of professional services
Adam Clark	Professional development liaison
Sean Coldiron	Technical liaison
Ryan Cook	Fiscal services liaison
Marla Edington	Systems assistant
Lisa Eckleberry	Director of EMIS
Eric Elsasser	Technical liaison
Paul Elswick	Technical liaison
Chuck Falter	Director data services
Dan Foss	Cisco academy
Stacie Hankins	Business manager's secretary
Chelsea Hardin	Student services liaison
Daryl Hartzler	Technical liaison
Dave Henshaw	Fiscal services liaison
Corey Hilliard	Technical liaison
Robert Howard	Professional development liaison
Cherri James	Inventory and receiving coordinator
Thomas Johnston	Technical liaison
Pamela Keefer	TDA CSADM coordinator/EMIS
David Kirkton	N.E. regional director
Bill Kollas	Technical liaison
Vernon Kollas	Technical liaison
Ryan Konkle	Systems assistant
Gary Koons	Business manager
Heather Koren	Student services liaison
Dustin Kraus	Online developer
Kevin Langdon	Technical liaison
Mike Medek	Technical liaison
Chuck Merkle	Coordinator of data and research
Brianna Miller	Marketing coordinator
James Montis	Technical liaison
Matthew Mowry	Technical liaison
Thomas Mustain	Technical liaison
Matt Newell	Systems assistant
Tammy North	Gradebook coordinator
Ken Papay	Fiscal services liaison
Mark Papenhausen	Database developer
Kevin Perkins	Systems manager
Carol Pfeiffer	Student services liaison
Linda Ratliff	Assistant treasurer
Mike Ring	Social services coordinator
Sue Ritzler	Coordinator of partnership services
Jennifer Schmidt	Data services assistant director
Eric Seitz	Technical liaison
John Shank	Assistant superintendent
Jeff Sharp	N.W. regional director
Cyrstal Shoemaker	Student services coordinator
David Shoffner	Technical liaison
Matt Tillett	Asst dir information technical services
Jeremy Vaught	Technical liaison
Michael Voss	Coordinator of professional development
Joe Wildenthaler	Project manager
Melanie Wilson	Computer systems investigator
Brian Wood	Technical liaison
James Wright	Angel management and internet librarian

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit

Model Number		Installed		Capacity/Density/Speed	
CPU:	Compaq Alpha ES40	Lines/Ports:	N/A	Memory Installed:	4 GB
Disk:	DS-RZIDF-VW	Units:	9	Total Capacity:	82 GB
Disk:	DS-RZIFC-VW	Units:	13	Total Capacity:	364 GB
Tape Unit:	TL891DLX Minilibrary	Units:	1	Max Density:	40/80(compress)
Printer:	LG06	Units:	1	Print Speed:	9600 LPM

USER ORGANIZATION DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
043687	Bucyrus City Schools	Crawford	X	X	X	X
046748	Big Walnut LSD	Delaware	X	X	X	X
046755	Buckeye Valley LSD	Delaware	X	X	X	X
043877	Delaware CSD	Delaware	X	X	X	X
050989	Delaware JVSD	Delaware	X	X	X	X
046730	Delaware-Union ESC	Delaware	X	X	X	X
046763	Olentangy LSD	Delaware	X	X	X	X
046995	Plain Local/New Albany LSD	Franklin			X	X
046896	Pickerington	Fairfield			X	X
051060	Great Oaks Institute of Technology	Hamilton			X	X
047829	Centerburg LSD	Knox	X	X	X	X
047837	Danville LSD	Knox	X	X	X	X
047845	East Knox LSD	Knox	X	X	X	X
047852	Fredericktown LSD	Knox	X	X	X	X
047811	Knox ESC	Knox	X	X	X	X
048413	Elgin LSD	Marion	X	X	X	X
044339	Marion CSD	Marion	X	X	X	X
048421	Pleasant LSD	Marion	X	X	X	X
048439	Ridgedale LSD	Marion	X	X	X	X
048447	River Valley LSD	Marion	X	X	X	X

USER ORGANIZATION DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
065268	Tri-Rivers CC	Marion	X	X	X	X
085647	Tri-Rivers Educational Compute	Marion	X	X		
048793	Cardington-Lincoln LSD	Morrow	X	X	X	X
048801	Highland LSD	Morrow	X	X	X	X
045534	Mount Gilead EVSD	Morrow	X	X	X	X
048835	East Muskingum LSD	Muskingum	X	X	X	X
045179	Zanesville CSD	Muskingum	X	X	X	X
045476	Marysville EVSD	Union	X	X	X	X
045260	Carey EVSD	Wyandot	X	X	X	X
050740	Mohawk LSD	Wyandot	X	X	X	X
047985	Johnstown – Monroe LSD	Licking	X	X	X	X
045625	Upper Sandusky EVSD	Wyandot	X	X	X	X
000593	Delaware Practical Arts Academy	Delaware	X			
148932	Franklin Digital Academy	Fairfield	X		X	X
000591	New Albany Academy for Performing Arts	Franklin	X	X		
000592	New Albany Elementary Performing Arts Academy	Franklin	X	X		
134080	Eagle Heights Academy	Mahoning	X	X	X	X
148916	Marion City Digital Academy	Marion	X		X	X
151035	Pleasant Community Digital	Marion	X		X	X
151167	Ridgedale Community School	Marion	X		X	X

USER ORGANIZATION DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
151043	River Valley Digital Academy	Marion	X		X	X
143305	TRECA Digital Academy	Marion	X	X	X	X
151076	Cardington Digital Academy	Morrow	X		X	X
149047	GOAL Digital Academy	Morrow	X		X	X
148981	Tomorrow Center	Morrow	X		X	X
000292	East Muskingum Digital Academy	Muskingum	X		X	X
TOTALS			43	33	42	42

Mary Taylor, CPA
Auditor of State

TRI-RIVERS EDUCATIONAL COMPUTER ASSOCIATION (TRECA)

TRUMBULL 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
OCTOBER 9, 2008

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