LICKING AREA COMPUTER ASSOCIATION (LACA)
STATE REGION - ISA, LICKING COUNTY

SAS - 70

AUGUST 25, 2007 THROUGH JULY 18, 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
Licking Area Computer Association (LACA)
195 Union Street, Suite C-2
Newark, Ohio 43055

To Members of the Board:

We have examined the accompanying description of controls of the Licking Area Computer Association (LACA) 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 LACA '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 LACA's controls; and (3) such controls had been placed in operation as of July 18, 2008. The LACA 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 ITC, 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 LACA 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 LACA's controls that had been placed in operation as of July 18, 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 LACA'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 25, 2007 to July 18, 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 LACA 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 25, 2007 to July 18, 2008.

The relative effectiveness and significance of specific controls at the LACA 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 LACA to provide additional information and is not part of the LACA'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 LACA is as of July 18, 2008, and information about tests of the operating effectiveness of specified controls covers the period from August 25, 2007 to July 18, 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 LACA 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 LACA, its user organizations, and the independent auditors of its user organizations.

Mary Taylor

Mary Taylor, CPA
Auditor of State

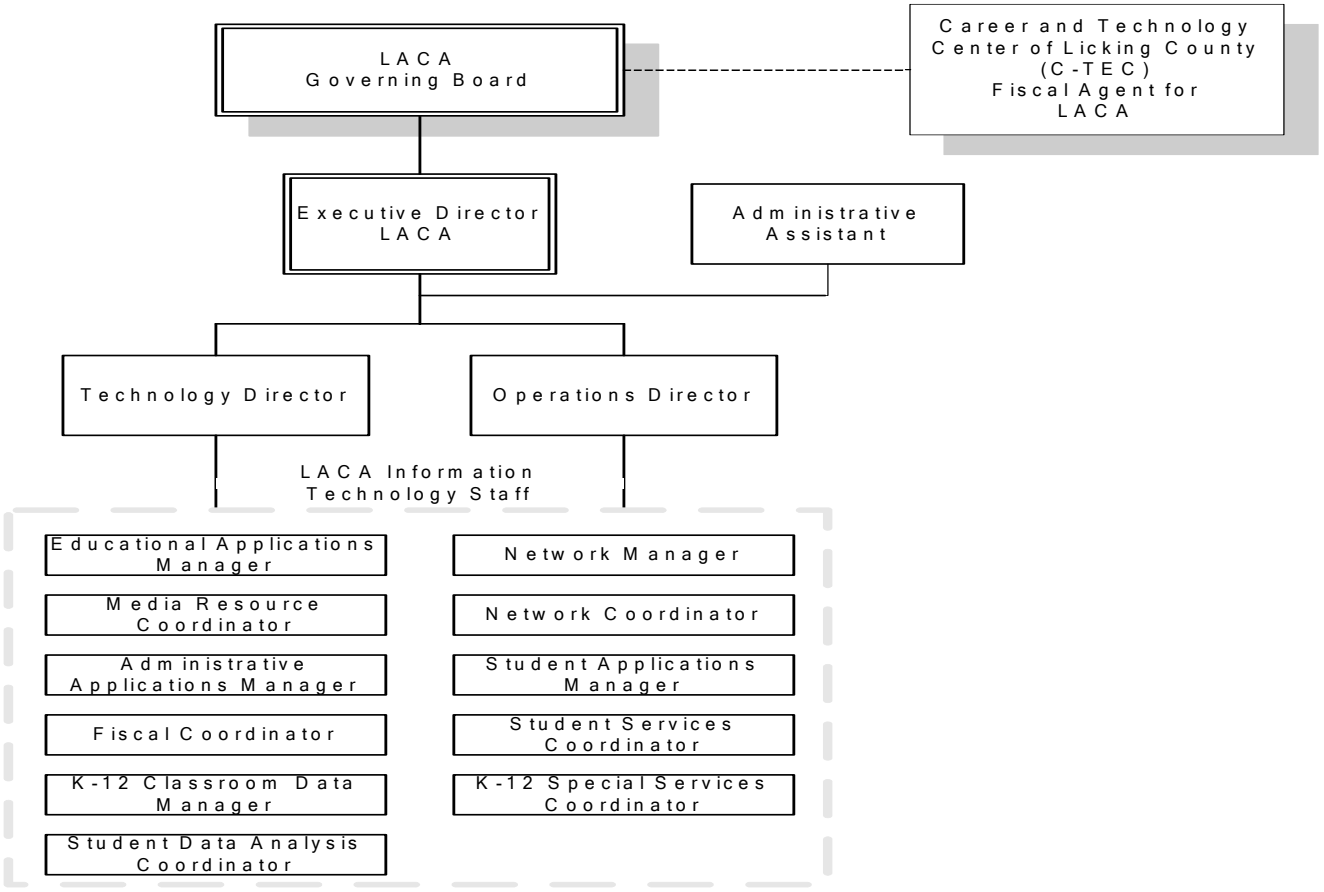
July 18, 2008

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The Licking Area Computer Association's (LACA) 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 LACA's description of controls.

OVERVIEW OF OPERATIONS



The LACA 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 LACA is derived from the state of Ohio and from user fees.

ITCs provide information technology services to user organizations, public 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 Councils of Government (COG) under ORC 167. ORC 3313.92 allows for user organizations 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 LACA is organized under section 3313.92. The Career and Technology Center of Licking County (C-Tec) serves as the fiscal agent for LACA.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the governing board. The governing board is the governing body of LACA and is composed of fifteen members, one Superintendent from each member district served by LACA. The board is required to meet bi-monthly, with additional meetings as necessary. The board has also established several sub-committees to assist in the operation of the LACA.

The LACA employs a staff of 15 individuals and is supported by the following functional areas:

Fiscal Administration Services: Provides end user support and training for all fiscal service applications, including USAS, USPS, and SAAS/EIS.

Technical WAN Services: Supports the LACA computer systems and its networked communications systems. In addition, provides users a variety of educational technology services, including software and Internet access, e-mail, training, technology planning, and technical assistance.

Student Administration: Supports end users in all aspects of the student service applications with a focus on EMIS.

Library Services Support: Supports end users with library services programs.

The LACA is generally limited to recording user organization transactions and processing the related data. User organizations are responsible for authorization and initiation of all transactions. The LACA's management reinforces this segregation of duties as a part of its new employees' orientation process, through on the job training, and by restricting employee access to user data. User organizations rarely request LACA to make changes to their data once entered; however, when they do request it only experienced LACA staff members are allowed to make these changes. The LACA maintains a file of all approved changes for each user organization.

The LACA'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 require professional development and other training as a condition of continued employment. Each staff member must attend at least 15 hours of approved professional development training annually, and at least 80 hours of approved training every four years. Management permits and encourages staff members to obtain additional professional training as deemed necessary.

The LACA has documented their own personnel policies and procedures, separate from their fiscal agent. When necessary, these policies have been updated and approved by the LACA governing board to address new concerns. Detailed job descriptions exist for all positions. The reporting structure and job descriptions are periodically updated to create a more effective organization. Staff evaluations are conducted annually. In addition, the board performs an annual evaluation of the executive director.

Risk Assessment

The LACA does not have a formal risk management process; however, the governing board is comprised of representatives from the user organizations who actively participate in the oversight of the LACA. As a regular part of its activity, the board addresses:

- New technology.
- Realignment of the LACA 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 LACA 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 Control" section of this report.

Monitoring

The LACA organization is structured so that managers/coordinators of each functional area report directly to the executive director. The key management employees have worked for LACA for many years and are experienced with the systems and controls at the LACA. The 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, LACA 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 management. Some of these reports are automatically run through a scheduler program and are sent to management via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily. In addition, the executive director, the technology director, and the administrative applications manager receive the same reports and monitor them for interrelated and recurring problems.

INFORMATION AND COMMUNICATION

The aspects of the information and communication component of internal control as it affects the services provided to user organizations are discussed within the "General EDP Control" section.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and/or Systems

The LACA staff does not perform system development activities. Instead, the LACA utilizes the software developed and supplied by the State Software Development Team (SSDT), located at the Northwest Ohio Computer Association (NWOCA), another Information Technology Center (ITC) of the OECN. The ODE determines the scope of software development for state-supported systems. Tactical means of accomplishing software development priorities are determined by the Software Advisory Committee (SAC), which consists of members from the Management Council of the OECN (MCOECN), the Ohio Association of School Business Officials, 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 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 LACA 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 LACA uses a software utility, called OECN_INSTALL, to unpack these zipped files and install each individual package into its proper OECN directory. The OECN_INSTALL utility has two options which will either install the new release on the system or install a patch for the current release. This utility ensures that all required components are installed properly and consistently.

Only vendor supplied changes are made to the operating system or system software documentation. The Northern Buckeye Education Council (NBEC), who acts as the fiscal agent for this and other participating ITCs, has entered into a licensing agreement 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 board of trustees of the MCOECN.

- Provide telephone technical support to the participating ITCs' 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 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.

Before new releases are installed at the LACA, 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 and support for new releases of applications are provided by the SSDT. Application release notes are distributed with each quarterly release and are also available through the web site.

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 LACA 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 (TSG) program under the MCOECN. (Note: The VAR program was restructured in September 2006 and became the MC TSG) The LACA is able to purchase the operating system software at a reduced cost under this program.

IT Security

The LACA has a security policy in place that outlines the responsibilities of user organization personnel, LACA personnel, and any individual or group belonging to neither. Additionally, the LACA uses a banner screen that is displayed before a user logs onto the system. The screen informs the user that "unauthorized use may result in denial of future privileges, revocation of access to the system and/or prosecution under the law."

The LACA grants its staff 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. Data center access is established, granted and reviewed by the executive director and no authorization form is used.

User organizations are granted access through LAMA (LACA Account Management Application), a web-based workflow system for maintaining user access. Designated administrators in the user organizations enter requests for new accounts, access changes, or deletion of accounts. Each request is individually approved by the superintendent (or designee) through the LAMA web interface. If fiscal (USAS, USPS, etc) or EMIS access is requested, the treasurer (or designee) will need to approve the request in LAMA as well. After a request has the required district-level approvals, the request is then routed into the work queue of a LACA staff member to be completed. Different members of LACA's staff build accounts, remove accounts, or grant the access, depending on the service area (fiscal support grants fiscal access, Progress Book support grants Progress Book access, etc). After LACA marks the request completed, the original submitter of the request receives an automated e-mail letting them know it is complete. Each quarter, a representative of each user organization is e-mailed and asked to log into LAMA to audit and confirm the listing of user accounts for their organization. The LACA requires all users with LACA accounts to agree to LACA's Internet Acceptable Use Policy.

The LACA policies and procedures are partly enforced through the use of system alarms and audits. 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 any security violations on LACA systems:

ACL:	Gives file owners the option to selectively alarm certain files and events. READ, WRITE, EXECUTE, DELETE or CONTROL modes can be audited.
AUDIT:	Produces a record of when other security alarms were enabled or disabled.
AUTHORIZATION:	Enables auditing 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, SUBPROCESS 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 any security violations from the operator log and place them in a file for subsequent review by the technology director. The report contains information on unsuccessful logon attempts and any use of the AUTHORIZE command, which is used to modify the user authorization file. The SYSTEM account owns the command procedure and only users with system privileges can access the command procedure or file.

The LACA utilizes Symantec Anti-Virus software in conjunction with Mail Marshall (spam e-mail filtering software) on two network servers to scan all inbound and outbound e-mail. Anti-Virus definitions are automatically updated on network servers and individual PC's. If a virus is found, the e-mail is discarded and logged.

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

The LACA utilizes proxy logins for local administration of the Web Server only. The LACA does not allow proxy logins to remote systems. 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.

A User Identification Code (UIC) is individually assigned to all data processing personnel employed at the LACA. All user organizations are assigned a group UIC and each user within that user organization is assigned unique UIC. The UIC is assigned at the request of the user organization. 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 CAPTIVE flag is used for all user accounts not belonging to the LACA staff or the system.

The system forces users to change their passwords periodically. All interactive UIC accounts have a specified password lifetime. The student applications manager 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 create a unique password when they first logon. Supervisors are notified via e-mail of the user account and the status of the password field. The minimum password length for each user has been established.

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

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

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

An Access Control List (ACL) may be associated with each object recognized by the operating system. When an access request is made to an object, ACLs are always checked first, which either grants or denies access to the user requesting it. When an ACL fails to specifically grant access, the system then defaults to UIC-based protection.

The system directory contains security files that control the security parameters for the system. When a user attempts to gain access to an object, such as a file or directory, the system compares the user's 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 the MAXSYSGROUP number. (2) Users with system privileges. (3) Users with group privileges whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

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

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

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

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

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

Access to the OECN software packages is controlled at the ITC level by a security mechanism called the OECN Security Authorization (OSA) utility. Access to specific packages is provided by granting the appropriate identifiers to authorized users. Each application package has a set of unique identifiers that permit access to programs. In addition to the standard identifiers for each package, a pass through identifier can be used to

further customize access. OSA is used in conjunction with the OECN menu processor utility thus allowing the users to see only the items they are authorized to execute. UIC-based protection prevents WORLD WRITE or DELETE access to USAS, USPS, SAAS/EIS and EMIS application data files.

OECN_SYSMAN is an identifier which grants access to all packages. The OECN_SYSMAN identifier grants the user the same access as OECN_USPS, OECN_USAS, etc., for all packages without having to grant each individual identifier. The identifier is defined by state software so it works the same for all ITCs. The identifier grants access to software functions inside the software. It does not grant access to data. Only LACA staff has this identifier.

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 LACA 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.

A firewall and additional routing devices have been placed between the Internet access provided by the OECN network and the two segments of the internal 10-dot network used by the LACA and its user organizations. To allow for LACA IP traffic to flow to the Internet a firewall has been installed at the gateway to the Internet. The firewall has been configured to assign the 10-dot internal network addresses to a true IP Internet address.

The LACA is located on the second floor of an office building. During normal business hours, LACA's main door is left unlocked; however, data center personnel are present at all times. A cipher punch-code lock secures the computer room itself; only the LACA staff and the maintenance personnel know the combination. The building is locked after hours. In addition, motion detectors and an alarm system are armed to detect unauthorized access to the building.

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

- Smoke detectors.
- Regular fire extinguishers.
- Gas fire extinguishers.
- Sprinkler system.
- Liebert environmental system.
- Humidity and temperature sensors.
- Un-interruptible power supply (UPS).
- Power-kill switches for the Liebert, the UPS, and the computer room electricity.
- Transfer switch and power generator.

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. All the LACA employees have 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 Alpha systems. In addition, all users, except students, have access to Site Scape Forum, a bulletin board system that allows the LACA employees to communicate concerns with users across the state. Users may post questions and/or comments to the LACA staff through this site.

Certain routine batch jobs can be initiated at the LACA for system maintenance and security monitoring. All daily processes that are run by the LACA are scheduled through a scheduler. This utility runs a list of periodic batch jobs scheduled by the technology director.

Hardware maintenance agreements exist with HP and DataServ; both are paid annually. The LACA has a provision within their HP hardware maintenance agreement called RECOVER-ALL, which covers the replacement of equipment in the event of its total loss. The agreement with DataServ provides for hardware maintenance of the LACA routers and switches. In addition, all data processing equipment is covered under an insurance policy.

The LACA documents personnel authorized to make changes to user organization data through the completion of individual Fiscal Authority Change Forms. The form states authorized users have the authority to authorize the LACA staff to make specific changes to user organization fiscal data under the contracting service applications of the respective user organization. Requests for changes are to be made via fax or email prior to changes being made. The written requests are then maintained in the user organization's file.

The LACA prevents file or data corruption with several programs that are run automatically through the scheduler procedure. This procedure is programmed to be re-submitted automatically each day. The purpose of these programs is to ensure the integrity of user organization files.

The LACA performs full system backups daily, Sunday through Saturday. Daily backups for the Alpha are maintained for at least four weeks. Daily backup tapes are stored on-site in the LACA computer room. An exact duplicate set of tapes is rotated off-site daily to the Career and Technology Education Centers of Licking County (C-TEC) by the administrative assistant. All data required by law to be maintained for a specific duration is maintained by the LACA. Calendar year and fiscal year end information is stored indefinitely for all the LACA user organizations. Periodic restores of data are performed at the request of the user organizations, but they are not documented. These restores are generally requested when data has been accidentally deleted or due to user error.

User organizations are responsible for handling abnormal terminations. If the users cannot solve the problem, they will contact the LACA. The technology director, network coordinator, and network manager handle the majority of service calls from the user organizations for problems with the network. The technology director, student services manager, and administrative applications manager handle the majority of service calls from user organizations for problems with the Alpha.

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

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

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Changes to Existing Applications and/or Systems

Changes to Existing Applications or Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Applications developed and maintained by the SSDT at the NWOCA are the same as those distributed to and utilized by LACA. The most recent application updates are distributed by the SSDT and LACA is required to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the object files for USAS, USPS, SAAS, and EMIS at LACA was compared to the CRC of the object files at SSDT. Discussed procedures LACA uses to install state software.	No relevant exceptions noted.
The SSDT distributes release notes and updated manuals to the LACA when application updates are released. Updated manuals are also provided on the SSDT web site.	Inspected the release notes for the most recent application release. Inspected the SSDT web site for availability of updated manuals for the most recent release.	No exceptions noted.
The LACA participates in the CSLG/ESL program in order to maintain a licensing agreement for the operating system software and technical support.	Inspected a copy of the LACA's CSLG licensing agreement with the NBEC and payment information to confirm it is current.	No exceptions noted.
In order to maintain continued support of their application software provided by the SSDT, the LACA is required to install new releases of the operating system.	Inspected a copy of the invoice and payment information for the operating system. Inspected upgrade procedures and discussed them with the technology director	No exceptions noted.
The LACA maintains Service Level Agreements (SLA) with the user organizations for IT services.	Inspected the SLAs between the LACA and their user organizations to confirm the agreements document the services provided to the user organizations and the user organization's responsibilities. Inspected the SLAs for signatures from both the LACA and the user organization.	No exceptions noted.

IT Security

IT Security - *Control Objective:* **Security Management** - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The LACA Security Policy is current and communicated to the user organizations via LACA's web site.	Inspected the LACA security policy.	No exceptions noted.
An End User Access Request Form must be completed by an authorized district representative before a user account can be added on the system.	Identified user accounts with access to USAS, USPS, EMIS, and/or SAAS/EIS. Sampled 40 of 341 usernames and inspected the End User Access Request Form to confirm they were completed by an authorized district representative. Inquired with the technology director and student applications manager to confirm the process for authorizing access to the system. Inspected a district account authorization form that is completed by the district stating who is authorized to request new accounts.	No relevant 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:*
Quarterly, the LACA sends an e-mail to a designated representative of each user organization requesting their review of user accounts and associated access rights. User management must enter a confirmation into the LACA Account Management Application (LAMA) indicating that all accounts and associated rights are accurate.	Confirmed the review process with the technology director. Inspected an example of the original e-mail and follow-up e-mail sent to the user organizations requesting the account review be performed. Inspected the acknowledgement screen within the LAMA application used to confirm the account review was completed. Inspected the status screen to identify the user organizations that had completed the quarterly account review.	No relevant exceptions noted.
The tracking of security related events, such as break-in attempts and excessive log failures, is enabled through the system and events are logged in the audit journal.	Inspected the security alarms and audits to confirm 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 security monitor report, listing security violations from the audit journal, is generated by the system on a daily basis for review by the technology director.	Inquired with the technology director about security monitoring procedures including the process for monitoring reports and the frequency of review. Inspected the following, relating to the security monitor reports to confirm these reports are produced daily and forwarded to the appropriate personnel. • Example of a security monitor report. • Security Monitor command procedure utilized to generate the report. • Scheduler command procedure and listing.	No exceptions noted.
Anti-virus software runs on the Windows 2003 servers to help protect against computer viruses. Definitions are updated daily and infected items are quarantined. All viruses found are reviewed by the network manager.	Inquired about anti virus software and monitoring procedures with the network manager. Inspected the anti-virus definitions update scheduler. Inspected an example of the daily virus scans and alerts which can be used to monitor virus attacks/threats. Inspected the last anti-virus definition update and current software version.	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:*
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 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:*
Individual user profiles are used to grant access rights and privileges to the system in accordance with LACA policy.	A batch file was created using security analysis tools to extract information from the user authorization file to identify user accounts with elevated privileges. Inspected the listed accounts and inquired with the student applications manager regarding the purpose and appropriateness of the accounts extracted.	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 system does not consist of an excessive number of unused or inactive user profiles.	Using security analysis tools, extracted the following information from the user authorization file: • User accounts that have not been used in at least 180 days. • User accounts that have not been logged into. Inspected the listed accounts and inquired with the student applications manager regarding the purpose and appropriateness of accounts extracted.	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 proxy listing for use of wild card characters.	No exceptions noted.
Access to the operating system command line is restricted to authorized users.	Using security analysis tools, identified user accounts which do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER or RESTRICTED flags set. Inquired with the student applications manager regarding the appropriateness of these accounts.	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:*
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 LACA and the number of profiles with pre-expired passwords is limited.	Using security analysis tools, extracted password information from the user authorization file to identify: • User accounts with password minimum lengths less than the established guidelines of LACA. • User accounts with password lifetimes greater than the established guidelines of LACA. • User accounts with pre-expired passwords.	No exceptions noted for password minimum lengths. There were 64 of 583 (11%) of the user accounts that had a password lifetime greater than the established value. These accounts do not have the ability to access the OECN applications. There were 124 of 583 accounts (21%) with pre-expired passwords. The majority of these accounts consisted of library accounts, system accounts, template accounts, and accounts used for e-mail purposes which do not require an interactive login.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameter settings. Confirmed settings have not been changed from suggested vendor settings.	No exceptions noted.
A program constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed at startup.	Inspected the HITMAN parameters to confirm parameters were set for idle time and action to be taken against inactive users. In addition, identified protected accounts and processes. Inspected the system startup file to determine 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 executables files with WORLD write and/or delete access.	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:*
Firewalls and a routing system are used to control Internet traffic and maintain a logical segregation between user organizations.	Inspected the network diagram to confirm components of the network which control internet access. Confirmed existence of a private internal network by review of firewall and router configurations.	No exceptions noted.
Telnet sessions are not allowed from outside the LACA network.	Inquired with the technology director regarding the process of connecting to the system from outside of the LACA network.	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 a listing of all accounts with OECN identifiers for evidence of the use of identifiers to segregate access to the applications. Reviewed 40 new accounts, compared the requested identifiers to those granted in the users' authorization file.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized users.	Inspected the listing of all users having the OECN_SYSMAN identifier to confirm only appropriate users were assigned the identifier.	No exceptions noted.
User Control Consideration: User Identification Codes (UICs), passwords and 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 sensitive facilities, such as, 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 and security files is restricted.	Inspected the system file directory listing for WORLD write and/or delete access. Inspected the file protection masks on the security files.	No exceptions noted.
System level user identification codes are restricted to authorized personnel.	Identified the maximum system group number. Used security analysis tools to identify a listing of all accounts with a UIC less than the maximum system group number. Inquired with the technology director to confirm the appropriateness of any identified accounts.	No exceptions noted.
An alternate user authorization file is not permitted to be used and does not exist.	Inspected the value of the user authorization alternate parameter for the system. Inspected the system directory listings to determine if a user authorization alternate file existed.	No exceptions noted.
Remote access to firewall and router configurations used to control Internet access is restricted through password protection.	Inspected the firewall and router configurations to confirm passwords were required to access the configuration menus and to confirm remote administration was permitted.	No exceptions noted.

IT Security - *Control Objective:* **Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Physical access to the computer room and its contents is restricted to authorized personnel.	Inspected the keypad entry device to ensure access is restricted to authorized personnel. Inquired with the technology director, regarding the periodic changing of the keypad entry device access codes to determine the frequency of key code changes.	No exceptions noted.
Environmental controls are in place to protect against and/or detect fire, water, humidity, changes in temperature, or power failures.	Observed with the technology director, the existence of environmental controls over the computer system. Inspected the Liebert system, diesel generator, and existence of smoke detectors and fire extinguishers.	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:*
The LACA maintains hardware service support with HP and DataServ to cover hardware maintenance and failures.	Inspected the HP hardware and DataServ SmartNet service agreements, purchase orders, invoices, and payment histories for the audit period.	No exceptions noted.
Routine system maintenance programs, such as purging of email, reorganizing of application files, and analyzing files are scheduled and run to help prevent file failure and data corruption. Routine monitoring reports, such as account verification lists and security monitoring reports are also created by programs automatically.	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. Inspected the ANALYZE log obtained from the technology director to confirm the functionality of the ANALYZE system utility.	No exceptions noted.
The LACA monitors network performance and hardware failures through use of IP Check. Logs of failures are reviewed and problems are fixed by appropriate personnel.	The LACA monitors network performance and hardware failures through use of IP Check. Logs of failures are reviewed and problems are fixed by appropriate personnel.	The LACA monitors network performance and hardware failures through use of IP Check. Logs of failures are reviewed and problems are fixed by appropriate personnel.
Requests for changes to school district data files must be written and requested by personnel who are listed on the district's Fiscal Authority Change Form. Changes to school district files are documented and retained in the corresponding district's file at the LACA.	Inspected Fiscal Authorization List and an example Fiscal Authority Change Form from the fiscal services coordinator. Inquired with the LACA staff regarding the process for changing user organization data. Inspected the user change data forms to confirm they were requested by authorized users.	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:*
The system does not consist of an excessive number of Disusered user profiles.	Used a third-party audit software package to identify user accounts that are flagged as 'Disuser' within the user authorization file.	No relevant exceptions noted.
All data center hardware and software equipment is covered by an insurance policy.	Inspected the insurance policy to confirm LACA equipment is insured in the event of a disaster.	No exceptions noted.
User Control Considerations: User organization management should periodically review the "AUDITS" report for unauthorized changes to application data.		

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:*
Written backup procedures outlining the frequency and type of backups to be performed are maintained. Incremental backups of systems and data are performed daily. All backups are automated and are scheduled.	Inspected the scheduler listing to confirm the backup procedures are executed regularly. Inspected the backup command procedure, an example backup log, and example backup report to confirm backups are automated and scheduled.	No exceptions noted.
Backup tapes are stored in secure on-site and off-site locations. They are rotated off-site on a daily basis.	Inspected the StorServer Manager's Guide to confirm policies and procedures exist for the daily, dual backups and rotation to an offsite location. Inspect the onsite security box and tapes to confirm backups were completed and stored in a secure location. Inspected the off-site storage location to confirm backup tapes were stored at C-TEC as indicated by the StorServer tape library dated 6/30/08.	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:*
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

SITE DATA

Name:	Licking Area Computer Association (LACA)
Number:	8
Node Name:	LACA
Chairperson:	Nelson McCray Superintendent Licking County ESC
Fiscal Agent District:	Career and Technology Education Centers of Licking County (C-TEC)
Administrator:	Sandra Mercer Executive Director LACA
Address:	195 Union Street, Suite C-2 Newark, OH 43055
Telephone:	740-345-3400
FAX:	740-345-3427
Website:	www.LACA.org

OTHER SITE STAFF

Chad Carson	Technology director
Mary Knicely	Administrative applications manager
Melody Hewitt	Fiscal coordinator
Joey Alexander	Network manager
David Stein	Network coordinator
Bobbie Warthman	Educational applications manager
Jerry Eby	Student applications manager
Linda Haynes	Student services coordinator
Trish Baker	Media resource coordinator
Jonathan Bowers	Operations director
Heather Cronbaugh	K-12 special services manager
Elizabeth Faulkner	K-12 classroom data coordinator
Helen Morris	Administrative assistant
Jeff Davis	Student data analysis coordinator

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	HP Alpha 4100 5/600	Lines/Ports:	N/A	Memory Installed:	5 GB
Disk:	EVA3000 SAN	Units:	1	Total Capacity:	up to 1913 GB
Tape Unit:	TTY13	Units:	1	Max Density:	8 mm
Tape Unit:	SDLT 110/220	Units:	1	Max Density:	SDLT
Tape Unit:	Storserver 2500	Units:	2	Density:	LT03
Printer:	LG10 Plus	Units:	1	Print Speed:	1000 LPM
Printer:	LA400	Units:	1	Print Speed:	N/A

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
044420	Mount Vernon CSD	Knox	X	X	X	X
045393	Granville EVSD	Licking	X	X	X	X
044115	Heath CSD	Licking	X	X	X	X
047985	Johnstown-Monroe LSD**	Licking	X	X	X	X
047993	Lakewood LSD	Licking	X	X	X	X
047977	Licking County ESC	Licking	X	X	X	X
043927	Career and Technical Center of Licking County	Licking	X	X	X	X
048009	Licking Heights LSD	Licking	X	X	X	X
044453	Newark CSD	Licking	X	X	X	X
048025	North Fork LSD	Licking	X	X	X	X
058033	Northridge LSD	Licking	X	X	X	X
045278	Southwest Licking LSD	Licking	X	X	X	X
045450	Maysville LSD	Muskingum	X	X	X	X
048884	West Muskingum LSD	Muskingum	X	X	X	X
048876	Tri-Valley LSD	Muskingum	X	X	X	X
000162	Newark Digital Academy	Licking	X			X
149328	Foxfire Alternative	Licking	X			X
149336	Southwest Licking Digital Academy	Licking	X			X

USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
151233	Lakewood Digital Academy	Licking	X			X
000941	Par Excellence Academy	Licking	X	X		X
TOTALS			**20**	**16**	**15**	**20**

**Johnstown-Monroe LSD became a member of Tri-Rivers Education Computer Association (TRECA) as of 7/1/08.

Mary Taylor, CPA
Auditor of State

LICKING AREA COMPUTER ASSOCIATION
(LACA)

LICKING COUNTY

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

Susan Babbitt

CLERK OF THE BUREAU

CERTIFIED
SEPTEMBER 23, 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