TRI-COUNTY COMPUTER SERVICES ASSOCIATION

STATE REGION - ISA, WAYNE COUNTY

SAS - 70

APRIL 24, 1999 THROUGH JUNE 30, 2000

JIM PETRO
AUDITOR OF STATE

STATE OF OHIO

TABLE OF CONTENTS

This Page Intentionally Left Blank

STATE OF OHIO
OFFICE OF THE AUDITOR

JIM PETRO, AUDITOR OF STATE

88 East Broad Street
P.O. Box 1140
Columbus, Ohio 43216-1140
Telephone 614-466-4514
800-282-0370
Facsimile 614-466-4490
www.auditor.state.oh.us

REPORT OF INDEPENDENT ACCOUNTANTS

Executive Committee
Tri-County Computer Services Association (TCCSA)
Wayne County
2125-B Eagle Pass
Wooster, Ohio 44691

To the Members of the Executive Committee:

We have examined the accompanying description of controls of the Tri-County Computer Services Association (TCCSA) applicable to the processing of transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), School Asset Account 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 TCCSA's controls that may be relevant to a member school district'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 member school districts applied the internal controls contemplated in the design of the TCCSA's controls; and (3) such controls had been placed in operation as of June 30, 2000. The control objectives were specified by the TCCSA 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.

As discussed in the accompanying description, TCCSA has a reciprocal agreement for use of hardware at another Data Acquisition Site. However, a formal disaster recovery plan has not been developed. The deficiency results in policies and procedures not being suitably designed to meet the control objective, "Adequate plans should exist for the recovery of critical resources following an event which disrupts data processing services for an extended period of time."

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of the TCCSA's controls that had been placed in operation as of June 30, 2000. Also, in our opinion, except for the matter described above, 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 member school districts applied the controls contemplated in the design of the TCCSA'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 April 24, 1999 to June 30, 2000. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to member school districts of the TCCSA and to their auditors to be taken into consideration along with information about the internal control at member school districts, when making assessments of control risk for member school districts. In our opinion, except for the matter described above, 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 II were achieved during the period from April 24, 1999 to June 30, 2000.

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

The information in Section IV describing the consortium profile information is presented by the TCCSA to provide additional information and is not part of the TCCSA'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 member school districts and, accordingly, we express no opinion on it.

The description of controls at the TCCSA is as of June 30, 2000, and information about tests of the operating effectiveness of specified controls covers the period from April 24, 1999 to June 30, 2000. 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 TCCSA 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 TCCSA, its member school districts, and the independent auditors of its member school districts.

JIM PETRO
Auditor of State

June 30, 2000

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The TCCSA'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 TCCSA's description of controls.

ORGANIZATION

The Tri-County Computer Services Association (TCCSA) is a not-for-profit computer service organization that is a subsidiary of the Midland Council of Governments. The primary function of the TCCSA is to provide information technology services to its member school districts with some emphasis placed on accounting, payroll and inventory control services.

The TCCSA is one of twenty-three regional service organizations serving over 600 public school districts in the State of Ohio that make up the Ohio Educational Computer Network (OECN). These service organizations are known as Data Acquisition Sites (DAS). The OECN is a collective group of Data Acquisition Sites, authorized pursuant to Section 3301.075 of the Revised Code, and their member school districts. 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 school districts. Funding for this network and for the TCCSA is derived from the State of Ohio and from user fees.

There are currently twenty consortium members (member school districts) in the Ohio counties of Ashland, Holmes, Medina and Wayne. These consortium members are comprised of public school districts and county educational service centers and are voting members of the TCCSA. Throughout the remainder of this report, any reference to member school districts will also include the county educational service centers.

The laws governing the Ohio Education Computer Network require that a board of education serve as fiscal agent for Data Acquisition Sites receiving state funds. Specifically, revised code section 3301.075 requires the TCCSA conform to revised code section 3313.92 in order for TCCSA to receive Ohio Education Computer Network funds from the State Department of Education. Agreements entered into pursuant to revised code section 3313.92 must be approved by the State Superintendent of Public Instruction, who has interpreted this revised code section to require a board of education to serve as fiscal agent for a Data Acquisition Site receiving funds from the Ohio Education Computer Network.

For this reason, the Tri-County Educational Service Center serves as fiscal agent for the TCCSA and performs certain functions that might otherwise be performed by the council in order to ensure receipt of funds from the Ohio Education Computer Network. Essentially, these functions are to apply for and maintain the Data Acquisition Site permit for the central data processing equipment and to hold legal title to the central data processing equipment. The TCCSA is located in Wooster, Ohio.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

The TCCSA is a subsidiary of the Midland Council of Governments. Operations are under the control of the Executive Director and the TCCSA Executive Committee. The Midland Council of Governments exists to foster cooperation among its member school districts in all areas of educational service. One member from each member district is appointed to the legislative body of the council known as the assembly and is normally the district superintendent. The assembly meets at least twice per year to estimate program costs, approve annual appropriations, select officers and members of the Executive Committee and approve other matters as determined to require the approval of the assembly.

The Executive Committee is the governing body of the TCCSA and is composed of seven elected members and two Ad Hoc members. The composition of the Executive Committee must contain two superintendents; two treasurers; two at large members; the Fiscal Agent's Superintendent as well as the two Ad Hoc members, the Executive Director of TCCSA and the Fiscal Agent Treasurer. The Executive Committee is required to meet every other month.

The TCCSA employs a staff of nineteen individuals and is supported by the following functional areas:

Application Support - Facilitates the implementation and operation of fiscal and student services of the TCCSA which include USAS, USPS, SAAS/EIS, EMIS and GAAP application systems, and provides user training and support.

Network/Systems Support - Designs and supports the TCCSA computer systems, its networked communications systems and provides user training and support as needed.

Educational Technology Support- Facilitates the implementation and operation of educational technology services to TCCSA member school districts and provides user training and support.

The managers of each of the functional areas report to the Executive Director.

The TCCSA follows the same personnel policies and procedures as the Midland Council of Governments. When necessary, additional TCCSA policies have been developed and approved by the TCCSA Board to address concerns of the TCCSA. Detailed job descriptions exist for all positions. The TCCSA is constantly re-evaluating its need for personnel to provide for the increasing range of services provided. The reporting structure and job descriptions are periodically updated to create a more effective organization.

Users are responsible for authorization and initiation of all transactions. Management reinforces this segregation of duties as a part of its new employee orientation process through on the job training and by restricting employee access to user data. Changes to user data are not performed.

Additional information regarding the control environment can be found in the section, “Overall Operation of the IT Function,” beginning on page six.

Risk Assessment

The TCCSA does not have a formal risk management process, however, the TCCSA Executive Committee is made up of representatives from the member school districts who actively participate in the oversight of the TCCSA.

As a regular part of its activity, the TCCSA Executive Committee addresses:

New technology,
Realignment of the TCCSA organization to provide better service,
Personnel issues, including hiring, termination, and evaluations,
Additional services provided to member school districts and other entities,
Changes in the operating environment as a result of ODE requirements, AOS and other accounting pronouncements and legislative issues.

In addition, the TCCSA has identified operational risks resulting from the nature of the services provided to the member school districts. 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 on pages six through twelve of this report.

Monitoring

The TCCSA organization is structured so that managers of each department report directly to the Executive Director. The key management employees have worked for TCCSA for many years and are experienced with the systems and controls at the TCCSA. The TCCSA Executive Director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

Hardware, software, network, database integrity, Internet usage, and computer security 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.

INFORMATION AND COMMUNICATION

The aspects of the information and communication component of internal control as they affect the services provided to member school districts are discussed within the General EDP control section.

GENERAL EDP CONTROLS

Overall Operation of the Information Technology Function

The TCCSA data processing staff consists of nineteen individuals. The breakdown of individuals by position is as follows:

Executive Director (1)
Manager Software Applications/Support (1)
Asst. Mgr. Software Applications/Support (1)
Manager of Network Operations (1)
LAN Administrator (1)
Educational Technologists (3)
Technicians (5)
Software Support Specialist (1)
Educational Technology Coordinator (1)
Technology Coordinator (1)
Workstation Repair Specialist (1)
Secretary (2)

The TCCSA acts as a service organization for member school districts and is physically separate from the user organizations. The TCCSA is generally limited to recording user organization transactions and processing the related data. The user organization is responsible for authorizing transactions and maintaining their accountability. Therefore, there is a high degree of interaction between the policies and procedures at the TCCSA and those at the user member school district organizations.

The TCCSA hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the organization require some type of college degree or experience in a computer-related field, and all the TCCSA staff members are required to attend professional development and other training as a condition of continued employment. Each staff member must attend at least fifteen hours of approved professional development training annually, and at least eighty hours of approved training every four years.

The legislative and advisory body of TCCSA is the Assembly which elects representatives from its ranks to a governing body called the Executive Committee. The Executive Committee is composed of the seven elected members and two Ad Hoc members. The Executive Committee works with the Executive Director as the planning group for the organization. Together they set the direction for all aspects of the TCCSA.

Acquisition and Implementation

There are no systems development activities which are actually performed by the TCCSA personnel. The TCCSA utilizes the software which is supplied by the State Software Development Team at the Northwest Ohio Computer Association (NWOCA) which is another Data Acquisition Site of the Ohio Education Computer Network. The Ohio Department of Education determines the scope of software development for state supported systems. Tactical means of accomplishing the priorities are determined by the State Software Development Team which consists of staff members from the Ohio Department of Education and the NWOCA. The development team meets on a periodic basis to discuss the status of proposed and ongoing projects.

The majority of the significant application changes are mandated by the Ohio Department of Education. For those changes which are not required by the ODE, a software change impact statement is completed by the SSDT after discussion of the need for the change. Requests for changes to applications originate from three sources, SiteScape Forum, the help line, or suggestions made by individuals on the State Software Development Team (SSDT). Requests may be made by users at member school districts, the Data Acquisition Sites or others with access to the Forum.

Changes to Applications

There are no maintenance activities which are actually performed by the TCCSA personnel. The TCCSA utilizes the software which is supplied by the State Software Development Team at the Northwest Ohio Computer Association (NWOCA). OECN requires the DAS to keep the version of each software package current based on the provider’s standard for continued support.

Procedures are in place to ensure that SSDT developed applications are used as distributed. On a quarterly basis, updates to the state software are downloaded from SSDT at NWOCA to the other Data Acquisition Sites. Source code is not distributed. Release notes explain the changes, enhancements and problems corrected. User and System Manager manuals are also distributed. NWOCA informs the other DASs that they will support only the latest release of the state software beginning 30 days following the software release date.

Computer Security

The TCCSA has a security policy which outlines the responsibilities of member school district personnel and students, the TCCSA personnel, and any individual or group not belonging to the member school district or the TCCSA.

The TCCSA staff are 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.

Member school districts are granted access upon written authorization from the member’s superintendent. Data center personnel access is established, granted and reviewed by the Executive Director.

Primary logical access control to the Compaq computers is provided by security provisions of the Open VMS operating system. This includes access to data, programs and system utilities. In Open VMS, the process performs the role of the subject, which is the active element that gains access to information. When a user logs in to use Open VMS interactively, or when a batch or network job starts, Open VMS creates a process which includes the identity of the user. A process is vulnerable to security breaches during creation and while accessing information. Open VMS manages process access to information using its authorization data and internal mechanisms.

The system directory contains security files which control the security parameters on the system. When a user attempts to gain access to an object (such as a file or volume), the system, checks the User Identification Code (UIC). This involves comparing the user's UIC to the owner's UIC of the object. An exception occurs when there is an Access Control List (ACL) on the object which grants access immediately to the requesting user. Users attempting to access system objects (such as files) always fall into one or more of the following categories:

> SYSTEM: Can be; (1) all users who have system privileges (SYSPRV); (2) users with low group numbers, usually from one through ten octal. These group numbers are generally for system managers, security administrators, system programmers, and operators; (3) users with the user privilege GRPPRV whose UIC group matches the group of the object's owner; and (4) for files on disk volumes, users whose UIC matches the owner UIC of the volume on which the file is located.
>
> OWNER: The user with the same UIC as the user who created and therefore owns the object.

GROUP: All users, including the owner, who have the same group number in their UIC as the object's owner.

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

Through this protection code, each category of user can be allowed or denied any of the following types of access:

READ, WRITE, EXECUTE, DELETE

The WRITE and DELETE access capabilities are not activated for WORLD access to the files in the SYS$SYSTEM directory. The UIC associated with each of these files is within the MAXSYSGROUP number.

Through the protection code, each category of users can be allowed or denied READ, WRITE, EXECUTE, and DELETE types of access. Default file protection is normal with SYSTEM having Read, Write, Execute, and Delete capabilities, OWNER having Read, Write, Execute, Delete capabilities, GROUP having Read and Execute capabilities and WORLD having no access capabilities.

User accounts which are not established as CAPTIVE accounts are set with the NORMAL parameter, the minimum level of access privileges. This limits users from any higher level system privileges. UIC based protection to production programs prevents WORLD WRITE or DELETE access.

To limit access to security files, the TCCSA has limited the WORLD access for the SYSUAF.DAT file, which contains account information to identify which users are allowed access to accounts on the system; the NETPROXY.DAT file, which contains proxy account information to identify which remote users are allowed access to proxy accounts on the system; and the RIGHTSLIST.DAT file, which contains names of the reserved system identifiers and identifiers for each user.

The system forces staff users, who use the various software packages, to periodically change their passwords. The DEFAULT account password lifetime field has been set to a lifetime of 90 days. When a user is added to the system, they are set up with a temporary password. The system then forces the user to create a unique password when they first login.

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:

C The terminal name is part of the association string for the terminal mode of break-in detection.

C Restriction on the time a user has to correctly enter a password on a terminal on which the system password is in effect.

C Amount 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.

C The period for which evasive action is taken is variable and will grow as further logon failures are detected from the suspect source.

C 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 Compaq established defaults. Any changes are logged and reviewed by the Executive Director or by the Software Applications and Support Manager in the Executive Director's absence.

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.

The following detection control alarms have been enabled through Open VMS to monitor any security violations:

ACL: Gives files 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 UAF or network proxy authorization file in addition to auditing changes to the rights database. The Executive Director can specify the AUTHORIZATION keyword with the /ENABLE qualifier of the SET AUDIT command.

BREAK-IN: Produces a record of break-in attempts. The Executive Director can specify the BREAKIN keyword with the /ENABLE qualifier of the SET AUDIT command to audit break-in attempts. The Executive Director can audit the DIALUP, LOCAL, REMOTE, NETWORK, and DETACHED break-in types can be audited.

Security violations are reviewed on a daily basis. 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 Executive Director and the Applications and Software Support Manager.
The report contains information on unsuccessful logon attempts and any use of the AUTHORIZE command which is used to modify the SYSUAF file. The command procedure is owned by the SYSTEM account and only users with system privileges can access the command procedure or file.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at TCCSA and all member school district personnel. District users are enabled a NORMAL privilege class which permits NETMBX and TMPMBX activities. Access is further controlled using captive login scripts to ensure that escape to the command line does not occur.

Access to the Ohio Education Computer Network (OECN) software packages is controlled at the DAS level by a security mechanism called the OECN Security Authorization (OSA) utility. Access to specific packages is provided by granting the appropriate Open VMS 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.

The data processing department is located in an office building which is secured by both key lock and a security system.   All doors are locked during off hours. During daytime hours the main door is unlocked, however, data processing personnel are present at all times. An individual must enter the printer room to access the computer room. The door to the printer room is always locked and is protected by a key pad lock. The combination is known by the data processing staff and the maintenance personnel. Motion detectors are in place throughout the building.

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

C Hand-held fire extinguishers.

C Air condition/humidity control devices.

C The computer room contains a UPS (Un-interruptible Power Supply), to provide power to key computer components for a short period of time during power interruptions.

C The room is equipped with smoke detectors built into the ceiling.

C The computer room has an eight inch raised floor to reduce the risk of damage from flooding.

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

Access to the Internet has been provided to the member school districts of the TCCSA. Access is provided through the OECN GOSIP network and routed to TCCSA. A Cisco PIX (Private Internet Exchange) firewall has been placed between the Internet access provided by the OECN network and the internal network of the member districts of the TCCSA. The PIX firewall performs the function of a proxy server and acts as a middle man between the Internet and the internal network. The PIX firewall equipment and an additional routing device deny all outbound traffic requests originating from the sub-network. The firewalls and routing devices also deny access to all inbound traffic unless the IP address originated from inside the network.

TCCSA also makes available an Internet content filter. The filter named Bess is an optional service which screens Internet site requests for “unsuitable” content.

Computer Operations

Traditional computer operations procedures are minimal since users at the member school districts initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. In addition, every employee has access to SiteScape Forums which is a billboard system that addresses a variety of problems common to VAX and ALPHA users.

TCCSA staff have maintained a listing of individuals to contact in the event of complications with the hardware environment. A service agreement with Compaq has been entered into by TCCSA to provide continued maintenance on all critical and sensitive peripheral equipment. The operating system monitors the hardware environment and reports all hardware malfunctions automatically through the console maintained by the system. A hardware error log hardware of errors identified by the VMS operating system is reviewed by the Executive Director and the Manager of Software Applications on a daily basis.

Certain routine batch jobs can be initiated at TCCSA for system maintenance. The TCCSA is responsible for a few operational maintenance tasks of which a few are: system backups, log reports, and other maintenance directed at the system as a whole.

Individual member school districts are responsible for running their own regular reports which are batch processes. Batch processes are initiated and completed by the individual member school districts. However, TCCSA runs some batch processes for the processing of EMIS data.

Member school districts are responsible for the handling of abnormal terminations. If the users cannot solve the problem they will contact TCCSA staff who act as service representatives.

The TCCSA follows the guidelines of the Ohio Educational Computer Network (OECN) for backing up system data and programs. An Alpha Server GS60 is used by the TCCSA for production. Full system backups are performed daily. The tapes are stored in the computer room and are rotated off-site to a safety deposit box at least twice a week. The backup tapes are documented in a backup log.

Daily backups are maintained for approximately 6-8 weeks. All data required by law to be maintained for a specific duration is maintained by the TCCSA. Calendar year and fiscal year end information is stored indefinitely for all the TCCSA member school districts.

The TCCSA has entered into two reciprocal disaster recovery agreements. One agreement is with the Area Cooperative Computerized Educational Service System (ACCESS) and the other is with the Licking Area Computer Association (LACA).

Only vendor supplied changes are made to the operating systems or system software documentation. The Northern Buckeye Education Council, (NBEC), acts as the fiscal agent for this and other participating Data Acquisition Sites, and has entered into a license under the Campuswide Software License Grant Program (CSLG) through the Management Council of the Ohio Education Computer Network (MCOECN), for acquiring and/or providing software maintenance services for a limited series of Compaq 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 Data Acquisition Sites for a limited series of Compaq software packages as approved by the Executive Committee of the MCOECN.

Provide telephone technical support to the participating Data Acquisition Sites technical staff for a limited series of Compaq software packages approved by the Executive Committee of the MCOECN.

Track and maintain an accurate listing of all Compaq 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 Data Acquisition Sites' technical staff on the latest releases of Compaq software packages covered under the agreement.

As a participating member of the program of the MCOECN the participating Data Acquisition Sites agree to the following:

To read, sign, and comply with the "Rules and Regulations" of the CSLG Program and the Education Software Library (ESL) Program as operated by NBEC on behalf of the MCOECN.

Read, cooperate, and comply with both the CSLG and ESL Management Plans as adopted and approved by the Executive Committee of the MCOECN.

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

Upon written notice, provide Compaq with physical access to computer facilities at reasonable times during normal business hours for the purpose of inspecting sites and system records for compliance with the terms of the CSLG and ESL Programs.

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 TCCSA'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 TCCSA and procedures performed at member school districts which utilize the TCCSA.

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

Overall Operation of the IT Function

Overall Operation of the IT Function - *Control Objective:* **IT Personnel** - IT personnel should have the appropriate knowledge and experience for the complexity of the IT environment.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The TCCSA has an organization chart and job descriptions to guide employees in the performance of their duties.	Obtained the TCCSA staff listing, organization chart and job descriptions. Compared the organization chart and job descriptions with the staff listing. Verified with the Executive Director that the staff listing is current. Selected four staff members and verified each had a copy of his job description and that it fairly represented his job duties	The TCCSA has an organization chart and job descriptions for each of its technical staff members. Each of the four members interviewed stated that his job description fairly described his duties.
Training is obtained by the TCCSA technical staff members.	Obtained and reviewed the Account Status Report for payment of training courses. Also obtained copies of certificates of completion from training classes attended by the TCCSA staff.	Thirteen of the seventeen technical staff members received training during the audit period. The amount of training received ranged from one to ten classes.
The TCCSA staff receive evaluations on an annual basis.	Judgementally selected four staff members and verified with each that he had received an evaluation on an annual basis.	Each of the staff members tested verified they receive an informal verbal evaluation on a yearly basis.

Overall Operation of the IT Function - *Control Objective:* **IT Planning** - IT strategy should be consistent with the overall strategy of the organization.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The Council of Governments is actively involved in managerial and planning issues.	Obtained and reviewed meeting minutes of the Executive Committee and the Full Membership for the audit period.	Observed that key planning and managerial issues were addressed in the board minutes.

Overall Operation of the IT Function - *Control Objective:* **IT Planning** - IT strategy should be consistent with the overall strategy of the organization.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
An annual budget is developed by the Executive Director, and approved by the Council of Governments, for short range planning purposes.	Obtained and reviewed the fiscal year 2000 and 2001 budgets.	Planning is conducted via the budgetary process on a yearly basis by the Executive Director to address technical services, equipment repair, and equipment purchases.

Changes to Applications

Changes to Applications - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Procedures are in place to ensure that SSDT developed applications are used as distributed. On a quarterly basis, updates to the state software are downloaded from SSDT at NWOCA to the other Data Acquisition Sites. Source Code is not distributed.	To ensure the state software tested at NWOCA is the version being utilized at the TCCSA, a cyclical redundance check (CRC) of the object program files at the TCCSA was compared to the CRC of the latest ODE version tested at NWOCA.	The CRCs of the object code for the USPS, SAAS/EIS and EMIS applications at the TCCSA were the same as the CRCs of the object code from NWOCA.
Release notes explain the changes, enhancements and problems corrected. Updated User and System Manager manuals are also available.	Obtained and reviewed release notes and manuals for the most recent release.	Release notes and updated manuals were available to all of the TCCSA employees.

Computer Security

<table>
<tr><td colspan="2"><b>Computer Security -</b> <i>Control Objective:</i>
<b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>The TCCSA has established a set of Data System Security Policies addressing the responsibilities of member school district personnel, the TCCSA personnel, and individuals or groups not belonging to the TCCSA or member school districts.</td><td>Obtained and reviewed the Data System Security policies to ensure that user responsibilities are documented.</td><td>The Data System Security policies exists and documents: data security procedures, data access requirements for school district and computer center personnel and access by outside users.</td></tr>
<tr><td>Detection control alarms are enabled through VMS to monitor security violations.</td><td>Obtained and reviewed the security alarms enabled from the Executive Director via the DCL command SHOW AUDIT/ALL.</td><td>Security alarms have been enabled for ACL, Audit, and Breakin. Security event logging has been enabled for ACL, Audit, Breakin, and Authorization.</td></tr>
<tr><td>Wild card characters are not used in the NETPROXY listing.</td><td>Obtained the PROXY listing from the Executive Director via the SH/PROXY command and reviewed the listing for use of wild card characters.</td><td>There were no wildcard characters used in the PROXY listing.</td></tr>
<tr><td>File protection masks are applied to user data files to prevent unauthorized usage or modification.</td><td>Obtained and reviewed a file listing of all member school district data files from the Executive Director. The listing indicated the file access restrictions applied to each file. Access restrictions were reviewed to ensure that no access was provided at the “WORLD” level.</td><td>There were no data files listed as having WORLD Write or Delete access.</td></tr>
<tr><td>File protection masks are applied to executable files to prevent unauthorized usage or modification.</td><td>Obtained and reviewed a directory listing of the executable files for the USAS, USPS, SAAS/EIS and EMIS application programs for WORLD access limited to Read and/or Execute.</td><td>Executable files do not have WORLD Write or Delete access and there were no ACLs attached to any of the executable files.</td></tr>
<tr><td>Authorization from the member school district superintendent is required prior to setting up a user account. Authorization of both the teacher and the student’s parent is required for student accounts.</td><td>Judgementally selected 65 accounts from a population of 4783 accounts and verified that the access provided was authorized by the district superintendent or the student’s parent and teacher.</td><td>Access authorization forms were present for 64 of the 65 accounts selected.   Authorization standards were complied with for all 64 authorization forms obtained.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Computer Security -</b> <i>Control Objective:</i>
<b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td colspan="4"><b>Member School District User Control Considerations:</b>
Users should be aware of the confidential nature of passwords and should take precautions to ensure passwords are not compromised.

When user member school district personnel leave or are otherwise terminated, all access capabilities for that user should be removed or modified. A message should immediately be sent to the TCCSA personnel notifying them of the vacancy and that privileges to the system should be revoked.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Computer Security -</b> <i>Control Objective:</i>
<b>System Level Access Controls</b> - Access to the computer system, programs, and data should be appropriately restricted.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Password values have been enabled to deter unauthorized access through compromised passwords.</td><td>PCDA, a security analysis tool, was used to extract information from the VMS security file, SYSUAF. LIS, to determine the following:
• User accounts having a password of less than six characters,
• User accounts with a password lifetime of greater than ninety days,
• The number of user accounts having pre-expired passwords.</td><td colspan="2">All accounts are required to be password protected with a password of at least six characters in length.
Account password lifetimes for 109 of the 4783 accounts exceeded the 90 day change requirement. One exception of the 109 exceptions was an error, with the remaining 108 being a combination of the following acceptable policy deviations:
1. Accounts used by substitute librarians to access the card catalog system.
2. Training accounts used to train new users who attend TCCSA training.
3. Application or operating system support accounts
4. Accounts used by students to access the card catalog system, and
5. Individual accounts used as guest or pass through accounts provided to individuals or other DASs as needed.
Numerous accounts (1257 accounts) were found to have pre-expired passwords.</td></tr>
</table>

Computer 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 DEFAULT templates used to create student, teacher, and staff accounts incorporate the TCCSA password standards.	The DEFAULT templates were obtained from the Executive Director and were reviewed for adherence to standards established by the TCCSA.	Default settings require that passwords are to be pre-expired, at least six characters in length, and changed every ninety days.
Log-in parameters have been set to control and monitor sign-on attempts.	Using the VMS System Generation (SYSGEN) Utility, the Executive Director printed the VMS Login parameters via the SHOW /LGI command. Parameters were reviewed for appropriateness.	Parameters have been set and controls are in place to address sign on attempts and sign on constraints for break-in detection and evasion. All of these SYSGEN parameters are consistent with the recommended Compaq defaults.
Login scripts are used to restrict users access to the command prompt.	Judgementally selected 60 accounts made up of both teacher/administration accounts and student accounts, from a total account base of 4783. Verified the use of “captive scripts” by examining the SYSUAF profile for each account selected. Identified the script used and reviewed the appropriate script.	In all accounts profiles examined, login scripts were used to direct user access to the OECN menu system, and prevent the user from gaining access to the system prompt.
HITMAN monitors terminal activity and logs off inactive users.	Reviewed HITMAN parameter listings for both Prime and Non-Prime hours. Reviewed the SYSTARTUP_VMS.COM file to ensure the HITMAN utility is part of the startup procedures.	First and second warnings are given at thirty-five and forty minutes respectively, with processes being killed at forty-five minutes of idle time. TCCSA staff member accounts and a limited number of system processes or system accounts are logged out after significantly longer intervals. From review of the SYSTARTUP_VMS.COM file, HITMAN is part of the daily start up procedure.

Computer 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 Cisco PIX (Private Internet Exchange) Firewall and a Cisco 7513 Router are utilized to control Internet traffic into and out of the TCCSA.	Obtained and reviewed network diagrams from the Network Operations Manager. Obtained and reviewed the syntax listing from the PIX box.	A Cisco Router and PIX Firewall have been placed between the Internet and the TCCSA internal network. Internet traffic is controlled within both devices given the current configuration settings.
The internal network used at the TCCSA uses a 10-dot network, which is an addressing scheme unable to be used over the Internet.	Confirmed the existence of the 10-dot network with the Network Operations Manager, and a Field Service Technician. Using the operating system command “SHOW USER/FULL” which displays the connection type of all users currently logged into the system, determined if a ten dot addressing scheme is being used at TCCSA.	A ten dot addressing scheme is used at TCCSA.
Remote administration of the firewalls and routers used to control Internet access is restricted to TCCSA staff.	Reviewed firewall, and router configurations.	Parameter settings require that two passwords must be entered before an individual can alter the configuration of the firewall or the router.

<table>
<tr><td colspan="2"><b>Computer Security -</b> <i>Control Objective:</i>
<b>Application Level Access Controls</b> - Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>A default menu system is provided as a part of the application software and restricts users to the application. The OECN Security Authorization (OSA) Utility of the application software controls access to applications based on VMS identifiers.</td><td>Discussed the OSA utility with the Executive Director and the Software Applications Support Manager.
Using the VMS “push” utility, recreated the security environment of seven users and observed the menus provided to these users by the OECN Security Authorization utility. Comparisons were then made between the menu provided and the identifiers listed on the user’s SYSUAF profile to ensure that the menu items listed corresponded to the profiles’ identifiers.</td><td>Identifiers are assigned at the VMS level to individual user accounts upon the request of the member school district to control their access to application software.
Programs listed on the menus provided by the OECN Security Authorization utility correspond to the identifiers listed in the selected SYSUAF profiles.</td></tr>
<tr><td>The OECN_SYSMAN identifier, which grants access to all state software packages without having to grant individual identifiers, is restricted to only authorized personnel.</td><td>Obtained and reviewed a listing of all users having the OECN_SYSMAN identifier. Discussed the functionality of the identifier with the Executive Director.</td><td>The OECN_SYSMAN identifier has been restricted to only authorized personnel. It was also noted that this identifier grants special privileges only to the OECN state software. It does not grant access to data.</td></tr>
<tr><td colspan="3"><b>Member School District User Control Considerations:</b>
Member school districts should ensure that User Identification Codes (UICs), passwords and associated access privileges for their district personnel are issued only to authorized users who need access to computer resources in order to perform their job function.
UICs should be individually assigned to each system user to improve individual accountability of user activity.</td></tr>
</table>

Computer Security - *Control Objective:* **Sensitive Facilities** - Use of sensitive facilities, such as, master passwords, powerful utilities, and system manager facilities, should be appropriately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
WORLD Write and Delete access are absent from the SYS$SYSROOT directories.	Obtained the file directory listing for the SYS$SYSROOT [SYSEXE] and SYS$SYSROOT [SYSMGR] directories and reviewed the file protection masks for WORLD Write or Delete access.	There were no files in the directory listings having WORLD access equal to Write or Delete.
User accounts do not have UIC group numbers less than MAXSYSGROUP.	Through the VMS System Generation (SYSGEN) utility using the SHOW MAXSYSGROUP command, determined the MAXSYSGROUP number. Utilizing PCDA, obtained a listing of all accounts with a UIC less than the MAXSYSGROUP number.	MAXSYSGROUP is set at eight. Only five accounts have UICs less than MAXSYSGROUP. One of the accounts is a generic operator account which is used to initiate backups. The remaining four accounts are default VMS system administration accounts. None of the accounts belong to member school district users.
Member school district accounts do not have privileges in excess of the minimum privileges necessary to use the system.	Utilizing PCDA, obtained a listing of all accounts having elevated privileges (more than NETMBX and TMPMBX)	All accounts with elevated privileges are either system administration accounts, accounts owned by the TCCSA staff, or application/operating system administration accounts. None of the accounts belong to member school district users.
WORLD access is absent from the SYSUAF.DAT, NETPROXY.DAT and RIGHTSLIST.DAT security files.	Obtained the file directory listing for the system directories and reviewed the file protection masks on the SYSUAF.DAT, NETPROXY.DAT and RIGHTSLIST.DAT files.	The security files NETPROXY.DAT and RIGHTSLIST.DAT, have no WORLD access. Read access at the WORLD level has been provided to the SYSUAF.DAT file.

<table>
<tr><td colspan="2"><b>Computer Security -</b> <i>Control Objective:</i>
<b>Physical Security</b> - Computer facilities and data should have appropriate physical access restrictions and be property protected from environmental dangers.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>Physical security controls include a key pad entry system and motion detectors.</td><td>Observed existence and use of the key pad entry devices throughout the period of fieldwork. Observed the existence of motion detection equipment.</td><td>Key pad entry devices protect the entrance into the computer room. Motion detectors are located just outside the entrance of the computer room, and throughout the offices of TCCSA.</td></tr>
<tr><td>Environmental controls include smoke detectors, temperature and humidity controls, elevated flooring and fire extinguishers.</td><td>Toured the computer room and observed the existence of the listed environmental controls.</td><td>An air conditioning system is used to control temperature and humidity. Fire extinguishers which are located in the computer room and through out the offices of TCCSA were tested in May of 2000. Elevated flooring is utilized in the computer room.</td></tr>
<tr><td>All data center equipment is covered by insurance.</td><td>Obtained and reviewed the signed copy of the property insurance policy for the period from 02/01/98 through 02/01/01 from the Executive Director.</td><td>The data center equipment and software are covered by the insurance policy.</td></tr>
<tr><td colspan="3"><b>Member School District User Control Considerations:</b>
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.</td></tr>
</table>

Computer Operations

Computer Operations - *Control Objective:* **Batch Processes** - Batch processes that must be run at specific times (e.g., daily, weekly, month-end, and year-end) should be documented, scheduled, and maintained on an ongoing basis.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The TCCSA performs certain routine jobs for reporting EMIS data automatically through various programs and a scheduling program call DECScheduler.	Obtained and reviewed the programs and DECScheduler jobs responsible for the automation of EMIS reporting.	EMIS reporting is an automated process accomplished through programs and DECScheduler. The reporting is scheduled to be performed on specific days of the week through DECScheduler.

Computer 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:*
Full system backups are initiated Monday through Friday for the Alpha system with the use of a batch job scheduler program.	Obtained and reviewed the DECScheduler list of jobs and a printout of the backup program. Obtained and reviewed copies of the backup log and system generated backup reports for indications that backups were performed throughout the audit period.	Backups are scheduled through DECScheduler to be performed Monday through Friday at 11:00 p.m. Two tapes are created which contain operating system files and user data.
Backups are taken off-site twice a week.	Observed the rotation of backups to the off-site location. Obtained and reviewed the backup log for documentation of the rotation of backups off-site.	The Manager of Network Operations took the second most recent and the third most recent set of backup tapes to the offsite facility located approximately five blocks away from the offices of the TCCSA. He returned with two sets of backup tapes from the previous week. Logs document backup rotation.

<table>
<tr><td colspan="2"><b>Computer Operations -</b> <i>Control Objective:</i>
<b>Backup</b> - Up-to-date backups of programs and data should be available in emergencies.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td colspan="3"><b>Member School District User Control Considerations:</b>
Member school districts 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.
Member school districts should establish and enforce a formal data retention schedule with the TCCSA for the various application data files.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Computer Operations -</b> <i>Control Objective:</i>
<b>Disaster Recovery</b> - Adequate plans should exist for the recovery of critical computer resources following an event which disrupts data processing services for an extended period of time.</td><td><b><i>Control Objective Has NOT Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>The TCCSA has entered into reciprocal agreements with ACCESS, and LACA for use of their computer facilities in the event of a disaster.</td><td>Obtained and reviewed the reciprocal agreements.</td><td>The TCCSA has reciprocal agreements with ACCESS and LACA.</td></tr>
<tr><td colspan="3"><b>Member School District User Control Considerations:</b>
Member school districts should develop, test and maintain contingency procedures to be performed in the event of an extended loss of computer resources. Such procedures should be established based upon the maximum outage tolerances for critical applications.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Computer Operations -</b> <i>Control Objective:</i>
<b>Recovery from Operational Failures</b> - There should be appropriate procedures to ensure that operational failures (e.g., disk drive problems, program ABENDS, and other emergencies) are identified, resolved in a timely manner, and where appropriate, approved respectively by appropriate IT staff and user.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>A maintenance utility is scheduled through the DECScheduler program to perform maintenance on a regular basis.</td><td>Obtained and reviewed the DECScheduler job listings.</td><td>A disk utility is used to perform routine maintenance, such as disk de-fragmentation to the hard drives of the Alpha system. It is scheduled to run on a weekly basis.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Computer Operations -</b> <i>Control Objective:</i>
<b>Recovery from Operational Failures</b> - There should be appropriate procedures to ensure that operational failures (e.g., disk drive problems, program ABENDS, and other emergencies) are identified, resolved in a timely manner, and where appropriate, approved respectively by appropriate IT staff and user.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>The TCCSA has hardware maintenance agreements with Compaq, Data Serv Inc. and Cisco Systems.</td><td>Obtained and reviewed hardware maintenance agreements in place during the audit period. Obtained and reviewed payment documentation for the Cisco agreement.</td><td>The TCCSA has ongoing maintenance agreements with Compaq, Data Serv Inc and Cisco Systems for support of the TCCSA computer systems.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Computer Operations -</b> <i>Control Objective:</i>
<b>Upgrades to System Software</b> - The selection of new software or upgrades to existing system software (e.g., operating system, plus any supplemental software in areas such as security, scheduling of batch processes, and networking) should not cause processing errors or undermine system software-based controls.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>The NBEC, who acts as the fiscal agent for this and other participating DAS, has entered into a license under the Campuswide Software License Grant (CSLG) program through the Management Council of the Ohio Education Computer Network (MC-OECN), in acquiring and/or providing software maintenance services for a limited series of Compaq software packages.</td><td>Obtained a copy of the CSLG agreement the NBEC has with the TCCSA to ensure the agreement is current.</td><td>The TCCSA has a current signed agreement with the NBEC for the period of July 1, 1999 to June 30, 2000.</td></tr>
</table>

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

CONSORTIUM PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Consortium Name:	Tri-County Computer Services Association (TCCSA)
Consortium Number:	19
Node Name:	TCCSA
Consortium Chairperson:	Edward Swartz Superintendent Tri-County Educational Services Center
Fiscal Agent District:	Tri-County Educational Services Center
Data Acquisition Site Administrator:	Stuart Workman Executive Director TCCSA
Site Administrator's Address:	2125-B Eagle Pass Wooster, OH 44691
Site Administrator's Telephone:	330-264-6047
FAX:	330-264-5703
Data Center Address:	2125-B Eagle Pass Wooster, OH 44691
Data Center Telephone:	330-264-6047

OTHER SITE STAFF

Jim Franks	Manager of Software Applications and Support
Sherry Williams	Assistant Manager of Software Applications and Support
John R. VanLanen	Manager of Network Operations
Brad Humrichouser	LAN Administrator
Doug Ackerman	Field Services Technician
Philip McNaull	Field Services Technician
Jonathan Johnson	Field Services Technician
Roger Doty	Field Services Technician
Roy Templeman	Field Services Technician
John Beno	Workstation Repair
Deb Carroll	Software Support Specialist
Joseph Picking	Educational Technology Coordinator
Kennard Meng	Technology Coordinator
Mary Barber	Educational Technologist
Thomas Grandy	Educational Technologist
Joanne Porr	Educational Technologist
Kim Suppes	Secretary
Alice Rehm	Secretary - Part Time

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	GS 60	Lines/Ports:	N/A	Memory Installed:	3 GB
Disk:	RZ1EF	Units:	2	Total Capacity:	36.0 GB
Disk:	RZ229	Units	11	Total Capacity:	49.5 GB
Tape Unit:	TZ89	Units:	1	Max Density:	N/A
Tape Unit:	TZ207	Units:	1	Max Density:	9 track 6250
Printer:	HP 2566	Units:	1	Print Speed:	900 LPM
Printer:	HP 2562	Units:	1	Print Speed:	450 LPM

CPU Unit 2

Model Number		Installed		Capacity/Density/Speed	
CPU:	DEC Alpha Server 1000/233	Lines/Ports:	N/A	Memory Installed:	256 Mb
Disk:	RZ29B	Units:	1	Total Capacity:	4.3 GB
	RZ28		1		2.1 GB
	RZ1ED		2		36.4 GB
	RZ1DN		2		18.2 GB
Tape Unit:	TL06	Units:	1	Max Density:	4.0 GB Dat

CPU Unit 3

Model Number		Installed		Capacity/Density/Speed	
CPU:	DEC VS 4000	Lines/Ports:	N/A	Memory Installed:	32 MB
Disk:	RZ25	Units:	1	Total Capacity:	426 MB
Disk:	RRD42CDROM	Units:	1	Total Capacity:	600 MB
Tape Unit:	TTI 8mm	Units:	2	Total Capacity:	8mm

MEMBER SCHOOL DISTRICT SITE DATA

IRN	MEMBER SCHOOL DISTRICT	COUNTY	USAS	USPS	SAAS/EIS	EMIS
062042	Ashland County - West Holmes JVSD	Ashland	X	X	X	X
043505	Ashland City SD	Ashland	X	X	X	X
045823	Hillsdale Local SD	Ashland	X	X	X	X
045468	Loudonville-Perrysville Ex Village SD	Ashland	X	X	X	X
045831	Mapleton Local SD	Ashland	X	X	X	X
047688	East Holmes Local SD	Holmes	X	X	X	X
047696	West Holmes Local SD	Holmes	X	X	X	X
044974	Wadsworth City SD	Medina	X	X	X	X
050534	Chippewa Local SD	Wayne	X	X	X	X
050542	Dalton Local SD	Wayne	X	X	X	X
050559	Green Local SD	Wayne	X	X	X	X
050567	North Central Local SD	Wayne	X	X	X	X
050575	Northwestern Local SD	Wayne	X	X	X	X
044610	Orrville City SD	Wayne	X	X	X	X
045591	Rittman Ex Village SD	Wayne	X	X	X	X
050583	Southeast Local SD	Wayne	X	X	X	X
050526	Tri-County Educational Service Center	Wayne	X	X	X	X
050591	Triway Local SD	Wayne	X	X	X	X
051714	Wayne County JVSD	Wayne	X	X	X	X
045120	Wooster City SD	Wayne	X	X	X	X
TOTALS:			**20**	**20**	**20**	**20**

State of Ohio
Office of the Auditor

Jim Petro, Auditor of State

88 East Broad Street
P.O. Box 1140
Columbus, Ohio 43216-1140

Telephone 614-466-4514
800-282-0370

Facsimile 614-466-4490

TRI - COUNTY COMPUTER SERVICES ASSOCIATION

WAYNE 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 5, 2000