TRI-COUNTY COMPUTER SERVICES ASSOCIATION (TCCSA)
STATE REGION - ISA, WAYNE COUNTY

SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

APRIL 1, 2010 THROUGH MARCH 31, 2011

Dave Yost · Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

Board of Directors
Tri-County Computer Services Association (TCCSA)
2125-B Eagle Pass
Wooster, Ohio 44691

To Members of the Board:

Scope
We have examined TCCSA's description of its Alpha GS60 system used for processing 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), throughout the period April 1, 2010 to March 31, 2011 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of TCCSA's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The TCCSA uses the North West Ohio Computer Association (NWOCA) service organization for systems development and maintenance of the USAS, USPS, SAAS/EIS and EMIS. The description in section 3 includes only the controls and related control objectives of the TCCSA and excludes the control objectives and related controls of the NWOCA. Our examination did not extend to controls of the NWOCA.

Service organization's responsibilities
In section 2, TCCSA has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. TCCSA is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period April 1, 2010 to March 31, 2011.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in section 3. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The information in section 5 describing the information technology center is presented by the management of TCCSA to provide additional information and is not part of the TCCSA's description of controls that may be relevant to a user entity'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 entities and, accordingly, we express no opinion on it.

Inherent limitations
Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion
In our opinion, in all material respects, based on the criteria described in TCCSA's assertion in section 2,

a. the description fairly presents the system that was designed and implemented throughout the period April 1, 2010 to March 31, 2011.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2010 to March 31, 2011 and user entities applied the complementary user entity controls contemplated in the design of the TCCSA's controls throughout the period April 1, 2010 to March 31, 2011.

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period April 1, 2010 to March 31, 2011.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Restricted use
This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of TCCSA, user entities of TCCSA's system during some or all of the period April 1, 2010 to March 31, 2011, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Dave Yost
Auditor of State

August 12, 2011

This Page Intentionally Left Blank

TRI-COUNTY COMPUTER SERVICES ASSOCIATION
Midland Council of Governments
2125 Eagle Pass
Wooster, Ohio 44691-5320
Phone: (330)264-6047 Fax: (330)264-5703

August 12, 2011

We have prepared the description of Tri-County Computer Services Association (TCCSA) Alpha GS60 system for user entities of the system during some or all of the period April 1, 2010 to March 31, 2011, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a) the description fairly presents the Alpha GS60 system made available to user entities of the system during some or all of the period April 1, 2010 to March 31, 2011 for processing their transactions. The criteria we used in making this assertion were that the description

   i) presents how the system made available to user entities of the Alpha GS60 system was designed and implemented to process relevant transactions, including

      1) how the system captures and addresses significant events and conditions, other than transactions.

      2) the process used to prepare reports or other information provided to user entities' of the system.

      3) specified control objectives and controls designed to achieve those objectives.

      4) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

   ii) does not omit or distort information relevant to the scope of the Alpha GS60 system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Alpha GS60 system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b) the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c) the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period April 1, 2010 to March 31, 2011 to achieve those control objectives. The criteria we used in making this assertion were that

i) the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii) the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely,

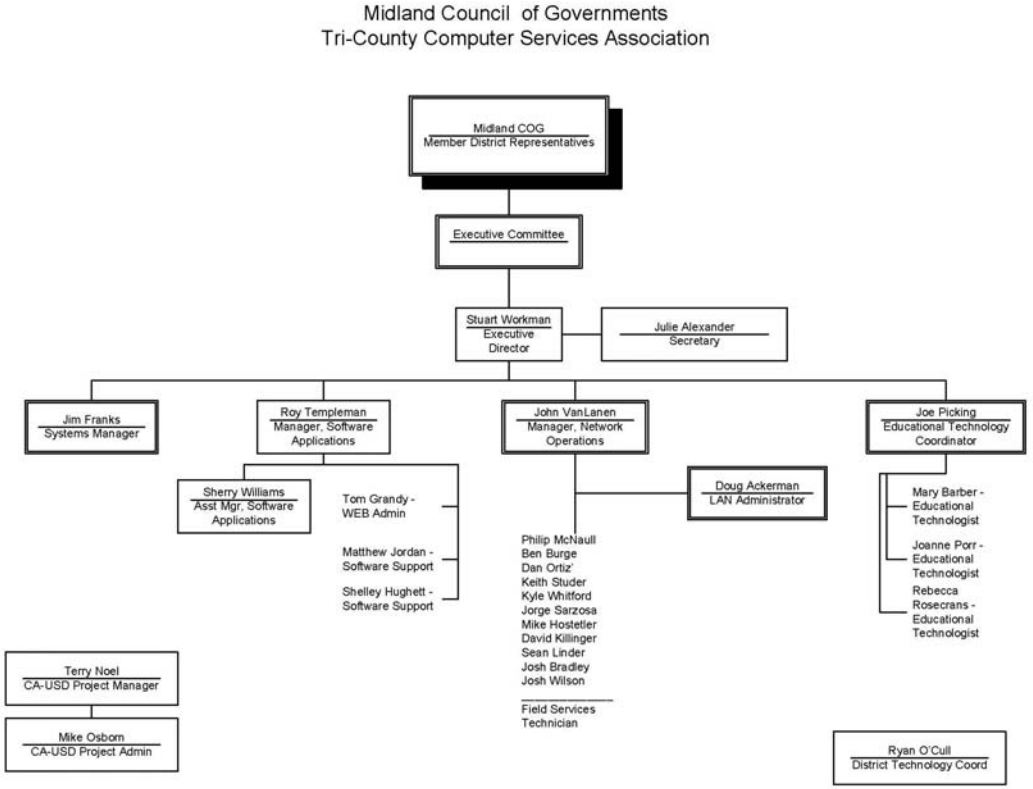
Stuart Workman
Executive Director, TCCSA

SECTION 3 - DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

The TCCSA's control objectives and related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results," to eliminate the redundancy that would result from listing them here in section 3 and repeating them in section 4. Although the control objectives and related controls are included in section 4, they are, nevertheless, an integral part of the TCCSA's description of controls.

OVERVIEW OF OPERATIONS



The TCCSA is one of 23 governmental computer service organizations serving more than 900 educational entities and 1.4 million students in the state of Ohio. These service organizations, known as Information Technology Centers (ITCs), and their users make up the Ohio Education Computer Network (OECN) authorized pursuant to Section 3301.075 of the Revised Code. Such sites, in conjunction with the Ohio Department of Education (ODE), comprise a statewide delivery system to provide comprehensive, cost-efficient accounting and other administrative and instructional computer services for participating Ohio entities. Funding for this network and for the TCCSA is derived from the state of Ohio and from user fees.

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

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

ITCs are organized as either consortia under ORC 3313.92 or Council of Governments (COG) under ORC 167. ORC 3313.92 allows for school districts to create a partnership (a consortia) to resolve mutual needs. One of the members of the consortia is designated as fiscal agent. The fiscal agent provides all accounting, purchasing, and personnel services for the consortia. A "COG" under ORC chapter 167 allows for one or more governmental entities to join together to form a new legal entity. A COG can have its own treasurer, make its own purchases, hire staff, and have debt obligations. The TCCSA is a subsidiary of the Midland Council of Governments (MCOG) organized under ORC 167. The MCOG serves as fiscal agent for the TCCSA.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and two oversight committees. Two members from each user entity are appointed to the legislative body of the council known as the assembly and are normally the user entity's superintendent and treasurer. The assembly meets at least twice per year to estimate program costs, approve annual appropriations, select officers and other 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 members and two ad hoc members. The composition of the executive committee includes two superintendents, two treasurers, two members at-large, and the educational service center superintendent. The executive director of TCCSA and the MCOG treasurer are the two ad hoc members. The executive committee is required to meet every two months.

The TCCSA employs a staff of 28 individuals, including the executive director, 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.
Educational Technology Support:	Facilitates the implementation and operation of educational technology services to TCCSA user entities 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.
Help Desk Support:	Implements and supports the Computer Associates™ help desk software, named Unicenter Service Desk (USD).

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 (MCOG). When necessary, additional TCCSA policies have been developed and approved by the MCOG board to address concerns of the TCCSA. Detailed job descriptions exist for all but two positions related to support of the helpdesk application software. 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.

The TCCSA's hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the organization require some type of college degree in a computer-related field, and all of the TCCSA staff members are required to attend professional development and other training as a condition of continued employment. Each full-time staff member must attend at least 20 hours of approved professional development training annually, and training hours for part-time staff members are prorated. In addition, management encourages staff members to obtain additional training and pays 100% of incurred costs of attending professional development seminars. Employee evaluations are conducted annually. The board performs an annual evaluation of the executive director.

TCCSA is also subject to ITC site reviews by the Technology Solutions Group of the Management Council – Ohio Education Computer Network MCOECN (mc•tsg). These site reviews are conducted by a team consisting of an employee of the Ohio Department of Education (ODE), two current and/or former school district administrators, two current and/or former ITC Directors, and one additional team member to provide training to subsequent teams. Approximately three to five ITC site reviews are conducted annually. The sites chosen for review are designated by the OECN Oversight Advisory Committee as approved by ODE. The guidelines and recommended procedures for these reviews are based on the Ohio Administrative Code, which cover the following areas: governance, administration, finance, personnel and staff development, physical facilities, hardware, software, user in-service, and operations. TCCSA's site review has not been scheduled.

Risk Assessment

The TCCSA does not have a formal risk management process; however, the TCCSA executive committee is made up of user entity representatives 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 user entities and other entities.
- Changes in the operating environment as a result of ODE requirements, Auditor of State (AOS), and other accounting pronouncements, and legislative issues.

In addition, the TCCSA has identified operational risks resulting from the nature of the services provided to their user entities. 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 structure of the TCCSA data center has been organized to provide a quick response to service problems. Employee positions are broken down between application support and technical support. Software and technical support managers report directly to the executive director. 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. To assist them in this monitoring, TCCSA uses a variety of "key indicator" reports to monitor the processes involved in processing transactions for user entities.

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 user entities are discussed within the General EDP control section.

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

The TCCSA staff members do not perform system development activities. Instead, the TCCSA utilizes the software developed and supplied by the State Software Development Team (SSDT), located at the North West Ohio Computer Association (NWOCA), another 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 (OASBO), the Ohio Department of Education (ODE) and the SSDT. The SAC meets four times per year to discuss the status of proposed and ongoing projects.

Changes to Existing Applications and 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 entities have access to forum conferences, providing end-user participation in the program development/change process.

The TCCSA 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 TCCSA 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 license under the Campuswide Software License Grant Program (CSLG) through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of Hewlett Packard (HP) software packages.

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

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

- Provide telephone technical support to the participant's 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 TCCSA, a backup of the application or operating system affected by the change is prepared to ensure retention of the existing application or operating system in case of an error stemming from the upgrade process.

Documentation for the current version of the OpenVMS operating system and new releases are provided on the HP web site. New releases include documented changes to the operating system and implementation procedures. In addition, the MCOECN provides all ITCs with purchasing discounts on hardware and software through the Technology Solutions Group program under the MCOECN (mc•tsg).

IT Security

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

The TCCSA staff is granted access within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities. Access for TCCSA employees is established, granted and reviewed by the executive director or manager of software applications and support. Access authorization forms are not used for TCCSA employees.

User entity personnel are granted access upon the receipt of a written authorization form from the user entity's superintendent and a signed network privacy and acceptable use form from the user. Both forms for are maintained at TCCSA.

Student authorization forms for Internet and e-mail accounts are maintained at the user entity. These accounts have no access to data on the Alpha server.

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/or security audits have been enabled through OpenVMS to monitor security violations on the TCCSA 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:	Enabled by default to produce a record of when other security alarms were enabled or disabled.
AUTHORIZATION:	Enables monitoring of changes made to the system user authorization file (UAF) or network proxy authorization file in addition to changes to the rights database.
BREAK-IN:	Produces a record of break-in attempts. The DIALUP, LOCAL, REMOTE, NETWORK, and DETACHED break-in types can be monitored.
LOGIN:	Provides the ability to audit successful logins by specifying the LOGIN keyword with the /ENABLE qualifier of the SET AUDIT command. The following login types can be audited: BATCH, DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESS, and DETACHED.
LOGFAILURE:	Provides a record of logon failures. The BATCH, DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESS and DETACHED logon failure types can be monitored.

The TCCSA provides their user entities with a listing of user email accounts from the Active Directory server on an annual basis. User entities are asked to review the listing and identify any accounts that should be removed. When the accounts are removed from the Active Directory server, any corresponding OpenVMS account is also deleted. The OpenVMS system houses the fiscal and EMIS applications. Application identifiers, which indicate user capabilities within each application, are not confirmed in this process.

The TCCSA uses Sophos Anti-Virus software, which interactively scans all inbound and outbound e-mail.

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

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.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the TCCSA. To promote user accountability, UICs are individually assigned to each user at the user entity. UIC based protection controls access to objects such as files, directories, and volumes.

The CAPTIVE and RESTRICTED flags are used for various application and system utility accounts. The CAPTIVE and RESTRICTED flags are typically not used for system administrative accounts (TCCSA staff members) because access to the DCL prompt is necessary for them to perform their job duties. Additionally, user accounts are not typically set with CAPTIVE or RESTRICTED flags, as their logins are captured within a menu system preventing access to the DCL command line. User accounts are also set with the NORMAL parameter giving them the minimum level of access privileges. UIC based protection to production programs and data prevents WORLD write or delete access.

The system forces users to change their passwords on a periodic basis. All general user accounts as well as all TCCSA staff member accounts, have a standard password lifetime. System or application maintenance accounts on the system have significantly longer password lifetimes. These accounts do not affect financially significant functions and are not able to access financial applications. Passwords are set to expire when a new user identification code is issued or when a user has forgotten his password. This parameter requires the user to change his password during the first logon procedure. A minimum password length for user and administrative accounts has been established. An identifier has been assigned to user entity personnel to aid in the resetting of passwords.

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 enter a correct 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.

System parameter standards have been established using established defaults. Changes to system parameters are logged and reviewed by the executive director or by the manager of software applications and support 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 non-use. The use of this program helps to reduce the risk of an unattended terminal being used to enter unauthorized transactions. In addition, timeout programs aid in the efficient use of system resources by maintaining connectivity with only active system users. A session timeout parameter for the USAS Web and USPS Web applications has been set to log users off the system after a pre-determined period of inactivity.

Associated with each object recognized by OpenVMS may be an access control list (ACL). When an access request is made to an object, ACLs are always checked first. An ACL may either grant or deny access to the user. 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 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 SYSGEN parameter for MAXSYSGROUP. (2) Users with system privileges (SYSPRV). (3) Users with group privileges (GRPPRV) whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

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

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

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

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

Certain privileges can override all UIC-based and ACL protection. OpenVMS analyzes privileges included in the user authorization file (UAF) record for each user 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 personnel, at the user entity, have NORMAL privileges.

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 TCCSA 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.

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 OpenVMS 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 the USAS, USPS, SAAS/EIS and EMIS application data files.

User entities have been set up with sub-networks which have addresses not recognizable to the Internet. Firewall equipment and routing devices deny all outbound traffic requests originating from the sub-network. Instead, the requests are routed to the firewall where an address translation is performed. The firewall and routing devices also deny access to all inbound traffic unless it is bound for the firewall. User entity management may request alterations to the firewall by sending an email or initiating a help desk ticket. Requests that are received via email are eventually entered into the help desk application by either the manager of network operations or the technical support specialist. These individuals inform the user of the risk associated with the requested configuration changes. The process of requesting changes to the firewall configuration was implemented in 2005. Documentation for firewall configuration changes is not available for changes requested prior to 2005.

TCCSA also makes available an Internet content filter. The filter is an optional service, which screens Internet site requests for unsuitable content.

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. The doors to the computer room are always locked and are 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:

- Hand-held fire extinguishers.
- Air conditioning/humidity control devices.
- The computer room contains a UPS (Un-interruptible Power Supply) and a generator to provide power to key computer components for a short period during power interruptions.
- The computer room has a raised floor to reduce the risk of damage from flooding.

IT Operations

Traditional computer operation procedures are minimal since user entity personnel initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. In addition, every employee has access to SiteScape Forum, which is a billboard system that addresses a variety of problems common to Alpha users.

The TCCSA staff maintains a listing of individuals to contact in the event of complications with the hardware environment. A service agreement with HP 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 to the console log maintained by the system. A hardware error log, which documents errors identified by the OpenVMS operating system, is reviewed by the executive director and the manager of software applications and support. TCCSA also has service agreements, which cover the communication and firewall equipment.

"What's up Gold" is used to monitor network communication problems and equipment outages in a real time setting. "Down" equipment is displayed on a web interface. Users also play a key role in identifying problems by contacting TCCSA when hardware or software problems are encountered.

User entity personnel are responsible for handling abnormal terminations. If users cannot solve the problem, they may contact TCCSA staff. TCCSA security practices prohibit the alteration of user entity data by TCCSA staff members. Data entry or processing errors must be corrected by user entity personnel within the context of the application. User entities have the option of printing an AUDIT report that shows all activity changes to their data files.

Certain routine jobs are initiated for system maintenance. TCCSA is responsible for operational maintenance tasks, such as system backups, log reports, and other maintenance directed at the whole system. These processes are automatically initiated with the use of DECScheduler. DECScheduler is a scheduling program that continually submits jobs on the Alpha system.

Individual user entities are responsible for running their own regular reports, which are batch processes. Batch processes are initiated and completed by the individual user entities; however, TCCSA does run some batch processes for the processing of EMIS data.

TCCSA helps prevent database failure or corruption using a program called Perfect Disk, which is run through DECScheduler. Perfect Disk scans all files once a week to verify all files are readable (e.g., no bad blocks, sectors or chains). Data integrity is maintained by the software through validity checks of all input. Every time the Perfect Disk program is run, an e-mail is sent to the executive director.

Full backups of user entity data are performed Monday through Friday on the production server. The backup cartridges are stored in a robotic tape silo inside the StorServer appliance and are rotated off-site to a safety deposit box at least twice a week.

Calendar year and fiscal year end backups are initiated manually. This information is stored indefinitely for all TCCSA user entities.

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

COMPLEMENTARY USER ENTITY CONTROLS

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

General EDP Control Procedures

1. User entities should have controls over their own web applications which access their data stored at the ITC to ensure only thoroughly tested and authorized web applications are implemented.

2. User entity management should have practices to ensure users are aware of the security policies of their ITC and that users take precautions to ensure passwords are not compromised.

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

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

5. User entities should have documented acceptable use policies to define the activities deemed appropriate for use of the Internet. Internet users should be required to accept the terms of the policy before access is provided.

6. Access privileges should only be issued to authorized users who need access to computer resources to perform their job function.

7. 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.

8. Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.

9. User entities 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.

10. User entities should establish and enforce a formal data retention schedule with their ITC for the various application data files.

The complementary user entity controls presented above do not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at the user entity.

SECTION 4 - INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

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 entity'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 user entities that 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

Changes to Existing Applications and Systems

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
In order to maintain continued support of the application software provided by SSDT, ITCs are required to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the USAS, USPS, SAAS/EIS, and EMIS object files at TCCSA was compared to the CRCs of the object files at NWOCA.	No exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements, and problems corrected. Updated user and system manuals for the applications are also made available.	Inspected the release notes and updated manuals for the most recent releases.	No exceptions noted.
Documentation for the current version of the operating system and new releases are provided on the HP web site.	Inspected the online manuals for the operating system at the HP web site.	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 TCCSA has established a data system security policy and a network privacy and acceptable use policy to outline user responsibilities regarding computer security and access. The policies are maintained on TCCSA's web site and are accessible by the user entities.	Inspected the data system security policy and the network privacy and acceptable use policy to confirm user responsibilities are documented. Inspected TCCSA's web site to confirm the policies are available online.	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:*
Authorization from the user entity's superintendent is required before setting up a user account on the system. The network privacy and acceptable use policy must be signed by the user to acknowledge their review and consent of the policy.	Identified all active accounts having identifiers granting access to the USAS, USPS, SAAS/EIS, and EMIS applications. Selected 60 user accounts from a population of 544 active accounts and inspected the user access authorization forms and the network privacy and acceptable use forms to confirm the required forms and signatures were present.	No exceptions noted.
Detection control alarms are enabled through OpenVMS to track security related events, such as break-in attempts and excessive login failures. The events are logged to audit journals for monitoring of potential security violations.	Inspected the security alarms enabled. Confirmed the procedures for reviewing the audit journals with the executive director.	Security alarms have been enabled; however, the logs are not reviewed on a consistent basis.
A positive confirmation of user e-mail accounts from the Active Directory server is performed annually with user entity management. User entity management is asked to identify user e-mail accounts that should be deleted. When the accounts are deleted from the Active Directory server, any corresponding Open VMS account is also deleted. The Open VMS system houses the fiscal and EMIS applications.	Inspected the confirmation tracking spreadsheet maintained by the TCCSA secretary during the confirmation process. Inspected the confirmation request prepared for one user entity during the audit period. Searched the system authorization file to ensure corresponding OpenVMS accounts were deleted for email accounts deleted per the annual confirmation.	The confirmation process does not include a listing of the application identifiers that indicate user capabilities within each financial application. No other 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:*
Anti-virus software is installed on the MailMarshal server and user terminals. Definitions are updated daily, and infected items are quarantined to help prevent and detect computer viruses.	Inspected the following information, relating to the Sophos anti-virus software, to confirm anti-virus software is actively scanning for viruses: • Sophos properties that indicate frequency of update and the server upon which the software is installed. • MailMarshall Configurator for virus scanners policy elements. • MailMarshal Configurator for inbound anti-virus e-mail policy. • MailMarshal Configurator for inbound content security e-mail policy. • Listing of virus detections for one week in July 2011.	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 TCCSA. The number of profiles with pre-expired passwords is limited. The OECN_RPC logical has been set to prevent users of the web applications from logging in with expired passwords.	Extracted information from the user authorization file to identify: • User accounts with a password minimum length less than TCCSA's standard. • User accounts with a password minimum length less than TCCSA's standard. • User accounts with pre-expired passwords. Inspected the results of the extracted information and inquired with the executive director regarding the appropriateness of the accounts. Inquired with the executive director whether the OECN_RPC logical has been set to prevent users from logging into the web applications with expired passwords.	Of the 887 enabled accounts on the system, the following exceptions were noted: • There were 75 accounts with a password lifetime greater than TCCSA's standard of 90 days. These accounts consisted of system or utility accounts (10), inquiry accounts for the library catalog (37), training accounts (25), and OECN accounts (3). • There were 193 accounts with pre-expired passwords. These accounts consisted of district user accounts (115), system and application accounts that do not register an interactive login (30), student training accounts (26), support accounts (8), miscellaneous auditor accounts (10), substitute teach accounts (3) and an EMIS processing account. The web application logical has not been defined at TCCSA. As a result, password expiration parameters do not apply to accounts using the web applications only. No other 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:*
Individual user profiles are used to grant access rights and privileges. The user profiles on the system do not consist of an excessive number of inactive or disabled users.	Extracted the following information from the user authorization file: • Inactive user accounts, defined as those accounts that have not been logged into in 180 days. • User accounts that have never logged into the system. Inspected the results of the extracted information and inquired with the manager of applications and support regarding the appropriateness of these accounts.	Of the 887 enabled accounts on the system, the following exceptions were noted: • There were 443 accounts that have not been logged into in over 180 days. • There were 78 accounts that have never been logged into the system. The majority of these accounts are user accounts that have been enabled for e-mail access only or for individuals using the web applications. The e-mail server and the web applications do not register logins against the user authorization file.
A password change identifier is used to enable user entity personnel to reset passwords in the event someone at the user entity forgets their password. The identifier is restricted by user entity and is normally granted to treasurers, technical coordinators and EMIS coordinators.	Inspected the user accounts having the password change identifier and inquired with the executive director regarding ownership of the listed accounts.	No exceptions noted.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameter settings.	No exceptions noted.
Log-in scripts are used to restrict user access to the command prompt.	Extracted information from the user authorization file to confirm the use of login scripts. Inspected the login scripts for each user entity to confirm the login scripts were captive in nature restricting the users to only the OECN menu system.	No exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls -** Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A program, HITMAN, constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed at startup.	Inspected the HITMAN parameters (prime and non-prime) to confirm they were set to automatically logoff inactive users. Inspected the startup file to confirm the HITMAN utility is part of the startup procedures.	Several images for check and purchase order processing have been excluded from termination. In addition, three accounts have been excluded from termination. They consist of the following: • A generic backup account used to initiate backups. • An account used by libraries for online public access. • Executive director's account. No other exceptions noted.
A timeout parameter, provided through the OECN web access menu system, logs off users after a period of inactivity.	Inspected the OECN web terminal log off parameters for the web based application systems to confirm TCCSA is logging off inactive web application users.	No exceptions noted.
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts are specifically defined to prevent blanket access.	Inspected the network proxy listing to confirm wild card characters were not used.	No exceptions noted.
Access to production data files and programs is properly restricted.	Identified and inspected production data files with WORLD access and executable 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:*
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user entities.	Firewall and network equipment was observed to confirm the existence of the equipment that controls internet traffic. The firewall configuration was inspected for evidence that Internet traffic is restricted through the firewall. Selected six static IP mappings and requested documentation to support the configuration changes within the TCCSA helpdesk software.	Two of the six configuration settings were not documented in the helpdesk software. They were originally configured before the use of the helpdesk software to document firewall changes. No other exceptions noted.
The TCCSA internal network uses a private internal addressing scheme, which is unable to be used over the Internet.	Inspected a listing of current users by using an operating system command to confirm TCCSA user entities use a ten-dot addressing scheme.	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.	A listing of all identifiers was extracted from the user authorization file for evidence of the use of identifiers to segregate access to the applications. Confirmed use of the OSA utility and the process used to assign application identifiers with the executive director.	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:*
A user access authorization form is used by TCCSA to establish application accounts. Included on the agreement form are the user name, user entity, and privileges granted.	Selected 60 user accounts from a population of 544 active accounts with audit significant identifiers. Inspected the access authorization forms to confirm the identifiers actually granted were authorized.	Three of the 60 accounts were found to have full USAS access that was not explicitly authorized on the authorization form or by TCCSA's undocumented business practices.

IT Security - *Control Objective:* **System Software and Utilities Access Controls -** Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized personnel as determined by TCCSA management.	Extracted accounts from the user authorization file with the OECN_SYSMAN identifer. Inspected the listing and inquired with the executive director regarding the appropriateness of the listed accounts.	No exceptions noted.
WORLD access to "key" system and security files is restricted.	Identified system files with WORLD write and/or delete access. Inspected the file protection masks on the security files to confirm WORLD access was absent.	No exceptions noted.

IT Security - *Control Objective:* **System Software and Utilities Access Controls -** Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
System level UICs are restricted to authorized personnel. UICs belonging to the system group are determined by the parameter value for MAXSYSGROUP. UICs less than the MAXSYSGROUP value have system level privileges.	Identified the MAXSYSGROUP value. Extracted accounts from the user authorization file to identify accounts with a UIC less than the MAXSYSGROUP value. Inspected the listed accounts and inquired with the manager of software applications and support regarding the appropriateness of the accounts.	No exceptions noted.
Accounts on the system with elevated privileges, defined as those accounts having more than the minimum privileges to use the system or participate in groups, is limited to authorized personnel as determined by TCCSA staff.	Extracted accounts from the user authorization file to identify accounts with elevated privileges. Inspected the listed accounts and inquired with the manager of software applications and support regarding the appropriateness of the accounts.	One support account used by a former staff member was noted. It was removed by the executive director upon notification. No other exceptions noted.
Use of an alternate user authorization file is not permitted.	Inspected the value of the alternate user authorization file parameter to determine whether an alternate file is permitted. Inspected the system directory listings to determine if an alternate user authorization file existed.	No exceptions noted.
Remote access to the firewall configuration used to control Internet access is restricted through password protection.	Inspected the firewall configuration to confirm passwords were enabled.	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 devices and existence of motion detection devices throughout the period of fieldwork.	No exceptions noted.
Environmental controls are in place to prevent data loss and damage as well as to detect fire or changes in temperature.	Observed the existence of temperature and humidity controls and elevated flooring. Inspected the TCCSA building and observed the existence of smoke detectors and fire extinguishers.	No exceptions noted.

IT Operations

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		***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 called DECScheduler.	Inspected the EMIS batch processing scripts and DECScheduler jobs responsible for the automation of EMIS reporting. Inspected the startup file to confirm that DECScheduler was initialized during the startup of the system.	No exceptions noted.
A disk maintenance utility, Perfect Disk, is scheduled with the use of the DECScheduler program to perform maintenance on a predetermined schedule. Redundant text files are purged via a scheduled procedure.	Inspected the DECScheduler program for the disk maintenance utility and the procedure for purging text files.	No exceptions noted.
TCCSA has a hardware maintenance agreement with Service Express, and DataServ for maintenance and repair of processing and network routing equipment.	Inspected the hardware maintenance agreements for services covered, period of coverage and related payment documentation.	No exceptions noted.

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Data center equipment is covered by insurance.	Inspected the insurance policy and payment documentation for evidence of coverage.	No exceptions noted.

IT Operations - *Control Objective:* **Backup -** Up-to-date backups of programs and data should be available in emergencies.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Backups of programs and data are performed regularly.	Inspected the backup command procedures for the TCCSA production servers. Inspected the DECScheduler procedures to confirm backups are scheduled daily.	No exceptions noted.
Backup tapes are stored in secure on- and off-site locations and are rotated regularly.	Inspected an inventory listing of backups maintained off-site. Inspected the on- and off-site storage facilities with the field services technician and confirmed the off-site backups agreed to the inventory listing.	No exceptions noted.

SECTION 5 - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name:	Tri-County Computer Services Association (TCCSA)
Number:	19
Node Name:	TCCSA
Chairperson:	Dr. Eugene Linton Superintendent Tri-County Educational Services Center
Fiscal Agent District:	Midland Council of Governments (MCOG)
Administrator:	Stuart Workman Executive director TCCSA
Address:	2125-B Eagle Pass Wooster, OH 44691
Telephone:	330-264-6047
FAX:	330-264-5703
Web site:	www.tccsa.net

OTHER SITE STAFF

Julie Alexander	Secretary	Keith Studer	Field services technician
Jim Franks	Systems manager	Kyle Whitford	Field services technician
Terry Noel	CA-USD project manager	Jorge Sarzosa	Field services technician
Mike Osborn	CA-USD project administrator	Mike Hostetler	Field services technician
Roy Templeman	Manager, software applications	David Killinger	Field services technician
Sherry Williams	Assistant manager, software applications	Sean Linder	Field services technician
Tom Grandy	Web administrator	Josh Bradley	Field services technician
Matthew Jordon	Software support	Josh Wilson	Field services technician
Shelley Hughett	Software support	Joe Picking	Educational technology coordinator
John VanLanen	Manager, network operations	Mary Barber	Educational technologist
Doug Ackerman	LAN administrator	Joanne Porr	Educational technologist
Philip McNaull	Field services technician	Rebecca Rosecrans	Educational technologist
Ben Burge	Field services technician	Ryan O'Cull	District technology coordinator
Dan Ortiz'	Field services technician		

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	Compaq Alpha GS60	Lines/Ports:	N/A	Memory Installed:	8.0 GB
Disk:	RZ1EF	Units:	2	Total Capacity:	80.0
Disk:	RZZ229	Units:	11	Total Capacity:	49.5 GB
Disk:	RZ29	Units:	36	Total Capacity:	655.0 GB
Tape Unit:	TZ89	Units:	1	Max Density:	N/A
Tape Unit:	TZ88	Units:	1	Max Density:	N/A
Tape Unit:	TZ207	Units:	1	Max Density:	9 track 6250
Tape Unit:	MSL5000 SDLT Tape Library	Units:	1	Total Capacity:	320GB
Printer:	HP 2566	Units:	1	Print Speed:	200 LPM
Printer:	HP 2562	Units:	1	Print Speed:	400 LPM
Backup Appliance	STORServer 3000N	Units:	1	Max Density	9.4 TB

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS/EIS	EMIS
043505	Ashland City SD	Ashland	X	X	X	X
009971	Ashland County Community Academy	Ashland	X		X	X
062042	Ashland County - West Holmes Career Center	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
048462	Black River Local SD	Medina	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
000640	Rittman Academy	Wayne	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 Schools Career Center	Wayne	X	X	X	X
045120	Wooster City SD	Wayne	X	X	X	X
TOTALS:			**23**	**21**	**23**	**23**

Dave Yost • Auditor of State

TRI-COUNTY COMPUTER SERVICES ASSOCIATION (TCCSA)

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 22, 2011

88 East Broad Street, Fifth Floor, Columbus, Ohio 43215-3506
Phone: 614-466-4514 or 800-282-0370 Fax: 614-466-4490
www.auditor.state.oh.us