HAMILTON/CLERMONT COOPERATIVE ASSOCIATION (H/CCA)
STATE REGION - ISA, HAMILTON COUNTY

SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

APRIL 1, 2015 THROUGH MARCH 31, 2016

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
Hamilton/Clermont Cooperative Association (H/CCA)
7615 Harrison Avenue
Cincinnati, OH 45231

To Members of the Board:

Scope
We have examined H/CCA's accompanying Description of its Administrative/HCCA1 system used for processing transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), and School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS) throughout the period April 1, 2015 to March 31, 2016 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 H/CCA'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 H/CCA uses the State Software Development Team (SSDT) located at the Northwest Ohio Computer Association (NWOCA) service organization for systems development and maintenance of the USAS, USPS, and SAAS/EIS application systems. The Description in section 3 includes only the controls and related control objectives of the H/CCA 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, H/CCA 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. H/CCA 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, 2015 to March 31, 2016.

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 H/CCA to provide additional information and is not part of the H/CCA'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 H/CCA's Assertion in section 2,

a. the Description fairly presents the system that was designed and implemented throughout the period April 1, 2015 to March 31, 2016.

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, 2015 to March 31, 2016 and user entities applied the complementary user entity controls contemplated in the design of the H/CCA's controls throughout the period April 1, 2015 to March 31, 2016.

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, 2015 to March 31, 2016.

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 H/CCA, user entities of H/CCA's system during some or all of the period April 1, 2015 to March 31, 2016, 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
Columbus, Ohio

June 22, 2016

This Page Intentionally Left Blank

HCCA ASSOCIATION COOPERATIVE
CLERMONT
HAMILTON

7615 Harrison Avenue
Cincinnati, Ohio 45231-3107

Telephone (513) 931-7120
FAX (513) 931-7202

Hamilton/Clermont Cooperative Association
7615 Harrison Avenue
Cincinnati, OH 45231

We have prepared the description of the Hamilton/Clermont Cooperative Association's Administrative HCCA1 /ES40 Alpha system for user entities of the system during some or all of the period April 1, 2015 to March 31, 2016 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 Administrative/HCCA1 system made available to user entities of the system during some or all of the period April 1, 2015 to March 31, 2016 for processing their transactions. The HCCA service organization uses the State Software Development Team (SSDT) located at the Northwest Ohio Computer Association (NWOCA) service organization for systems development and maintenance of the USAS, USPS, and SAAS/EIS. The description includes only the controls and related control objectives of the HCCA service organization and excludes the control objectives and related controls of the NWOCA service organization. The criteria we used in making this assertion were that the description

   i) presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including
      1) the classes of transactions processed.

      2) the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.

      3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.

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

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

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

      7) 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.

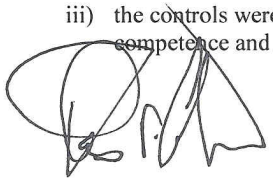
   ii) does not omit or distort information relevant to the scope of the Administrative/HCCA1 system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Administrative/HCCA1 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 Administrative/HCCA1 system during the period from April 1, 2015 to March 31, 2016
c) the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period April 1, 2015 to March 31, 2016 to achieve those control objectives and subservice organizations applied the controls contemplated in the design of HCCA service organization's controls 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 Hamilton/Clermont Cooperative Association;

   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.



Thomas F. Collins, Executive Director
June 22, 2016

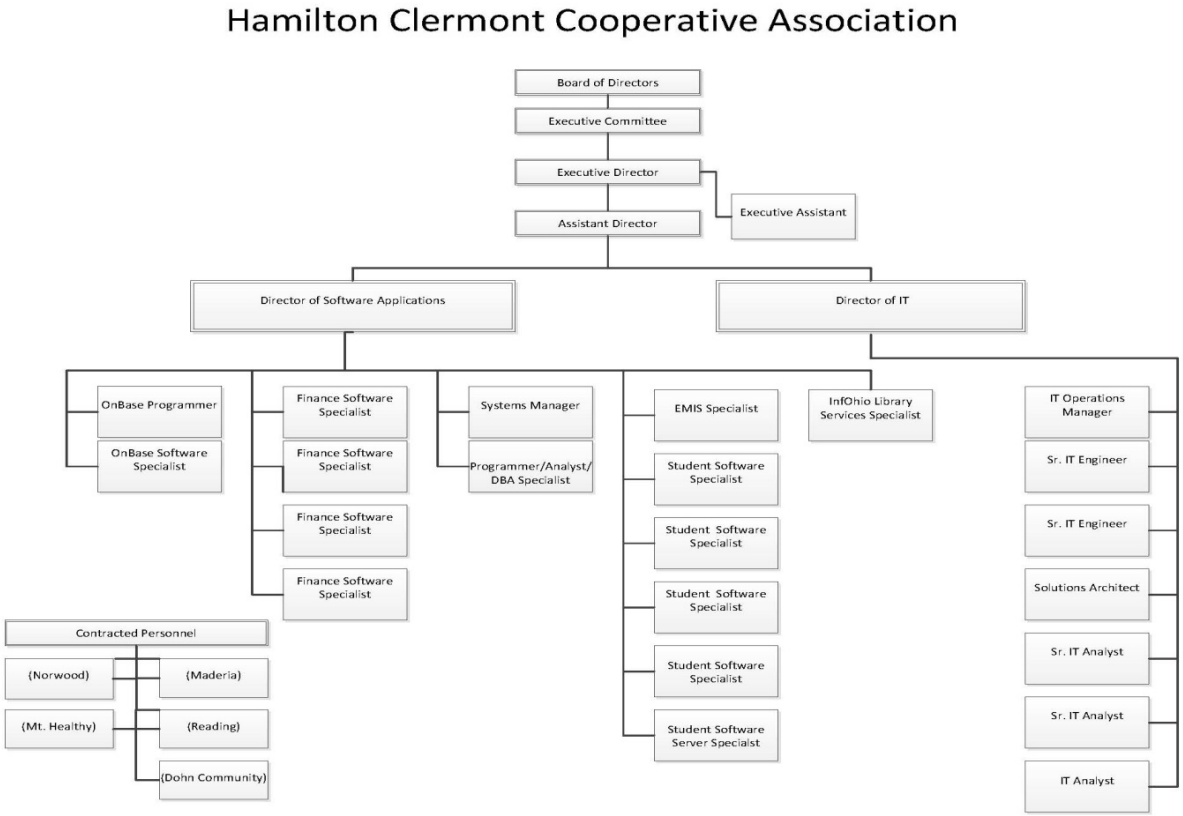
This Page Intentionally Left Blank

SECTION 3 - DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

The H/CCA'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 H/CCA's description of controls.

OVERVIEW OF OPERATIONS



The H/CCA is one of 19 governmental computer service organizations serving more than 973 educational entities and 1.475 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 H/CCA is derived from the state of Ohio and from user fees.

ITCs provide information technology services to school districts, community (charter) schools, career/JVS and 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).

ITCs are organized as either consortia under ORC 3313.92 or Regional Councils of Government (RCOG) under ORC 167. ORC 3313.92 allows for user entities to create a partnership (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 "RCOG" under ORC chapter 167 allows for one or more governmental entities to join together to form a new legal entity. A RCOG can have its own treasurer, make its own purchases, hire staff, and incur debt obligations. The H/CCA is organized under ORC chapter 167 and the Hamilton County Educational Service Center (ESC) serves as the fiscal agent.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the H/CCA executive committee. The executive committee is the managerial body of the H/CCA and the advisory body to the H/CCA board of directors. The executive committee is composed of eight members; two superintendents from each county (Hamilton and Clermont), one treasurer from each county, the fiscal agent superintendent or designee, and the treasurer of the fiscal agent serving as a non-voting ex-officio member. The executive committee is responsible for directing and supervising the daily operation of the H/CCA and making policy recommendations to the board of directors. These duties include, but are not limited to, supervising the staff, administering and implementing salaries and benefits, hiring and discharging the H/CCA employees, and supervising the operation of the computer system. The executive committee meets six times a year and additional meetings may be called as necessary.

The board of directors is the legislative and policy making body of the H/CCA. It is composed of the superintendent, treasurer, or designee from each user entity and one representative designated by the group of affiliate members to vote on their behalf. The affiliate members consist of board approved public governmental entities that subscribe to at least one of the services offered by the H/CCA and pay the annual membership fee. The board meets semiannually.

The H/CCA employs a staff of 31 individuals including the executive director and is supported by the following functional areas:

Fiscal Services:	Provides support to end users for all fiscal services applications. Fills in for vacancies in the business offices when there is a change of staff, vacations, maternity leave, or a user entity needs additional assistance for a period of time.
Student Services:	Supports end users in all aspects of the student service applications with a focus on EMIS.
Network/Systems Support:	Supports the H/CCA computer systems and its networked communication system. Provides user training and support.
INFOhio/Library Support:	Provides support to end-users of automated library applications. Also provides support in all aspects of the INFOhio program.

The directors of each of the functional areas report to the executive director through the assistant director. The H/CCA is generally limited to recording user entity transactions and processing the related data. User entities are responsible for authorization and initiation of all transactions. H/CCA's management reinforces this segregation of duties as a part of its new employees' orientation process, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced H/CCA employees may alter user data and only at the request of the user entity.

The H/CCA follows the same personnel policies and procedures as their fiscal agent, the Hamilton County ESC. When necessary, additional policies are developed and approved by the H/CCA board of directors to address concerns of the H/CCA. Detailed job descriptions exist for all positions. The H/CCA 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. Most staff evaluations are delegated to the Assistant Director and the two line supervisors for the personnel under their supervision. The Assistant Director and the two line supervisors are evaluated by the Executive Director annually. The executive committee is responsible for the annual evaluation of the executive director.

The H/CCA'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 or experience in a computer-related field, and all the H/CCA 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 15 hours of approved professional development training annually, and part-time staff member training hours are prorated. In addition, management encourages staff members to obtain additional training by paying 100% of incurred costs in attending professional development seminars.

The H/CCA is also subject to ITC site reviews by the Ohio Department of Education and the Management Council – Ohio Educational Computer Network (MCOECN. 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. The H/CCA's ITC site review was completed April, 2015.

The H/CCA provides a service level agreement (SLA) to its user entities as part of a signed contract for certain computer, data processing, and applications services. The SLA conveys to its user entities services provided by the H/CCA. The user entities agree to pay a fee based upon a fee schedule set forth by the governing board and to abide by the security policies implemented by the H/CCA. These SLAs are in effect beginning July 1, 2008, and will be in effect until terminated in writing by either the user entity or the H/CCA.

Risk Assessment

The H/CCA does not have a formal risk management process; however, the board of directors and executive committee actively participate in the oversight of the organization. As a regular part of their activities the board of directors and executive committee address:

- New technology.
- Realignment of the H/CCA organization to provide better service.
- Oversight and supervision of the overall operation of the H/CCA.
- Personnel issues, including hiring, termination, and evaluations.
- Additional charges and services provided to 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 H/CCA has identified operational risks resulting from the nature of the services provided to the 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 "IT General Control" section of this report.

Monitoring

The H/CCA organization is structured so that department directors report to the executive director through the assistant director. Key management employees have been with the H/CCA for several years and are experienced with the systems and controls at the H/CCA. The H/CCA 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, computer security and user help desk reports are monitored on an ongoing basis by departmental management. Some of these reports are automatically run through a scheduler program and sent to management via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily.

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 "IT General Control" section.

IT GENERAL CONTROL OBJECTIVES AND RELATED CONTROLS

Development and Implementation of New Applications or Systems

The H/CCA staff members do not perform system development activities. Instead, the H/CCA utilizes the software developed and supplied by the State Software Development Team (SSDT), located at the Northwest Ohio Computer Association (NWOCA), another ITC of the OECN. The ODE determines the scope of software development for state-supported systems. The Fiscal State Software Oversight Committee (SOC), which consists of members from the Management Council of the OECN (MCOECN), the Ohio Association of School Business Officials (OASBO), the ODE and the SSDT, assists in prioritizing specific goals and objectives. The SOC meets as needed to monitor SSDT projects and provide feedback on project priorities.

Changes to Existing Applications and Systems

End users have access to the SSDT website that contains user and technical documentation for the applications. Specific support issues or questions can be communicated to the SSDT via helpdesk software. Solutions are communicated directly to H/CCA staff. Global issues are posted to the SSDT support website.

The H/CCA 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. Upon notification of their availability from the SSDT, ITCs obtain quarterly updates by downloading zipped files from the SSDT's download site. The source code is not distributed with these files. Release notes, which explain the changes, enhancements and problems corrected, are provided via the SSDT website. User and system manager manuals are also made available via the SSDT website with these releases. The SSDT informs the ITCs that they will support only the latest release of the state software and encourage installation within 30 days following the software release date.

The H/CCA uses a software utility called OECN_INSTALL to unpack these zipped files and install each individual package into its proper OECN directory. The OECN_INSTALL utility has two options which will either install the new release on the system or install a patch for a current release. This utility ensures that all required components are installed properly and consistently.

Only vendor-supplied changes are made to the operating system or system software documentation. As a participating member of the MCOECN, an ITC can enter into a cooperative agreement, "Campuswide Software License Grant (CSLG) and Education Software Library (ESL) Program", through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of Hewlett Packard (HP), and other supplier's, software packages as approved by the MCOECN board of trustees.

The services acquired and/or provided by the MCOECN 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 and maintain support on one (1) license of Process Software's Multinet TCP/IP stack for each system registered under this program.

As a participating member of the MCOECN program, the participating ITCs agree to the following:

- Maintain its status as a member in good standing of the MCOECN as a qualification for participating in (or continuing to participate in) this program.
- Read, sign, and comply with the rules and regulations of the CSLG Program as operated by the MCOECN.
- Provide unrestricted privileged access to all computer systems covered under the agreement for the purposes of identifying and/or correcting problems, distributing software, or assuring licensing compliance.
- 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 MCOECN for services under the agreement within 30 days of the receipt of an invoice for said services.

Before new releases are installed at the H/CCA, a backup of the application or operating system affected by the change is prepared to ensure retention of the existing application or operating system in case of an error stemming from the upgrade process.

Documentation for the current version of the operating system and new releases are provided on the HP web site. New releases include documented changes to the operating system and implementation procedures. In addition, the H/CCA has purchased a copy of the operating system disks from INS, a third-party vendor in partnership with the MCOECN. The H/CCA is able to purchase the operating system software at a reduced cost under MCOECN. No new releases were installed during the audit period.

IT Security

The H/CCA has a security policy that outlines the responsibilities of user entity personnel, the H/CCA personnel, and any individual or group not belonging to the user entity or the H/CCA. These responsibilities include the use of the computer system, data access, outside access, and password guidelines. However, the policy is not distributed to users for acknowledgement and signature. In addition to the security policy, the H/CCA uses banner screens that are displayed prior to a user login and after a user successfully logs on to the system. The screen informs the user that unauthorized access of the system is prohibited and individuals using this computer system are subject to having their activities monitored by the H/CCA personnel.

The H/CCA staff is granted access within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities. Access is established, granted and reviewed by the systems manager and no authorization form is used.

An electronic authorization form must be completed and signed by the appropriate user entity management to obtain a new user account or request a change to an existing user account. These authorization forms are sent to the H/CCA for processing. Notification is sent to the user entity management after the new account or change has been made. All approved user access forms are stored in the OnBase imaging system. In addition, new users must sign an authorization form stating that they are aware of their responsibilities in regard to safeguarding system security.

The H/CCA runs a program nightly that generates a list of accounts and access privileges for each user entity. This listing is automatically placed in the user entity-wide print file where the treasurers and/or superintendents can review it daily. The user entities notify the H/CCA if a user needs to be removed by filling out a user access form for account deletion. In addition, a user access listing is sent to the user entities annually to verify user access privileges are correct.

Access to the Internet has been provided to the user entities through the OSC (Ohio Super Computer) network and Cincinnati Bell Fuse. The H/CCA has a basic Internet policy for all users with Internet access. The user entities may also have their own Internet and e-mail policies which would be maintained at the local user entities. User entities have been set up with sub-networks that have addresses not recognizable to the Internet, referred to as a private internal network. The firewall and routers also prevent outside connections (traffic) from accessing inside hosts or servers unless the host requires access from outside the network and has been designated as such by an administrator/manager. These hosts include web servers, mail servers, and certain application servers (ex. Progress Book), etc. These hosts have translated addresses on the firewall so the private IP address is not visible to the outside. Typical hosts on a network, i.e. user workstations, are not accessible from outside the network. In addition, the H/CCA is relying on the operating system security, including UICs, and restricted and captive flags to ensure that only proper access is granted to the system.

User entities use a Telnet connection to the H/CCA. All terminal sessions to and from the public internet are encrypted and secured. The H/CCA will contact a user entity if they determine they are not connected using SSH and push to have the encrypted version installed at the user entity. Use of encrypted terminal sessions is up to each user entity.

Users must provide a valid operating system username and password to authenticate to the USAS and USPS web applications. The SSDT developed a program called OECN_RPC (Remote Procedure Call) service which, in conjunction with Universal Service Provider (USP) created by Hewlett Packard, allows users to authenticate through a XML interface using standard operating system authentication policies. If authentication is successful, the RPC service "impersonates" the user by acquiring an operating system security profile of the authenticated user (i.e. default privileges and security identifiers). Once the RPC has acquired the corresponding security profile, the operating system process has the same security rights as the authenticated user. The network client then provides a code indicating the user entity data to be used. The RPC service uses the user entity code to define logical definitions to associate the server process with the desired user entity data.

Only default privileges from the user's authorization file record are enabled during a session. The session does not enable any authorized privileges. Therefore, when the service process accesses data files, the default login security profile is used. A user can select predefined OECN software functions that are available to the OECN_RPC service. (For example, USAS functions for posting a requisition). When the user has finished using the respective web application the logout button is clicked to disconnect. Alternatively, the session may disconnect automatically after the configured inactivity timeout.

The H/CCA uses three wireless networks, including a public connection used for on-site visitors or training for e-mail and web access. The internal wireless network is secured with an encryption key and is only accessible by H/CCA staff. The H/CCA IT staff utilizes a wireless network for testing outside of its network.

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 (i.e., audit journal); alarms are sent to the operator log file. Access to the operator log and audit log is limited to data processing personnel. The following security alarms and security audits have been enabled through the operating system to monitor security violations.

ACL:	Gives file owners the option to selectively alarm certain files and events. Read, write, execute, delete, or control modes can be audited.
AUDIT:	Enabled by default to produce a record of when other security alarms were enabled or disabled.
AUTHORIZATION:	Enables monitoring of changes made to the system user authorization file (UAF) or network proxy authorization file in addition to changes to the rights database.
BREAK-IN:	Produces a record of break-in attempts. The DIALUP, LOCAL, REMOTE, NETWORK, and DETACHED break-in types can be monitored.
LOGFAILURE:	Provides a record of logon failures. The BATCH, DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESSES, and DETACHED logon failure types can be monitored.

A batch processed command procedure executes each night to extract any security violations from the audit journal and creates a summary report and a detail report which contains information on unsuccessful logon attempts and any use of the AUTHORIZE command. These security monitoring reports are e-mailed to the systems manager and reviewed daily. If an event is deemed suspicious, further investigation is performed to determine the exact nature of the event and the corrective action needed. The systems manager maintains approximately one week of these reports.

The H/CCA utilizes MailMarshal software to scan all inbound and outbound e-mail. Virus infected messages are quarantined to a specific folder and then removed after four calendar days.

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

The H/CCA utilizes proxy logins. A proxy login enables a user logged in at a remote node to be logged in automatically to a specific account at the local node, without having to supply access control information. A proxy login differs from an interactive login because an interactive login requires a user to supply a user name and password before the user can perform any interactive operations. Proxy records are located in the proxy file.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the H/CCA and to all personnel at the user entities which use the H/CCA system. UICs are assigned at the user entity's request. UIC based protection controls access to objects such as files, directories, and volumes.

Certain limited access accounts require a less restrictive environment than captive accounts. Accounts, under which network objects run, for

example, require temporary access to the operating system prompt. Such accounts must be set up as restricted accounts, not captive accounts. User accounts should be set with the RESTRICTED flag instead of the CAPTIVE flag if they need to use network applications like MAIL or network proxy accounts. All user accounts not belonging to the H/CCA or system are assigned the RESTRICTED and CAPTIVE flags, respectively. The RESTRICTED flag allows access to MAIL, but since the CAPTIVE flag is also assigned, the use of the SPAWN command to gain access to the operating system prompt is prohibited.

The system forces users to periodically change their passwords. User accounts have a password lifetime in accordance with management's established standards. 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. Administrative account passwords also follow the same standards.

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

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

System parameter standards have been established through the use of HP established defaults. Any changes are logged and reviewed by the systems manager.

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

The only fiscal applications running on a SQL server at H/CCA are USASDW and BuySpeed. The USASDW application is used by the user entities to view purchase orders, invoices, checks, accounts, vendors, and receipts. The SQL server is running Microsoft's SQL software. Access to manage the database is restricted to six H/CCA staff.

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

The system directory contains security files that control the security parameters for the system. When a user attempts to gain access to an object, such as a file or directory, the system compares the user's User Identification Code (UIC) to the owner's UIC for that object. In UIC-based protection, the relationship between the user's UIC and the object's UIC determines whether access is granted. Owner relationships are divided into four categories:

SYSTEM: Any of the following: (1) Users with a UIC group number between 1 and SYSGEN parameter MAXSYSGROUP (default decimal 8, octal 10). (2) Users with system privileges (SYSPRV). (3) Users with group privileges (GRPPRV) whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

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

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

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

Through the protection code, each category of users can be allowed or denied read, write, execute, and delete access. The default file protection is for (1) SYSTEM having read, write, execute, and delete capabilities; (2) OWNER having read, write, execute and delete capabilities; (3) GROUP having read and execute capabilities; and (4) WORLD having no access capabilities. UIC-based protection prevents WORLD, write, or delete access to USAS, USPS, and SAAS/EIS application production and data files.

Certain privileges can override all UIC-based and ACL protection. The operating system analyzes privileges included in the user's authorization record and places the user in one of seven categories depending on which privileges have been granted to the user. Default privileges are those authorized privileges that are automatically granted at login. If an authorized privilege is not a default privilege, it will not automatically be effective at login, and must be enabled or disabled by the user. H/CCA's user accounts within the NORMAL privilege class include NETMBX, TEMPMBX and OPER 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 H/CCA 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 operating system identifiers to authorized users. Each application package has a set of unique identifiers that permit access to programs. In addition to the standard identifiers for each package, a pass through identifier can be used to further customize access. OSA is used in conjunction with the OECN menu processor utility thus allowing the users to see only the items they are authorized to execute. UIC-based protection prevents WORLD write or delete access to USAS, USPS, and SAAS/EIS

application data files.

The OECN_SYSMAN identifier (defined by state software applications and consistent for all ITCs) and the BYPASS privilege (defined by the operating system) grant access to all application packages. The OECN_SYSMAN identifier or BYPASS privilege are used to grant users the same access to software functions without having to grant each individual identifier. The OECN_SYSMAN identifier and BYPASS privilege do not grant access to data.

The data processing department is in an enclosed area that is secured by key pad entry and monitored by an alarm system. All doors are locked during non-business hours. During daytime hours the main door is locked and electronically controlled, requiring staff to unlock the door using a remote mechanism. All exterior entries to the building require use of a key fob to gain entrance to H/CCA. Visitors can be granted access via the receptionist located in the lobby of the Mt. Healthy City School Board office. The computer room remains locked at all times and is secured by combination keypad locks. The combinations are known only by the data processing staff and are changed routinely or upon employee separation.

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

- Smoke detectors.
- Raised floor with water sensors.
- Pager/phone calls system to alert key DP personnel of environmental alarms.
- Two halon fire extinguishers.
- Liebert air conditioning system.
- Liebert diesel generator.
- Liebert 50KVA UPS battery pack system.

IT Operations

Traditional computer operations procedures are minimal since user entity personnel initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All H/CCA employees have access to a procedures manual, which provides directions and guidelines for most of the operational functions performed. They also have access to operations procedure manuals for the system. In addition, all users, except students, have access to the SSDT Wiki

Certain routine jobs are initiated at the H/CCA for system maintenance. The H/CCA is responsible for operational maintenance tasks, such as: system backups, file rebuilds, file integrity testing, log reports, and other maintenance directed at the system as a whole. These tasks are scheduled to run automatically through SUBMITALL.

The H/CCA helps to prevent failures or file corruption through the use of CONVERTALL, which is run through SUBMITALL. CONVERTALL analyzes all files weekly to ensure they are readable (i.e. no bad blocks, sectors, or chains). Data integrity is maintained by the software through validity checks of all input. The log report lists any problems that were found, and it is reviewed by the systems manager.

Common problems that arise daily, such as terminal lockups and program crashes, are usually handled by H/CCA service representatives over the phone and documented on the help desk, Cherwell Service Management, that is used by all ITCs. These are reviewed periodically by the technical services supervisor to ensure that all problems have been resolved on a timely basis and to determine when the problems that are still open will be resolved. The H/CCA has technicians on staff to handle most hardware problems.

User entities are responsible for changes to their own data. Use of mass change programs within the software leaves an audit trail. The H/CCA very rarely changes user entity data. If they do, they require an e-mail from the user entity indicating what the change is and why it is needed. This information is entered into the help desk, Cherwell. In addition, the user entities may view or print out an "AUDIT" report that shows all changes to the data file.

The H/CCA has agreements with HP for hardware maintenance and business recovery purposes and a disaster recovery agreement with the MCOECN. In addition, all data processing equipment is covered under an insurance policy.

Network monitoring and fault notification is accomplished through one application: Paessler Router Traffic Grapher (PRTG). PRTG monitors the state of switch connectivity to internal devices. Interfaces on those devices that directly connect the schools are monitored as well as the devices (switches) themselves. The H/CCA monitors its devices using PRTG. CBT monitors the school connectivity through the gateway and the local CBT device on school premises. Emails, alerts and tickets are sent to IT when a school loses connectivity. PRTG uses polling to detect connectivity problems. The application sends out a poll to each device and interface and receives a response back indicating that the devices are active. Emails are also sent out to the appropriate personnel for immediate support response. When the devices are active again, an "up" email is sent out to the appropriate personnel to notify them that the device is responding again. IT staff can also access PRTG. The H/CCA also uses PRTG for monitoring server availability and system status (i.e. disk space, processor utilization and memory) on selected servers. H/CCA personnel are notified in the event a system exceeds the established thresholds.

The H/CCA follows the guidelines of the OECN for backing up system programs, data, and related documentation. Full system backups are performed nightly. Backups to the disaster recovery (DR) site are performed seven days a week. A standalone backup of the operating system is performed prior to any updates to the OpenVMS operating system. In addition, backups are periodically used to restore data for user entity personnel. Requests for data restoration must be made either via e-mail or the help desk. Backups of the internal network are performed daily on the Windows and Linux servers. VEEAM is used to backup the VMs, which includes most of the servers. Evault is only used to backup the Alpha and a few physical servers located at H/CCA. One storage vault is used and located on site.

All system and program documentation is stored electronically and is subject to the same backup procedures as other data files. All data is required by law to be maintained for a specific duration by the H/CCA.

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 H/CCA. User auditors should consider whether the following controls have been placed in operation at the user entity:

1. Confirm if the user entity has developed or is in the process of developing its own web applications to access its data stored at the H/CCA.

2. User entities should have controls over their own web applications which access their data stored at the H/CCA.

3. User entity management should have practices to ensure users are aware of the confidential nature of passwords and the precautions necessary to ensure passwords are not compromised.

4. User entity management should immediately request the H/CCA to revoke the access privileges of user entity personnel when they leave or are otherwise terminated.

5. User entity management should have a procedure for confirming user accounts and access rights as requested by H/CCA.

6. User entity management should retain signed copies of the authorization form for new user accounts and utilize the PTR report generated by the H/CCA to review and manage their user accounts.

7. 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.

8. User entities should deploy antivirus software with timely updates to the virus definition.

9. User Identification Codes (UICs), passwords and associated access privileges should only be issued to authorized users who need access to computer resources to perform their job function.

10. 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.

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

12. User entity wireless networks should be secured via encryption.

13. The user entity should establish and enforce a formal data retention schedule with the H/CCA 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 H/CCA'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 H/CCA and procedures performed at user entities that utilize the H/CCA.

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.

IT GENERAL CONTROL OBJECTIVES AND RELATED CONTROLS

Changes to Existing Applications and Systems

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Requests for application program changes or system upgrades should be appropriately considered and processed.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
In order to maintain continued support of the application software provided by the SSDT, ITCs are encouraged to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the H/CCA object files for USAS, USPS, and SAAS/EIS was compared to the CRCs of the object files at the SSDT.	The POFORM was modified for customized changes specific to H/CCA due to differences in purchase order forms. No other 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 reelase notes and user system manuals, and inquired with the systems manager regarding its availability.	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:*
Authorization from appropriate user entity management is required before setting up a new user account.	Identified active user accounts with OECN identifiers from the user authorization file. Selected 13 user accounts from a population of 128 new accounts and inspected the forms for new users to confirm the required signatures were present.	No exceptions noted.
User entities are requested to confirm user accounts annually with a positive confirmation. H/CCA tracks the status of the confirmation and performs any necessary follow-up communication to facilitate a response from the user entity.	Inspected the following information regarding the confirmation of user access by H/CCA: • Example of the initial letter dated April 21, 2015 sent to the user entities requesting confirmation of user accounts. • Spreadsheet used to record positive confirmation from the user entity. • User entity confirmation response.	No exceptions noted.
Tracking of security-related events, such as break-in attempts and excessive login failures, are enabled through the operating system. The events are logged to audit journals for monitoring of potential security violations.	Inspected the security alarms and audits enabled to confirm security related events are recorded.	No exceptions noted.

IT Security - *Control Objective:* **Security Management -** Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A procedure runs nightly to create reports that list security violations from the audit journal and e-mails the reports to the systems manager for review.	Inspected the following information with the systems manager to confirm these reports are produced and reviewed daily: • Example of security monitor report. • Command procedure that is utilized to generate and e-mail the report to the systems manager. • Command procedure to confirm the procedure that creates the report is included in the scheduler and submitted daily.	No exceptions noted.
Anti-virus software scans all inbound and outbound e-mail before the mail is forwarded to the server. Definitions are updated automatically on a regular basis.	Inspected the following with the systems manager to confirm active virus protection: • An example of a virus log. • Update schedule. Discussed responsibility of log review with the systems manager,	No exceptions noted.

IT Security - *Control Objective:* **System Level Access Controls -** Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The use of wild card characters in proxy accounts is restricted to ensure proxy accounts are specifically defined to prevent blanket access.	Inspected the proxy listing with the systems manager to confirm wild card characters were not used.	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 operating system. Passwords used by individual profiles agree to password policies established by the H/CCA.	Inspected information from the system user authorization file to identify user accounts with: • User accounts with password minimum lengths less than H/CCA policy. • User accounts with a password lifetime greater than H/CCA policy. Inspected the listed accounts and inquired with the systems manager regarding the listed accounts.	Of the 2,038 enabled accounts on the system, the following 49 exceptions were noted: • Five communication system accounts had a required minimum password length shorter than H/CCA policy. These accounts are not logged into. • Forty nine accounts had a password lifetime not equal to H/CCA policy for normal user accounts: There were 3 system accounts 1 test account and 45 application accounts whose password cannot expire. There were no user accounts with a password lifetime greater than H/CCA's standard. No other exceptions noted.
Password expiration for the web applications is defined at the system or process level.	Inspected the parameter to confirm password expiration for web applications.	No exceptions noted.
Log-in parameters have been set to control and monitor sign-on attempts.	Inspected the log-in parameter settings to determine parameters met standards.	No exceptions noted.
System and web application activity is monitored and inactive users are automatically disconnected after a predetermined amount of idle time.	Inspected the HITMAN parameters to confirm parameters were set for idle time and action to be taken against inactive users. Inspected the system startup file to confirm that the HITMAN program was part of the startup procedures. Inspected the configuration for the timeout values on the USAS and USPS web 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:*
Access to production data files and programs on the system is restricted to authorized users.	Inspected the file protection masks to identify production data files with WORLD access and executable files with WORLD write and/or delete access.	No exceptions noted.
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user entities.	Inspected the network diagram to confirm components of the network which control Internet access. Inspected the firewall configuration for evidence that Internet traffic is restricted through the firewall. Confirmed diagram components and firewall settings with the systems manager.	No exceptions noted.
Connection to the system from the user entities is restricted through emulation software installed on each authorized user's computer. Telnet sessions are not allowed from outside the H/CCA network.	Confirmed user entity Telnet access restrictions with the systems manager. Inspected logon procedures for connecting to the system. Confirmed Telnet session restrictions from outside the H/CCA network with the systems manager.	No exceptions noted.
H/CCA does not broadcast the Set Identifier (SSID) for their wireless networks and access requires a Wi-Fi Protected Access (WPA) key.	Identified wireless networks using personal computer tools and inquired with the systems manager about availability of wireless access to the network. Confirmed the security settings for the wireless access point with the systems manager.	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 entity management.	Inspected the user authorization file listing all identifiers for evidence of the use of identifiers to segregate access to the applications. Inquired with the systems manager regarding the OSA utility and the process used to assign application identifiers. Extracted a listing of all OECN identifiers from the user authorization file for evidence of the use of identifiers to segregate access to the applications. Selected 13 of 128 new user accounts and compared the listed identifiers to account request forms or annual confirmations to confirm access was authorized.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state-developed applications is restricted to authorized users.	Inspected all accounts with the OECN_SYSMAN identifier. Confirmed the appropriateness of the accounts with the systems manager.	No exceptions noted.

IT Security - *Control Objective:* **System Software and Utilities Access Controls -** Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
World access to "key" system files is restricted.	Inspected the file protection masks on the system files to confirm WORLD write and/or delete access was absent. 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.	Identified the maximum system group number and inspected a listing of extracted accounts with a UIC less than the maximum system group number. Confirmed the appropriateness of the accounts with the systems manager.	No exceptions noted.
Use of an alternate user authorization file is not permitted to be used and does not exist.	Inspected the value of the alternate user authorization parameter to confirm the parameter's setting does not allow for use of an alternate user authorization file. Inspected the system directory listings to confirm that an alternate user authorization file does not exist.	No exceptions noted.
Remote access to firewall and router configurations used to control Internet access is restricted to authorized users through password protection and limited login attempts.	Inspected the firewall configuration to confirm passwords are required to access the routing equipment used to control Internet access and to confirm remote access is allowed. Confirmed password parameter with the systems manager.	No exceptions noted.
Accounts on the system with elevated privileges are limited to authorized personnel as determined by the H/CCA staff.	Extracted accounts from the user authorization file to identify accounts with elevated privileges. Inspected the listings and inquired with the systems manager regarding the appropriateness of the accounts.	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 via security devices, including an electronic keypad for the computer room and security monitoring equipment for the H/CCA offices.	Inspected security devices including door locks, keypad entry devices and security monitoring equipment within the H/CCA facility. Inspected the service agreement and payment documentation for security monitoring.	No exceptions noted.
Environmental controls are in place to protect against and or detect fire, water, humidity, or changes in temperature.	Inspected the computer room to confirm the existence of environmental controls. Inspected the maintenance agreement and payment documentation for maintenance of the air conditioning unit.	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:*
Routine system maintenance programs, such as file rebuilds, file cleanups and disk space management are scheduled to run via a scheduling program.	Inspected the scheduling program's job listing for June 20, 2016 to confirm that routine system maintenance jobs are automatically scheduled to run daily. Inspected the batch queue to confirm the scheduling program resubmits itself daily.	No exceptions noted.
A system utility is run weekly to help prevent file failure and data corruption.	Inspected the scheduling program's job listing to confirm the system utility is automated and is run through the scheduling program. Inspected the system utility's job description, the system utility's program, and an example of a job log for June 14, 2016.	No exceptions noted.
Paessler Router Traffic Grapher (PRTG) monitors network performance and alerts staff of hardware failures and system problems.	Inspected screens and alerts with the IT operations manager of the monitoring application to confirm user entity equipment is monitored and alerts are sent when equipment fails.	No exceptions noted.
A service agreement with HP covers maintenance and failures on the computer hardware.	Inspected the service agreement and payment documentation to confirm coverage was in effect during the audit period.	No exceptions noted.
All data center equipment is covered by insurance in case of loss or damage.	Inspected the insurance policy and payment documentation to confirm coverage for computer equipment and software.	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:*
Incremental system backups of programs and data are performed nightly and sent to the disaster recovery site in Columbus.	Inspected the command procedure that runs nightly and the backup log for June 14, 2016 to confirm successful backup to the disaster recovery site. The status of the backup is sent via e-mail to H/CCA staff for inspection.	No exceptions noted.
Data restoration from backup is performed and logged when requests are received either via e-mail or the help desk.	Inspected the following documentation to confirm backup tape restoration: • Restore command procedure. • Example of a restore log for a performed restore on April 19, 2016.	No exceptions noted.

SECTION 5 - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION *(Unaudited)*

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name:	Hamilton/Clermont Cooperative Association (H/CCA)
Number:	24
Node Name:	HCCA1
Chairperson:	Todd Yohey Superintendent Oak Hills Local SD
Fiscal Agent:	Hamilton County Educational Service Center
Administrator:	Tom Collins Executive director H/CCA
Address:	7615 Harrison Avenue Cincinnati, OH 45231
Telephone:	513-931-7120
FAX:	513-931-7202
Website:	www.hccanet.org

OTHER SITE STAFF

Laura Gallogly	Assistant director
Jill Griffith	Systems manager
Tim Thompson	Senior IT analyst
Adam Blevins`	Director of IT
Kelley Underwood	Senior IT engineer
Jeff Reasoner	Senior IT engineer
Susan Patrick	IT operations manager
Kevin Gassert	OnBase programmer
Alyssa Phlaumer	Finance software specialist
Terri Dobbs	Finance software specialist
Catherine Bach	Finance software specialist
Marcia Wylie	Finance software specialist
LaWanda Englemen	Contracted personnel-Mt. Healthy
Frank Baird	Contracted personnel-Reading
Jeff Ewing	Student software/server specialist
Kimberly Bussell	Student software specialist
Deb Kaehr	Student software specialist
Graham Handler	IT analyst
Doug Leighton	Programmer/analyst/DBA specialist
Henrietta Philpot	Executive assistant
Tracy Varner	InfOhio library services specialist
Karen Ryan	EMIS specialist
Deanne Devine	OnBase software specialist
Randall Grandstaff	Contracted personnel-Norwood
Mary Jo Pfaffinger	Contracted personnel-Madeira
Debbie Purvis	Contracted personnel-Dohn Community
Vacant	Solutions architect
Kathy Rose	Student software specialist
David Downs	Director of software applications
Kirk Holliday	Senior IT Analyst
Julie Edmondson	Student software specialist

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	DEC Alpha ES40	Lines/Ports:	0	Memory Installed:	4 GB
Disk:	RA7000	Units:	9	Total Capacity:	90 GB
Disk:	RZ1ED	Units:	5	Total Capacity:	162 GB
Disk:	SAN	Units:	15	Total Capacity:	600 GB
Tape Unit:	TZ89	Units:	1	Max Density:	70 GB
Tape Unit	8mm	Units	1	Max Density:	8 GB
Tape Unit	TSZ07	Units	1	Max Density:	6250 BPI
Tape Unit	SDLT 160/320	Units	1	Max Density:	320 GB

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS	OTHER
046300	Batavia Local SD	Clermont	X	X	X	X
046318	Bethel-Tate Local SD	Clermont	X	X	X	X
013259	Center for Collaborative Solutions	Hamilton	X	X		X
043752	Cincinnati Board of Education	Hamilton	X		X	X
014742	Cincinnati Generation Academy	Hamilton	X	X		
046292	Clermont County ESC	Clermont	X	X	X	X
046326	Clermont-Northeastern Local SD	Clermont	X	X	X	X
043851	Deer Park Community City SD	Hamilton	X	X	X	X
133264	Dohn Community School	Hamilton	X	X	X	X
046334	Felicity-Franklin Local SD	Clermont	X	X	X	X
047332	Finneytown Local SD	Hamilton	X	X	X	X
047340	Forest Hills Local SD	Hamilton	X	X	X	X
046342	Goshen Local SD	Clermont	X	X	X	X
047324	Hamilton County ESC	Hamilton	X	X	X	X
045345	Indian Hill Ex. Vill SD	Hamilton	X	X	X	X
014234	Lighthouse Community	Hamilton	X			X
044230	Lockland City SD	Hamilton	X	X	X	X
044289	Madeira City SD	Hamilton	X	X	X	X
044313	Mariemont City SD	Hamilton	X	X	X	X
010226	Management Council – Ohio Education Computer Network (MCOECN)	Franklin	X	X		

USER ENTITY SITE DATA

IRN	USER ENTITY	COUNTY	USAS	USPS	SAAS	OTHER
045500	Milford Ex. Vill SD	Clermont	X	X	X	X
044412	Mount Healthy City SD	Hamilton	X	X	X	X
045559	New Richmond Ex. Vill SD	Clermont	X	X	X	X
044511	North College Hill City SD	Hamilton	X	X	X	X
044578	Norwood City SD	Hamilton	X	X	X	X
014912	Norwood Conversion Community School	Hamilton	X	X		X
047373	Oak Hills Local SD	Hamilton	X	X	X	X
044693	Reading Community City SD	Hamilton	X	X	X	X
047381	Southwest Local SD	Hamilton	X	X	X	X
044719	St. Bernard-Elmwood Place City SD	Hamilton	X	X	X	X
044867	Sycamore Community City SD	Hamilton	X	X	X	X
047399	Three Rivers Local SD	Hamilton	X	X	X	X
062802	US Grant JVSD	Clermont	X	X	X	X
046359	West Clermont Local SD	Clermont	X	X	X	X
046367	Williamsburg Local SD	Clermont	X	X	X	X
044081	Winton Woods City SD	Hamilton	X	X	X	X
045146	Wyoming City SD	Hamilton	X	X	X	X
TOTALS:			**37**	**35**	**31**	**35**

OTHER* - Applications other than USAS, USPS, and SAAS/EIS, used by the user entities.

This page intentionally left blank.

Dave Yost • Auditor of State

HAMILTON-CLERMONT COOPERATIVE ASSOCIATION

HAMILTON 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 27, 2016

88 East Broad Street, Fourth Floor, Columbus, Ohio 43215-3506
Phone: 614-466-4514 or 800-282-0370 Fax: 614-466-4490
www.ohioauditor.gov