NORTHWEST OHIO AREA COMPUTER SERVICES COOPERATIVE (NOACSC)
ALLEN COUNTY

SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

APRIL 1, 2018 THROUGH MARCH 31, 2019

OHIO AUDITOR OF STATE
KEITH FABER

TABLE OF CONTENTS

This Page Intentionally Left Blank

-

OHIO AUDITOR OF STATE
KEITH FABER

88 East Broad Street, 10th Floor
Columbus, Ohio 43215-3506
(614) 466-3402 or (800) 443-9275
StateRegion@ohioauditor.gov

Independent Service Auditor's Report

Board of Directors
Northwest Ohio Area Computer Services Cooperative (NOACSC)
4277 East Road
Lima, OH 45807

To Members of the Board:

Scope
We have examined NOACSC's description of its Information Technology General Controls (ITGC) System entitled "Description of NOACSC's ITGC System," for processing user entities' transactions for the Uniform School Accounting System (USAS), Uniform School Accounting System Redesign (USAS-R), Uniform Staff Payroll System (USPS), Uniform Staff Payroll System Redesign (USPS-R), and School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS) throughout the period April 1, 2018 to March 31, 2019 (the "description") and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "NOACSC's Assertion" (the "assertion"). The controls and control objectives included in the description are those that management of NOACSC believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the ITGC System that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in section 5, "Other Information Provided by NOACSC" is presented by management of NOACSC to provide additional information and is not a part of NOACSC's description of its system made available to user entities during the period April 1, 2018 to March 31, 2019. Information about NOACSC's ITC Profile including site data, other site staff, hardware data, and user entity site data, has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of NOACSC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities
In section 2, NOACSC 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. NOACSC is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and 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 stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively 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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, 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, 2018 to March 31, 2019. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls 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 the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.

- 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.

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations
The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements 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 ineffective.

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

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

a. the description fairly presents the ITGC System that was designed and implemented throughout the period April 1, 2018 to March 31, 2019.

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, 2018 to March 31, 2019 and user entities

applied the complementary controls assumed in the design of NOACSC's controls throughout the period April 1, 2018 to March 31, 2019

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period April 1, 2018 to March 31, 2019 if complementary user entity controls assumed in the design of NOACSC's controls operated effectively throughout the period April 1, 2018 to March 31, 2019.

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 management of NOACSC, user entities of NOACSC's system during some or all of the period April 1, 2018 to March 31, 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and 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 misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Keith Faber
Auditor of State

Columbus, Ohio

December 29, 2019

This Page Intentionally Left Blank

Northwest Ohio Area Computer Services Cooperative

NOACSC'S ASSERTION

We have prepared the description of the Northwest Ohio Area Computer Services Cooperative's (NOACSC) Information Technology General Controls (ITGC) System entitled "Description of NOACSC's ITGC System," for processing user entities' transactions for the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), Uniform School Accounting System Redesign (USAS-R), Uniform Staff Payroll System Redesign (USPS-R) and School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS) throughout the period April 1, 2018 to March 31, 2019 (the "description") for user entities of the system during some or all of the period April 1, 2018 to March 31, 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have 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 misstatement of user entities' financial statements.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of NOACSC's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

a) the description fairly presents the ITGC System made available to user entities of the system during some or all of the period April 1, 2018 to March 31, 2019, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The NOACSC service organization has a vendor relationship with the State Software Development Team (SSDT) located at the Northwest Ohio Computer Association (NWOCA) and uses the USAS, USPS, SAAS/EIS, USAS-R and USPS-R application software as provided by the SSDT. 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 user entity transactions, including, if applicable,

      1) the types of services provided, including, as appropriate, the classes of transactions processed.

      2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

      3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

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

      5) the process used to prepare reports and other information for user entities.

      6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

      7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls assumed in the design of the service organization's controls.

Ray Burden
Executive Director
4277 East Road, Lima, Ohio 45807
419-228-7417
419-222-5635

8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii) includes relevant details of changes to the service organization's system during the period covered by the description.

iii) does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the ITGC System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b) the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period April 1, 2018 to March 31, 2019, to achieve those control objectives if the user entities applied the complementary controls assumed in the design of NOACSC's controls throughout the period April 1, 2018 to March 31, 2019. 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 management of the service organization.

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

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

Ray Burden
Executive Director
Northwest Ohio Area Computer Services Cooperative (NOACSC)

SECTION 3 – DESCRIPTION OF NOACSC'S ITGC SYSTEM

CONTROL OBJECTIVES AND RELATED CONTROLS

The Northwest Ohio Area Computer Services Cooperative (NOACSC) 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 NOACSC's description of controls.

OVERVIEW OF OPERATIONS

The NOACSC is one of 18 government computer service organizations serving more than 1,110 educational entities and 1.796 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 NOACSC 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 of more of the following applications:

State Software Development Team (SSDT Redesign):

- Uniform School Accounting System – Redesign (USAS-R).
- Uniform Staff Payroll System Redesign (USPS-R).

State Software Development Team (SSDT Classic):

- 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 Council of Governments (COG) under ORC 167. ORC 3313.92 allows school districts 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 "COG" under ORC chapter 167 allows one or more governmental entities to join to form a new legal entity. A COG can have its own treasurer, make its own purchases, hire staff, and have debt obligations. NOACSC is organized under ORC 167 and is not required to have a board of education serve as its fiscal agent.

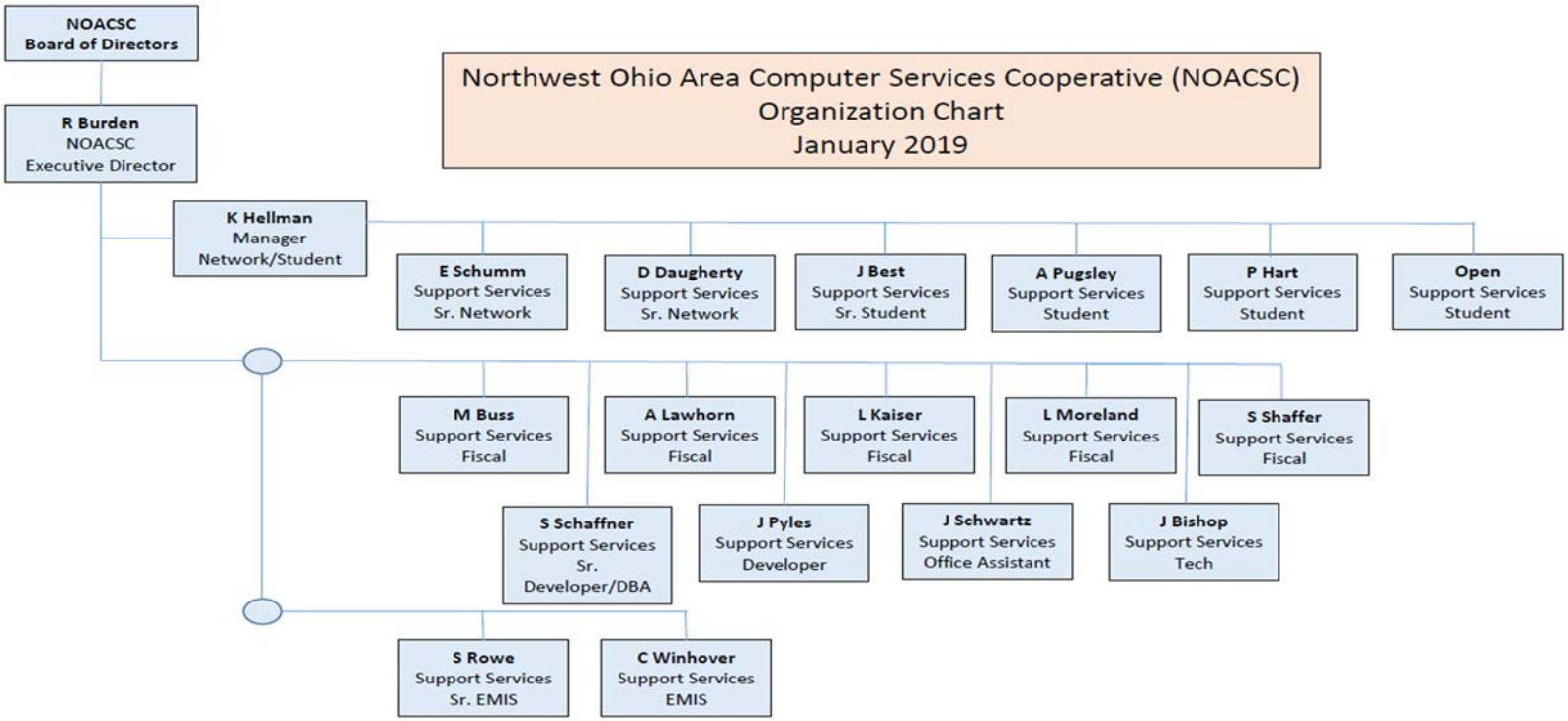
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the governing board. The governing board is composed of two members from each county elected by a majority vote of all charter member user entities in each county, plus one representative from the fiscal agent. The board meets four times a year and at other times as deemed necessary.

The NOACSC employs a staff of 18 individuals, including the executive director and is supported by the following functional areas:

Fiscal Services:	Provides end user support and training for the NOACSC user entities for the state software applications, including USAS, USAS-R, USPS, USPS-R and SAAS/EIS.
Technology:	Provides a variety of educational technology services to subscribing NOACSC user entities including software and Internet access, training, technology planning, and technical assistance.
Student Services:	Support end users in all aspect of the student service applications.
Network Support:	Provides user training and support for the NOACSC computer system and its networked communication system.



The NOACSC is generally limited to recording user entity transactions and processing the related data. Users are responsible for authorization and initiation of all transactions. Management reinforces this segregation of duties as a part of its new employee's orientation process, through on the job training, and by restricting employee access to user data. Changes to user data are infrequent. Only experienced NOACSC employees may alter user data and only at the request of the user entity.

The NOACSC follows personnel policies and procedures adopted by the Governing Board. Detailed job descriptions exist for all positions. The NOACSC 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 entity.

The NOACSC's hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Some NOACSC staff members are required to attend professional development and other training as a requirement to maintain certification or licensure. The NOACSC tracks continuing education requirements for those employees. The NOACSC pays 100% of the incurred costs in attending professional development seminars. Employee evaluations are conducted annually by the executive director. The board performs an annual evaluation of the executive director.

The NOACSC is also subject to ITC Site Reviews by ODE and the Management Council (MC) of the OECN. These site reviews are conducted by a team consisting of an employee of the ODE, two current and/or former user entity 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. NOACSC's last site review was in January, 2019.

The NOACSC has Service Level Agreements (SLA) with their user entities for certain computer, data processing, and application services. The user entities agree to pay a fee based upon a fee schedule set forth by the governing board and they agree to abide by the security policies implemented by the NOACSC. 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 NOACSC.

Risk Assessment

The NOACSC does not have a formal risk management process; however, the governing board actively participates in the oversight of the entity. As a regular part of its activity, the governing board addresses:

- New technology.
- Realignment of the NOACSC organization to provide better service.
- Personnel issues, including hiring, termination, and evaluations.
- Additional 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 NOACSC 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 NOACSC is structured so that each staff member ultimately reports to the executive director. Key employees have worked here for a number of years and are experienced with the systems and controls at the NOACSC. The NOACSC executive director and network services manager monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, NOACSC 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, 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. In addition, the executive director receives the same reports and monitors for interrelated and recurring problems.

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

NOACSC Environment Overview

NOACSC offers two versions of the financial software as provided by the State Software Development Team (SSDT), which includes the Classic version (USAS, USPS, SAAS/EIS) running on an Open VMS operating system and the Redesign version (USAS-R and USPS-R) running on a Ubuntu Linux operating system.

Acquisition and Implementation of New Applications or Systems (SSDT Redesign)

User entities that choose to migrate to the Redesign have several trial data loads performed by NOACSC staff about two months prior the final load into Redesign. This provides an opportunity to correct any data abnormalities and balancing issues. These practice loads are done to ensure extractions are working properly and that loads complete timely. Balancing issues are addressed and any data cleanup is done before the final load into Redesign is scheduled. The user entity participates in a mandatory two-day training covering the key aspects of both payroll and budgetary in the new software. Once the user entity's final load is complete, they begin usage by performing dual entry of the same transactions into both the Redesign and Classic software. NOACSC recommends each user entity continue dual entry through at least one payroll cycle. The user entity can decide how long they wish to perform dual entry before committing to go into production on the Redesign. Once the user entity goes live, they sign-off on the "Certification Questionnaire for Redesign Go-Live Authorization" form confirming their intention to use the Redesign applications exclusively and cease using the Classic version.

Changes to Existing Applications and Systems (SSDT Redesign)

Redesign updates are applied automatically each night. Updates are set to pull updates for USAS-R and USPS-R each night for all six user entities live on Redesign.

The SSDT distributes release notes explaining the changes, enhancements and problems corrected. Updated user and system manuals are also made available. Release notes were available at and address application changes and processing procedure revisions. Manuals were also available on the SSDT website.

IT Security (SSDT Redesign)

NOACSC staff authenticate through Active Directory (AD) to access the Redesign application. Only NOACSC fiscal support staff have access within the application for user entity support. Active directory account policies have been set. User entity login is to NOACSC's site, which is secured by HTTPS. Each user entity has access to the web site and enter a username and password to access the application.

NOACSC has implemented a User Authorization Form specifically for Redesign. The form must be completed by the user entity and authorization signatures from the Treasurer and/or Superintendent are required. Requested access is set up by the NOACSC fiscal support team. Access is based on the user access request for received from the user entity. Roles and identifiers are assigned to segregate users within the application.

Password parameters governing minimum password length and complexity have been established as well as authentication break-in and detection rules.

IT Operations (SSDT Redesign)

Full system image backups are performed nightly and are replicated to disks located at a local user entity site. In addition, daily data disk backups are performed nightly, with that data being replicated to Van Wert as well. Weekly tape backups are also performed, which is completed on Friday nights. All backup tapes are stored in the onsite safe daily and rotated to an offsite storage location on weekly.

Development and Implementation of New Applications or Systems (SSDT Classic)

The NOACSC staff members do not perform system development activities. Instead, the NOACSC 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 MC, 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 (SSDT Classic)

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 NOACSC staff. Global issues are posted to the SSDT support website.

The NOACSC personnel do not perform program maintenance activities for USAS, USPS, or SAAS. 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 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. In order to maintain continued support of the application software provided by the SSDT, ITCs are expected to apply updates within 30 days of release.

The NOACSC uses a software utility called OECN_INSTALL to unpack these zipped files and install each individual package into its proper OECN directory. The OECN_INSTALL utility has an INSTALL_PACKAGE procedure with several functions that installs full package releases, partial releases or patches on the system. This utility ensures that all required components are installed properly and consistently.

Only vendor-supplied changes are made to the operating system or system software documentation. As a participating member of the MC, an ITC can enter into a cooperative agreement, "Campuswide Software License Grant (CSLG) and Education Software Library (ESL) Program", through the MC, 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 MC board of trustees.

The services acquired and/or provided by the MC 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 MC.

- 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 MC.

- 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 MC program, the participating ITCs agree to the following:

- Maintain its status as a member in good standing of the MC 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 MC.
- 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 MC 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 MC for services under the agreement within 30 days of the receipt of an invoice for said services.

Before new releases are installed at the NOACSC, 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. There were no upgrades to the operating system during the audit period.

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. The NOACSC is able to purchase the operating system software at a reduced cost under MC. No new releases were installed during the audit period.

IT Security (SSDT Classic)

The NOACSC has a security policy that outlines the responsibilities of user entity personnel, the NOACSC personnel, and any individual or group not belonging to a user entity or the NOACSC. The NOACSC uses the signatures on the authorized account application forms as an acceptance to the security policies of the NOACSC. Every year user access is confirmed with user entity management through a positive confirmation process. A list of users and their corresponding access rights within the user entity is generated and sent to the respective treasurer. The treasurer is required to confirm that all users are valid active users and their corresponding identifier/user access is appropriate. In addition, every 120 days, the account review team meets to review and discuss OpenVMS account adds, deletes, and changes for the last 120 days. All changes to user entities are reviewed and discussed.

Users from the user entities are granted access upon the receipt of a written "Authorized Account Application" form from the superintendent, treasurer, and/or supervisor. These authorization forms are sent to fiscal services who follow a documented process regarding the establishment of new accounts or modifications to existing accounts. The NOACSC 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. The manager network/student establishes, grants, and reviews access rights for data center personnel and an authorization form is not used.

The NOACSC policies and procedures are partly enforced using system alarms and audits. The following security alarms and audits have been enabled through the operating system to monitor security violations on the NOACSC system:

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 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, SUBPROCESS and DETACHED logon failure types can be monitored.

In addition, the following security audits have been enabled through OpenVMS to monitor for additional security violations:

INSTALL:	Audits modifications made to the last known file through the install utility.
TIME:	Monitors modification of the system time.
SYSGEN:	Monitors modifications of a system parameter with the system generation utilities, SYSGEN or AUTOGEN.

A batch processed command procedure executes each night to extract security violations from the audit log and creates summary and detail reports. These reports, also called security monitor reports, are e-mailed to the executive director and network services 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 NOACSC utilizes anti-virus software to scan inbound and outbound e-mail. Virus definitions are updated daily, and infected items are deleted.

Primary logical access control to the HP computers is provided by security provisions of the operating system. Individual user profiles are used to grant access rights and privileges for the system. This includes access to data, programs and system utilities. When a user logs in to use the system interactively, or when a batch or network job starts, it 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 NOACSC utilizes proxy logins. A proxy login enables a user logged in at a remote node to be logged in automatically to a specific account at the local node, without having to supply any access control information. A proxy login differs from an interactive login because an interactive login requires a user to supply a user name and password before the user can perform any interactive operations.

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.

Access to the operating system command line is restricted using login scripts and the CAPTIVE flag. All user accounts are set up with the CAPTIVE flag, which restricts access to the command line. The CAPTIVE flags are typically not used for administrative accounts (NOACSC employees or system accounts) because they require command line access.

Users must provide a valid operating system username and password to authenticate to the USAS and USPS web applications. Once authenticated, users are automatically given only those privileges assigned in each user's default login security profile. The SSDT developed a program called OECN_RPC (Remote Procedure Call) service, which, in conjunction with VXS created by the SSDT, allows users to authenticate through an 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, their 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 system forces users to change their passwords periodically. The systems manager sets passwords to expire when a new user identification code is issued. New users must log in "interactively" to change their passwords. Notification of password expiration for existing users occurs automatically prior to the password expiration date. The NOACSC has established minimum password lengths for all user accounts. When a user logs in to the USAS and/or USPS web applications, the user authorization file is updated to reflect that a non-interactive login has occurred. When a user logs in to the FISCWEB application, the user authorization file is not updated to reflect that a login has occurred.

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.

System parameter standards have been established using HP established defaults. Any changes are logged and reviewed by the executive director and/or network services manager.

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. The web applications also have a time-out feature that was created by the SSDT. This allows the NOACSC to modify the time-out parameter to match NOACSC policies. Also, timeout programs aid in efficient use of system resources by maintaining connectivity with only active system users.

The User Identification Codes (UIC) are individually assigned to all accounts. UIC based protection controls access to objects such as files, directories, and volumes.

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

SYSTEM: Any of the following: (1) Users with a UIC group number between 1 and the SYSGEN parameter for 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.

Through a firewall and switch, user entities have been set up with sub-networks that have addresses not recognizable to the Internet, known as a private internal network. The firewall and switch also prevent all outside connections from accessing inside hosts or servers, unless the IP address originated from inside the network or the user entity requests certain access to their network from outside (i.e. HTTP, and e-mail, etc.). The NOACSC staff use an internal wireless access point to provide a convenient means of access to the network. Wireless traffic is encrypted from point to point within the building. Access to the wireless device's configuration is controlled through password protection.

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 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.

A powerful identifier, OECN_SYSMAN, grants all access privileges to all state developed software and is restricted to authorized NOACSC staff. In addition, the BYPASS privilege automatically grants the user the OECN_SYSMAN identifier. The BYPASS privilege is an operating system privilege and functions the same for all ITCs.

To limit access to security files, the NOACSC has limited the WORLD access for the user authorization file. The user authorization file contains account information to identify which users are allowed access to accounts on the system; the proxy file, which contains proxy account information to identify which remote users are allowed access to proxy accounts on the system; and the rights file, which contains names of the reserved system identifiers and identifiers for each user.

The write and delete access capabilities are not activated for WORLD access to the files in the system directory. The UIC associated with each of these files is within the MAXSYSGROUP number.

Certain privileges can override all UIC-based and ACL protection. The operating system analyzes privileges included in the user's UAF record and places the user in one of seven categories depending on which privileges have been granted to the user. Default privileges are those authorized privileges that are automatically granted at login. If an authorized privilege is not a default privilege, it will not automatically be effective at login, and must be enabled or disabled by the user. All user entity users have NORMAL privileges.

Remote access to the firewall and various switches is restricted through password protection. Additionally, passwords are encrypted in the devices' configurations.

The data processing department is in an enclosed area, secured by both a key lock and a Lima Security alarm system. All doors are locked during off hours. During daytime hours, all doors entering the building and to the computer room remain locked at all times. The Lima Security Inc. monitors all building doors and motion detectors 24 hours a day, 7 days a week.

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

- Fire extinguishers.
- Heat alarm in the event the temperature exceeds preset level.
- Two split Goodman units are used to monitor temperature and humidity.
- All devices are connected to battery backup systems.
- Entire building utilizes a standby natural gas powered generator that can run the entire building.

The environmental controls and alarms are attached to the security system, which will alert the security company if something is detected. The security company will then contact the appropriate personnel.

IT Operations (SSDT Classic)

Traditional computer operations procedures are minimal because user entity personnel initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All NOACSC employees have access to an operations procedures manual, which provides directions and guidelines for most of the operational functions performed. In addition, all users, except students, have access to the SSDT website that contains user and technical documentation for the applications.

The NOACSC staff has privileges that permit them to assist participating user entities in performing data entry transactions. The privilege is necessary in order to respond to requests to resolve data entry inaccuracies. NOACSC personnel are not allowed to make modifications to user entity data outside the normal application process. Additionally, NOACSC requires approval via e-mail or phone call (help desk ticket) prior to assisting user entities. In addition, NOACSC as part of the fiscal year end procedures runs the FISCALCD.COM for USAS and USPS reports. The reports created by this command file are put on the web and are burned to CDs that are given to the user entities. The user entities may print out an "AUDIT" report, which shows activity changes to the data file for changes made through the application.

Operations at the NOACSC consist primarily of application installation, system software installation, backup procedures, restart and recovery procedures, and maintenance procedures. The NOACSC also serves as a help-line to the user entities. The user entity's users call the NOACSC whenever they have a problem with applications or hardware.

NOACSC is responsible for operational maintenance tasks, such as system backups, file rebuilds, log reports, and other maintenance directed at the whole system. They use two automated applications to schedule and perform these tasks.

User entities are responsible for handling abnormal terminations. If the users cannot solve the problem, they will contact the NOACSC staff. Service Express is contacted for hardware problems that cannot be solved by the NOACSC staff. The NOACSC staff often handles daily problems (e.g., terminal lockups or program crashes) over the phone. If necessary, a staff person will come on-site to resolve the problem.

Network devices at the NOACSC are continuously monitored with the use of the Pinger application software. The program continuously contacts all network devices. In the event a device does not respond, a network technician is contacted through an automated process to resolve the issue. Full system image backups are performed daily to disks located at Elida Local schools. In addition, daily data disk backups are performed nightly, with that data being replicated to Van Wert. Nightly Tape backups are also performed for all data except for archive data, which is backed up to tape on Friday nights. All backup tapes are stored in the onsite bank vault daily, with the full system backup tape from Friday night being rotated to an offsite storage location on Wednesday of each week.

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

COMPLEMENTARY USER ENTITY CONTROLS

NOACSC's controls related to its Information Technology General Controls (ITGC) System only cover a portion of overall internal control for each user entity of NOACSC. It is not feasible for the control objectives related to the ITGC System to be achieved solely by NOACSC. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with NOACSC's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified under each control objective below, where applicable. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

IT General Control Procedures (SSDT Redesign)

Acquisition and Implementation of New Applications or Systems – *Control Objective:* Management should assess the ongoing needs for new Information Technology (IT) and monitor the installation of any acquisition(s) to ensure its successful implementation.
1. User entities should perform parallel system testing and maintain evidence of management review of testing results. 2. User entities should maintain current service level agreements with their ITC for USASR and USPSR support.

Changes to Existing Applications and Systems – *Control Objective:* Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.
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.

IT Security – *Control Objective:*
Management should ensure the implementation of access control policies and procedures, which are based on the level of risk arising from access to programs and data.

1. User entity management should have practices to ensure USAS/USPS-Redesign users are aware of their ITC's security policies and that users take precautions to ensure passwords are not compromised.

2. User entity management should immediately request the ITC to revoke the USAS/USPS-Redesign access privileges of user entity personnel when they leave or are otherwise terminated.

3. 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.

4. User entity management should provide training to ensure users have the knowledge to detect cyber threats and the procedures of how to report these threats to management.

5. Access privileges for USAS/USPS-Redesign should only be issued to authorized users who need access to computer resources to perform their job function.

6. 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.

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

IT Operations – *Control Objective:*
Management should have controls in place for the operation of the computer system to guard against high-levels of system downtime, data processed against incorrect files, job failures, and reruns.

1. 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.

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

IT General Control Procedures (SSDT Classic)

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.
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.

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.
1. User entity management should have practices to ensure users are aware of the ITC's security policies and that users take precautions to ensure passwords are not compromised. 2. User entity management should immediately request the ITC to revoke the access privileges of user entity personnel when they leave or are otherwise terminated. 3. User entity personnel should respond to account confirmation requests from their ITC. 4. 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. 5. User entity management should provide training to ensure users have the knowledge to detect cyber threats and understand the procedures for reporting identified threats to management.

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

IT Security - *Control Objective:* **Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.
1. 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. 2. Communication lines, junction and modems should be secured in an area that restricts access to only authorized individuals.

IT Operations - *Control Objective:* **Backup -** Up-to-date backups of programs and data should be available in emergencies.
1. 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. 2. User entities should establish and enforce a formal data retention schedule with their ITC for the various application data files.

.

SECTION 4 – DESCRIPTION OF NOACSC'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND THE INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Information Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at NOACSC.

Our examination was limited to the control objectives and related controls specified by NOACSC in Sections 3 and 4 of the report, and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, NOACSC's controls may not compensate for such weaknesses.

NOACSC's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by NOACSC. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by NOACSC, we considered aspects of NOACSC's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Test	***Description***
Inquiry	Inquiry of appropriate personnel and corroboration with management.
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control.
Reperformance	Reperformance of the control.

In addition, as required by paragraph .35 of AT-C section 205, Examination Engagements (AICPA, Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

IT GENERAL CONTROL OBJECTIVES AND RELATED CONTROLS

NOACSC offers two versions of the financial software as provided by the State Software Development Team (SSDT), which includes the Classic version (USAS, USPS, SAAS/EIS) running on an OpenVMS operating system and the Redesign version (USAS-R and USPS-R) running on a Ubuntu Linux operating system. Testing below will be designated as either SSDT Classic or SSDT Redesign.

A list of NOACSC's user entities and the applications being used by each entity was provided by NOACSC and is included in Section 5 of this report.

Acquisition and Implementation of New Applications or Systems (SSDT Redesign)

Acquisition & Implementation of New Applications or Systems - *Control Objective:* I**mplementation** - Management should assess the ongoing needs for new Information Technology (IT) and monitor the installation of any acquisition(s) to ensure its successful implementation.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Test import logs are reviewed for errors and any errors identified are communicated to the user entity.	Inspected a copy of the migration procedures from the fiscal liaison to confirm testing is performed before going live.	No exceptions noted.
The user entity and ITC sign off that parallel testing has been completed for at least one processing period and financial totals have been successfully compared and reconciled	Inspected an example of the "Certification Questionnaire for Redesign Go-Live Authorization" form with the fiscal liaison to confirm user entities have to sign off on this for before go live.	No exceptions noted.
Balancing reports are used to reconcile data between the USAS/USPS Classic system and the USAS/USPS Redesign system. Errors identified during the balancing process are communicated to the user entity.	Inspected the procedures and checklists with the fiscal liaison to confirm balancing is done for each user entity.	No exceptions noted.
NOACSC provides training to the user entities where user entities process transactions using training checklists.	Inspected the training documentation with the fiscal liaison to confirm training was provided to the user entities.	No exceptions noted.

Changes to Existing Applications and Systems (SSDT Redesign)

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:*
NOACSC uses the SSDT provided Cron job script to schedule a nightly run to search for updates from the SSDT's Delivery Pipeline.	Inspected the nightly Cron job script with the fiscal liaison for evidence of the nightly search for updates.	No exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements and problems corrected. Updated user and system manuals are also made available.	Inspected the release notes and updated manuals to confirm they have been updated for the 2019 releases.	No exceptions noted.

IT Security (SSDT Redesign)

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:*
USAS-R and USPS-R users are restricted to predefined logical access identifiers that grant varying access privileges.	Obtained and inspected a listing of all USAS-R and USPS-R security roles and their related permissions to ensure application level access has been set to enhance the segregation of duties.	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 appropriate user entity management was required before setting up an account for the USAS-R and USPS-R applications.	Inquired with the office assistant to confirm authorization from user entity management is required. Inspected the USAS-R and USPS-R user listings for all user entities to confirm access is segregated. Compared the prior year SYSUAF file to the current USAS-R and USPS-R user listing to identify newly added users. Inspected two of the two new user accounts for the Redesign applications and confirmed access granted was in agreement with the access authorized by management per the access request forms.	No exceptions noted.
Application level parameter settings for passwords and authentication procedures have been established for users of the Redesign applications.	Inspected the application level parameter settings for passwords and authentication procedures to confirm the following: • Password minimum length and complexity requirements are in agreement with NOACSC's policies. • Authentication and lockout parameters have been set to limit access.	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:*
NOACSC staff authenticate through Active Directory (AD) in order to access the Redesign applications for support.	Inspected the AD parameters with NOACSC staff to confirm restrictions were in place for login.	Domain policies have not been set to industry standards for password expiration and invalid login attempts; however, individual parameter settings have been established for all but the following two NOACSC accounts: • Administrator • MCOECN Student Support account limited to SIS servers through VPN. No other exceptions noted.
User access is protected by a secure site login and default administrator passwords have been changed.	Inspected the NOASC website and attempted to enter default usernames and passwords to confirm Redesign logins are secure and default passwords have been changed.	No exceptions noted.
Access to the Hyper-V Management console is restricted to NOACSC personnel.	Obtained and inspected access to the Hyper-V Management console, with the network services manager, to confirm access is restricted to NOACSC staff.	No exceptions noted.

IT Operations (SSDT Redesign)

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:*
All data center hardware and software equipment is covered by an insurance policy.	Inspected the property insurance policy and proof of payment for coverage of NOACSC equipment to confirm coverage was in place during the audit period.	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:*
Software monitors network performance and alerts staff of hardware failures.	Inspected the system status screen for the network monitoring software with the manager network/student to confirm the network monitoring software is used to detect and resolve hardware problems.	No exceptions noted.
NOACSC uses the SSDT provided Cron job script to provide complete backups of the database servers twice a day. The backups are replicated to an offsite storage facility daily.	Obtained and inspected the CRON job script with the manager network/student for evidence of the daily backup schedules and policies.	No exceptions noted.

Changes to Existing Applications and Systems (SSDT Classic)

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 the SSDT, ITCs are encouraged to install new releases within 30 days of the software release date.	A cyclical redundancy check (CRC) of the USAS, USPS, OECN, and SAAS/EIS object files at NOACSC was compared to the CRCs of the object files at the SSDT.	No exceptions noted.
The SSDT distributes release notes explaining the changes, enhancements and problems corrected. Updated user and system manuals 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 documentation for the most recent version of the operating system.	No exceptions noted.

IT Security (SSDT Classic)

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 NOACSC requires a standard form for user authorization for all users other than NOACSC staff. The authorization form must be signed by the appropriate management before adding, modifying or removing a user account on the system.	Inspected 15 user authorization forms from a population of 154 new users to confirm the required signatures were present. Selected four accounts from a population of 17 existing user accounts that were modified during the audit period, and inspected the authorization forms to confirm the required signatures were present.	No exceptions noted.

IT Security - *Control Objective:* **Security Management -** Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
User access is confirmed every other year through a positive confirmation process. NOACSC tracks the status of the confirmation and follows up with a reminder message to facilitate a response from the user entity.	Inquired with the executive director to confirm the confirmation process. Inspected the confirmation checklist used to track the return of the confirmations.	No exceptions noted
The 120-day account review team meets to review and discuss modifications made to OpenVMS accounts for the last 120 days.	Inspected documentation maintained to confirm the 120-day account review process.	No exceptions noted
Detection control alarms are enabled through the operating system 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 enabled security audits to confirm security violations are being logged.	No exceptions noted.
A command procedure executes each night to extract security violations from the audit log and create summary and detail reports called the security monitor report. The security monitor report is generated daily and is e-mailed to NOACSC staff for review.	Inspected the following information related to the security monitor report to confirm reports are produced and available for review daily: • Security monitor reports. • Command procedure used to generate the reports. • Scheduler job parameters for the security monitor reports. Independently confirmed the process for review of the security monitor report with the network/student manager.	No exceptions noted.
Anti-virus software interactively scans all inbound and outbound email on the mail server and file server before the mail is forwarded to the virtual Alpha. Updates to the ESET definitions occur at regular intervals.	Inspected the properties on the ESET server to confirm virus definition files are updated and incoming traffic is scanned for viruses and spam.	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 to confirm wild card characters are not used.	No exceptions noted.
Access to the operating system command line is restricted to authorized users.	Inspected user accounts that do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER, or RESTRICTED flags set with the manager network/student to confirm the appropriateness of the accounts.	No exceptions noted.
Password parameters are in place to aid in the authentication of user access to the system. Passwords used by individual profiles are in accordance with the password policies established by NOACSC.	Inspected the results of extracted information from the user authorization file to identify: • Accounts with password minimum length less than the NOACSC standards. • Accounts with a password lifetime greater than the NOACSC standards.	No exceptions noted.
Password expiration for the web applications is defined at the system or process level.	Inspected the system logical that controls remote access to confirm password expiration is enforced for the web applications.	No exceptions noted.
Login parameters have been set to control and monitor sign-on attempts.	Inspected the system login parameters to confirm parameters were set to control and monitor sign-on attempts.	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:*
System and web application activity is monitored and inactive users are automatically disconnected after a predetermined amount of idle time that meets industry standards.	Inspected the HITMAN parameters to confirm they were set to logoff inactive users. In addition, identified protected accounts and confirmed the appropriateness of accounts with the manager network/student. Inspected the system startup file to confirm the HITMAN utility was part of the startup process. Inspected the configuration for the timeout values on the OECN RPC service. Inspected the configuration for the timeout values on the USAS and USPS web system.	The HITMAN parameter setting for killing processes after a period of inactivity, has been set at an amount greater than suggested by best practices. No other exceptions noted.
Access to production data files and programs 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 that control Internet access. Inspected settings in the firewall configuration to confirm Internet traffic is restricted through the firewall and to confirm the existence of a private internal network.	No exceptions noted.
The wireless access point used by NOACSC staff is encrypted to prevent unauthorized access to the system.	Inspected the wireless router configuration to confirm encryption is used.	No exceptions noted.

IT Security - *Control Objective:* **Application Level Access Controls -** Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Users are restricted to predefined logical access identifiers that grant varying access privileges based on requests from user management.	Inspected all active user accounts with the OECN identifiers for the USAS, USPS, and SAAS/EIS application systems. Inspected the reports to confirm the identifiers were used to segregate access to the applications. Selected 15 accounts from a population of 154 new users and inspected the user authorization forms to confirm the access requested matched the access granted. Selected four accounts from a population of 17 user accounts modified during the audit period, and inspected the user authorization forms to confirm the access requested matched the access granted.	No exceptions noted.
The OECN_SYSMAN identifier that grants all access privileges for all state developed applications is restricted to authorized NOACSC users.	Inspected accounts from the user authorization file with the OECN_SYSMAN identifier. Confirmed the appropriateness of the listed accounts with the manager network/student.	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.
System level UICs and accounts with elevated privileges are restricted to authorized personnel as determined by NOACSC staff. 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 listings with the manager network/student regarding the appropriateness of the listed accounts.	No exceptions noted.
Use of an alternate user authorization file is not permitted.	Inspected the value of the alternate user authorization parameter to confirm an alternate file is not permitted. Inspected the system directory listings to confirm an alternate user authorization file did not exist.	No exceptions noted.
Remote administration of the firewall used to control Internet access is restricted.	Inspected the firewall and main switch/router configurations to confirm remote administration was permitted and to confirm passwords are required to access the configuration menus.	No exceptions noted.

IT Security - *Control Objective:* **Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Physical access to the computer room and its contents is restricted to authorized personnel.	Inspected the computer room and inquired with the executive director regarding personnel access to the room. Inspected the service agreement and payment documentation to Lima Security Inc.	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 with the executive director to confirm the existence of the environmental controls.	No exceptions noted.

IT Operations (SSDT Classic)

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:*
A service agreement with Service Express covers maintenance and failures on the computer hardware.	Inspected the Service Express agreement for services covered, period of coverage, and the corresponding payment documentation to confirm the agreement was in place during the audit period.	No exceptions noted.
NOACSC runs routine system maintenance programs such as cleanup of data files, backup creation, and security log creation.	Inspected the startup file and the scheduler procedure listing to confirm routine system maintenance programs are initiated at startup and automatically scheduled to run.	No exceptions noted.
Software monitors network performance and alerts staff of hardware failures.	Inspected the system status screen for the network monitoring software with the manager network/student to confirm the network monitoring software is used to detect and resolve hardware problems.	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:*
All data center hardware and software equipment is covered by an insurance policy.	Inspected the property insurance policy and proof of payment for coverage of NOACSC equipment to confirm coverage was in place during the audit period.	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:*
Daily full backups of systems and data are performed Sunday through Saturday. Full backups are automated.	Inspected the backup command procedure and an example of the daily backup log with the manager network/student to confirm backup procedures.	No exceptions noted.
Backup tapes are stored in a secure on-site location and rotated to a secure off-site location regularly. Additionally, backup tape listings are used to track the location of backups.	Confirmed backup tape rotation procedures with the manager network/student. Inspected the on-site and off-site storage locations to confirm the backups were stored in secure locations. Inspected the backup tape listing to confirm the backups listed were stored at either the on-site or off-site storage locations.	No exceptions noted.
Backups of programs and data are replicated to off-site servers.	Inspected the off-site backup command procedure to confirm backups are automated and scheduled. Inspected example backup log and verification emails to confirm the backup status is verified and monitored.	No exceptions noted.

SECTION 5 - OTHER INFORMATION PROVIDED BY NOACSC (*Unaudited)*

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Name:	Northwest Ohio Area Computer Services Cooperative (NOACSC)
Chairperson:	R. Todd Schmutz Superintendent Pandora-Gilboa Local Schools schmutzt@pgrockets.org
Fiscal Officer:	Michelle Buss, Fiscal Liaison/Treasurer Michelle@noacsc.org
Administrator:	Ray Burden Executive Director NOACSC ray@noacsc.org
Address:	4277 East Rd Elida, OH 45807
Telephone:	419-228-7417
FAX:	419-222-5635
Web site:	www.noacsc.org

OTHER SITE STAFF

Kevin Hellman	Manager Network/Student
Eric Schumm	Sr. Support Network
Dave Daugherty	Sr. Support Network
Scott Schaffner	Sr. Developer/DBA
Carolyn Winhover	Support EMIS
Sheila Rowe	Sr. Support EMIS
Jaime Best	Sr. Support Student
Alanna Pugsley	Support Student
Paige Hart	Support Student
Michelle Buss	Fiscal Liaison/Treasurer
Amy Lawhorn	Support Fiscal
Larry Kaiser	Support Fiscal
Leah Moreland	Support Fiscal
Jon Pyles	Developer Fiscal
Jennifer Schwartz	Office Assistant
Sherry Shaffer	Support Fiscal – Part Time
James Bishop	Tech Services (assigned to user entity)

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	Dell PowerEdge R710 Dual Intel® Xeon® CPU E5620 @ 2.40 GHz Stromasys Charon - AXP	Lines/Ports:	3	Memory Installed:	64 GB
Disk:	300 GB	Units:	8	Total Capacity	1.8 TB Available
Tape Unit	Dell PowerValut 124 T	Units	1	Max Density	200 GB
Printer	HP8150		2	Print Speed	32 PPM

USER ENTITY SITE DATA

			SSDT Classic				SSDT Redesign[c]	
IRN	**USER ENTITY**	**COUNTY**	**USAS**	**USPS**	**SAAS/EIS[a]**	**OTHER [b]**	**USAS-R**	**USPS-R**
045740	Allen County ESC	Allen	X	X	X	X		
045757	Allen East LSD	Allen	X	X	X	X		
050773	Apollo JVSD	Allen	X	X	X	X		
045765	Bath LSD	Allen	X	X	X	X		
045211	Bluffton EVSD	Allen	X	X	X	X		
043885	Delphos CSD	Allen	X	X	X	X		
045773	Elida LSD	Allen	X	X	X	X	05/07/18	05/07/18
044222	Lima CSD	Allen	X	X	X	X		
085639	Northwest Ohio Area Computer Services Cooperative	Allen					X	X
045781	Perry LSD	Allen	X	X	X	X		
045799	Shawnee LSD	Allen	X	X	X	X		
045807	Spencerville LSD	Allen	X	X	X	X	04/05/19	04/05/19
151175	West Central Learning Academy	Allen	X	X		X		
044727	St. Marys CSD	Auglaize	X	X	X	X		
044982	Wapakoneta CSD	Auglaize	X	X	X	X		
047415	Arcadia LSD	Hancock	X	X	X	X		
047423	Arlington LSD	Hancock	X	X	X	X		
047431	Cory-Rawson LSD	Hancock	X	X	X	X		
043984	Findlay CSD	Hancock	X	X	X	X		
000402	Findlay Digital Academy	Hancock	X			X		
047407	Hancock County ESC	Hancock	X	X	X	X		
047449	Liberty Benton LSD	Hancock	X	X	X	X		
047456	McComb LSD	Hancock	X	X	X	X		
047464	Van Buren LSD	Hancock	X	X	X	X		
047472	Vanlue LSD	Hancock	X	X	X	X		

USER ENTITY SITE DATA

			SSDT Classic				SSDT Redesign[c]	
IRN	**USER ENTITY**	**COUNTY**	**USAS**	**USPS**	**SAAS/EIS[a]**	**OTHER [b]**	**USAS-R**	**USPS-R**
045187	Ada EVSD	Hardin	X	X	X	X		
043729	Celina CSD	Mercer	X	X	X	X		
045310	Coldwater EVSD	Mercer	X	X	X	X		
048595	Fort Recovery LSD	Mercer	X	X	X	X		
048553	Marion LSD	Mercer	X	X	X	X		
048546	Mercer County ESC	Mercer	X	X	X	X	05/02/19	05/02/19
048579	Parkway LSD	Mercer	X	X	X	X		
048587	St. Henry Conservatory SD	Mercer	X	X	X	X		
048991	Antwerp LSD	Paulding	X	X	X	X		
045575	Paulding EVSD	Paulding	X	X	X	X		
049031	Wayne Trace LSD	Paulding	X	X	X	X		
134999	Western Buckeye ESC	Paulding/Van Wert	X	X	X	X		
049312	Col. Grove LSD	Putnam	X	X	X	X		
049320	Continental LSD	Putnam	X	X	X	X		
049338	Jennings LSD	Putnam	X	X	X	X		
049346	Kalida LSD	Putnam	X	X	X	X	07/02/18	07/02/18
049353	Leipsic LSD	Putnam	X	X	X	X		
049361	Miller City-New Cleveland LSD	Putnam	X	X	X	X		
049379	Ottawa-Glandorf LSD	Putnam	X	X	X	X		
049387	Ottoville LSD	Putnam	X	X	X	X		
049395	Pandora-Gilboa LSD	Putnam	X	X	X	X		
049304	Putnam County ESC	Putnam	X	X	X	X		
044891	Tiffin CSD	Seneca	X	X	X	X		
050351	Crestview LSD	Van Wert	X	X	X	X		
050369	Lincolnview LSD	Van Wert	X	X	X	X		
044966	Van Wert CSD	Van Wert	X	X	X	X		

USER ENTITY SITE DATA

			SSDT Classic				SSDT Redesign[c]	
IRN	**USER ENTITY**	**COUNTY**	**USAS**	**USPS**	**SAAS/EIS[a]**	**OTHER [b]**	**USAS-R**	**USPS-R**
051672	Vantage JVSD	Van Wert	X	X	X	X		
043638	Bowling Green City Schools	Wood			X	XX		
050674	Eastwood Local Schools	Wood			X	X	11/01/18	11/01/18
050708	North Baltimore LSD	Wood	X		X	X		
		TOTALS:	**52**	**50**	**52**	**52**	**6**	**6**

[a] SAAS/EIS – X[a] active user entities. All other user entities have SAAS/EIS data files, but are not actively using the application.

[b] Other – Applications other than SSDT-Classic and SSDT-Redesign used by the user entities.

[c] SSDT Redesign – dates in the USAS-R and USPS-R columns indicate the date the user entity went live on the SSDT Redesign applications.

OHIO AUDITOR OF STATE
KEITH FABER

NORTHWEST OHIO AREA COMPUTER SERVICES COOPERATIVE

ALLEN 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
JANUARY 2, 2019

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