NORTHWEST OHIO COMPUTER ASSOCIATION (NWOCA)
STATE REGION - ISA, HENRY COUNTY

SAS - 70

MAY 26, 2007 THROUGH MAY 23, 2008

Mary Taylor, CPA
Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

Mary Taylor, CPA
Auditor of State

INDEPENDENT ACCOUNTANTS' REPORT

Board of Directors
Northwest Ohio Computer Association (NWOCA)
22-900 State Route 34
Archbold, Ohio 43502

To Members of the Board:

We have examined the accompanying description of controls of the Northwest Ohio Computer Association (NWOCA) applicable to the processing of transactions for users of the Uniform School Accounting System (USAS), Uniform Staff Payroll System (USPS), School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS), Education Management Information System (EMIS), and Community Schools Average Daily Membership (CSADM). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the NWOCA's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the internal controls contemplated in the design of the NWOCA's controls; and (3) such controls had been placed in operation as of May 23, 2008. The control objectives were specified by the NWOCA management for the processing of USAS, USPS, SAAS/EIS, EMIS and CSADM with the assistance of the Ohio Department of Education. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of the NWOCA's controls that had been placed in operation as of May 23, 2008. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the NWOCA's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from May 26, 2007 through May 23, 2008. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user organizations of the NWOCA and to their auditors to be taken into consideration along with information about the internal control at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance the control objectives specified in Section III were achieved during the period from May 26, 2007 through May 23, 2008.

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

The information in Section IV describing the information technology center is presented by the ITC to provide additional information and is not part of the ITC's description of controls that may be relevant to a user organization's internal control. Such information has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for user organizations and, accordingly, we express no opinion on it.

The description of controls at the NWOCA is as of May 23, 2008, and information about tests of the operating effectiveness of specified controls covers the period from May 26, 2007 through May 23, 2008. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the NWOCA is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of the NWOCA, its user organizations, and the independent auditors of its user organizations.

Mary Taylor

Mary Taylor, CPA
Auditor of State

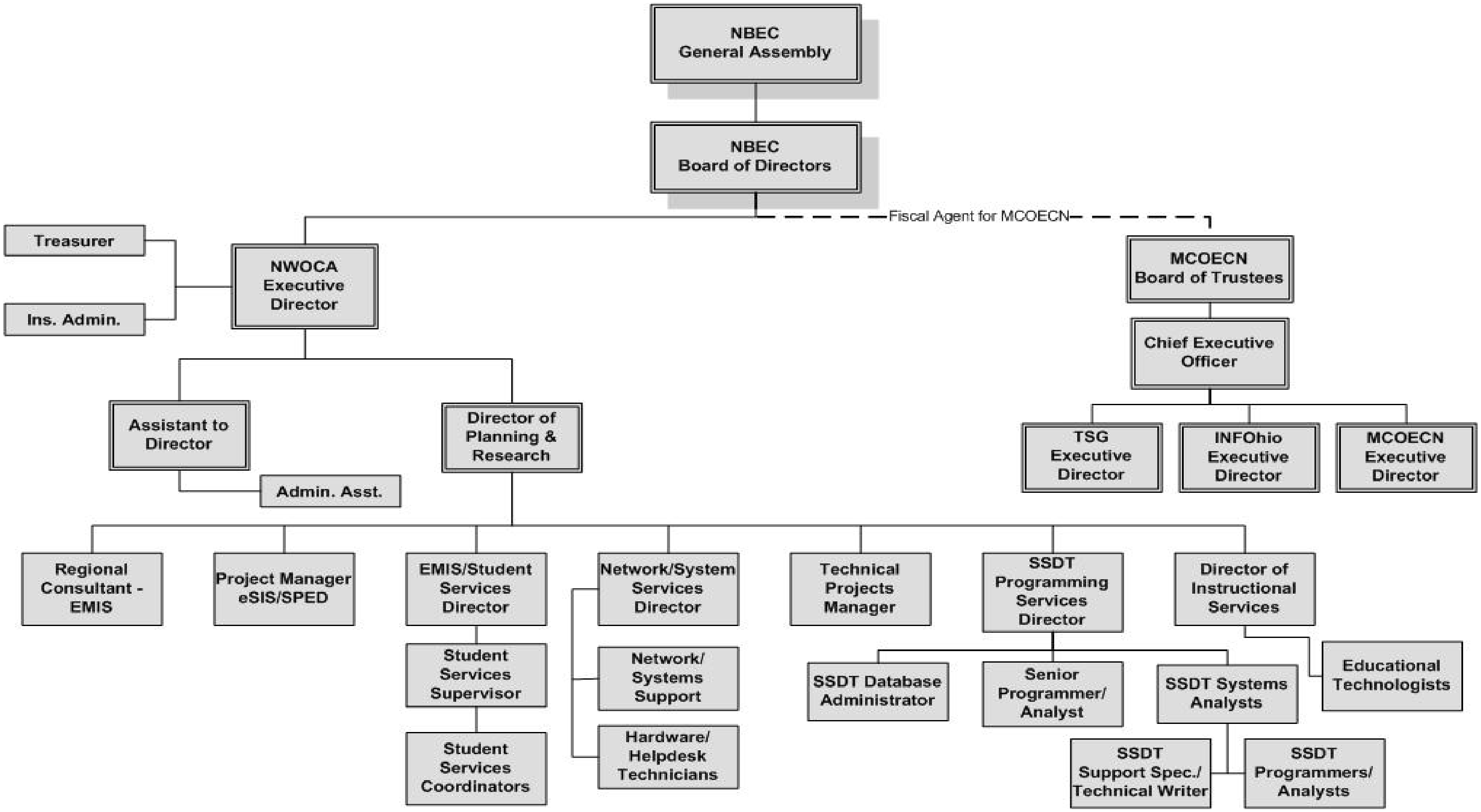
May 23, 2008

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The NWOCA's control objectives and related controls are included in section III of this report, "Information Provided by the Service Auditor", to eliminate the redundancy that would result from listing them here in section II and repeating them in section III. Although the control objectives and related controls are included in section III, they are, nevertheless, an integral part of the NWOCA's description of controls.

OVERVIEW OF OPERATIONS



The NWOCA is one of 23 not-for-profit computer service organizations serving more than 890 educational entities and 1.4 million students in the state of Ohio. These service organizations, known as Information Technology Centers (ITCs), and their users make up the Ohio Education Computer Network (OECN) authorized pursuant to Section 3301.075 of the Revised Code. Such sites, in conjunction with the Ohio Department of Education (ODE) comprise a statewide delivery system to provide comprehensive, cost-efficient accounting and other administrative and instructional computer services for participating Ohio entities. Funding for this network and for the NWOCA is derived from the state of Ohio and from user fees.

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

Uniform School Accounting System (USAS).
Uniform Staff Payroll System (USPS).
School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS).
Education Management Information System (EMIS).
Community School Average Daily Membership (CSADM)

ITCs are organized as either consortia under ORC 3313.92 or Council of Governments (COG) under ORC 167. ORC 3313.92 allows school districts to create a partnership (a consortia) to resolve mutual needs. One of the members of the consortia is designated as fiscal agent. The fiscal agent provides all accounting, purchasing, and personnel services for the consortia. A “COG” under ORC chapter 167 allows for one or more governmental entities to join together to form a new legal entity. A COG can have its own treasurer, make its own purchases, hire staff, and have debt obligations. The NWOCA is a subsidiary of the Northern Buckeye Education Council (NBEC). The NBEC is a council of governments, which exists to foster cooperation among its user organizations in all areas of educational service. The NWOCA is organized under both Chapter 167 and section 3313.92. Program assets of NWOCA are held in trust by Four County Career Center in its official role as fiscal agent for NWOCA.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the executive director and the NBEC board of directors. One member from each member user organization is appointed to the legislative body of the council known as the assembly and is normally the district superintendent. These member user organizations are voting members of the NBEC. The assembly meets at least twice per year to estimate program costs, approve annual appropriations, select officers and other members of the board of directors, and approve other matters as determined to require the approval of the assembly.

The board of directors is the governing body of the NBEC and is composed of two assembly representatives for each of the counties of Defiance, Fulton, Henry, Lucas, Williams and Wood, a representative of the fiscal agent of the NWOCA, and the representative of the Northwest Ohio Educational Service Center. The board is required to meet at least five times per year; however, it usually meets monthly. The board has also established several advisory committees to assist in the operation of the NBEC and its programs.

The NBEC board of directors has elected to work with the executive director in acting as the planning group for the organization. Because the board of directors sets direction for all aspects of the NBEC, the strategy for information technology is an integral part of the planning process. The manner in which planning occurs ensures the NWOCA information technology strategy is consistent with the direction being taken not only at the NWOCA program, but also at the NBEC as a whole.

The NWOCA employs a staff of 64 individuals 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 organization needs additional assistance for a period.

Student Services: Supports end users in all aspects of the student service applications with a focus on EMIS. Assists in the software development of the EMIS.

State Software Support: Develops, distributes and maintains the state software applications, including USAS, USPS, SAAS/EIS and EMIS. Provides documentation and training to ITC personnel responsible for training end users. Provides end user support for NWOCA user organizations.

Instructional Services: Provides a variety of instructional services to subscribing NWOCA user organizations including software and Internet access, training, technology planning, technical assistance, and grant writing assistance.

Network/Systems Support: Supports the NWOCA computer systems and its networked communication system. Provides user training and support.

The managers of each of the functional areas report to the director of planning and research.

The NWOCA is generally limited to recording user organization 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. Requests for changes to user data are infrequent and only experienced NWOCA employees may make these changes. Before NWOCA may make the change to user data, the user organization completes a User Intervention Form. The director of planning and research periodically reviews these forms to verify processing was not interrupted.

The NWOCA has adopted their own set of policies and guidelines, which are available to all employees via the web. Detailed job descriptions exist for all positions. The NWOCA is constantly re-evaluating its need for personnel to provide for the increasing range of services provided. Management periodically updates the reporting structure and job descriptions to create a more effective organization.

The NWOCA's hiring practices place an emphasis on hiring and developing skilled information technology professionals. Most positions within the organization require some type of college degree in a computer-related field, and all the NWOCA staff members are required to attend professional development and other training as a condition of continued employment. Each staff member must attend at least fifteen hours of approved professional development training annually, and at least eighty hours of approved training every four years. In addition, management encourages staff members to obtain additional training by providing a tuition reimbursement program for approved college work, and by paying 100% of incurred costs for attending professional development seminars. Employee evaluations are conducted annually. The managers for each of the functional areas perform the evaluations for their staff. The executive director performs the evaluations for the administrative staff and the director of planning and research performs the evaluations for the supervisory staff. The governing board performs the evaluation of the executive director.

Risk Assessment

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

- New technology.
- Realignment of the NWOCA organization to provide better service.
- Personnel issues, including hiring, termination, and evaluations.
- Additional services provided to user organizations.
- Changes in the operating environment as a result of ODE requirements, Auditor of State and other accounting pronouncements, and legislative issues.

In addition, the NWOCA has identified operational risks resulting from the nature of the services provided to the user organizations. These risks are primarily associated with computerized information systems. These risks are monitored as described under “Monitoring” below and in additional detail throughout the “General EDP Control” section of this report.

Monitoring

The NWOCA organization is structured so that department managers report to the director of planning and research. Key management employees have worked at NWOCA for many years and are experienced with its systems and controls. The NWOCA executive director and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, NWOCA uses a variety of “key indicator” reports to monitor the processes involved in processing transactions for user organizations.

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 run automatically through a scheduler program. Management receives these reports via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily. In addition, the director of planning and research and the network/systems services director receive the same reports and monitor these for interrelated and recurring problems.

INFORMATION AND COMMUNICATION

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

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

The NWOCA staff does not perform system development activities. Instead, software is developed and supplied by the State Software Development Team (SSDT). The SSDT is co-located with the NWOCA. The NWOCA has an agreement with the Ohio Department of Education Information Technology Office (ITO) to act as the fiscal agent and oversee the functions of the SSDT. The primary functions of the SSDT are to:

- Perform software development and maintenance of the OECN.
- Provide technical assistance in the use of the OECN state software.
- Coordinate and facilitate technical assistance to the OECN ITCs in the area of Internet access and network security.

The ODE determines the scope of software development for state-supported systems. Tactical means of accomplishing the priorities is determined by the Software Advisory Committee (SAC), which consists of members from the Management Council of the OECN (MCOECN), the Ohio Association of School Business Officials (OASBO), the ODE and the SSDT. The SAC meets approximately four times per year to discuss the status of proposed and ongoing projects.

JIRA is utilized for development of the COBOL production side of the applications. JIRA consists of a database of unique, sequentially numbered issues, maintained electronically, and is used to track program development. Each JIRA issue entry will contain a description of the change, the date requested, the date assigned, the scheduled release date, the programmer assigned, sign-offs for testing and documentation, management approval, and the date of completion. This system allows management to generate various reports to monitor each phase of the development process. In addition, a Work Hours Expended report documents the estimated and actual hours expended and can be generated and reviewed by management as necessary.

For development of the web enabling user interface, the JIRA issue tracking system is also used. A change order is referred to as a JIRA issue. Programmers select their own assignments from JIRA issues and assign the JIRA issues to themselves. JIRA maintains a list of outstanding issues that have been scheduled and prioritized by the team and systems analysts. Each programmer can select from this list without intervention from the systems analysts. The team leader is notified by JIRA via e-mail at each of the following stages of the JIRA issue process:

- When a JIRA issue has been assigned to a team member.
- When the process begins.
- When the JIRA issue is marked as resolved.

A JIRA issue is not closed until a systems analyst or the SSDT programming services director reviews it.

Cost benefit studies are not required as part of the program design phase of the development system because the majority of the significant application changes are mandated by the ODE, Internal Revenue Service (IRS) or School Employees Retirement System (SERS). A software change impact statement is completed by the SSDT after discussion of the need for the change. Because of the high degree of communication offered for the user community and the SSDT by SiteScape Forum and e-mail, programming errors can be brought to the attention of the SSDT management for quick resolution.

The SSDT Programmers Handbook is available to guide programmers when developing or maintaining structured programs. Included in the handbook are general programmer instructions for the following:

- Naming conventions for programs, data files, and logical and frame variables.
- Program report layouts.
- Use of GOTO statements, sub-programs, and source code comments.
- Standardization of CAP screens, screen layouts, PF-Keys, and help/error messages.
- Development, testing, and distribution of JAVA applications.

Standards and procedures have been established and made available to staff members to assist them in the testing process. Tests are performed for all significant program modifications, and programmers must approve JIRA issues electronically to document completion of the testing phase. The SSDT systems analyst or supervisor is required to review test results as part of the JIRA process. The SSDT systems analyst approves the JIRA issue when testing is completed.

Support specialist/technical writers are responsible for developing and maintaining user manuals and help screen documentation. User manuals include background information, a purpose statement, the theory behind a program, the goals of the program, start up information, reference material, how and when a program should be used, and error conditions. Documentation updates are included as a part of the quarterly software releases. Manuals are also available from the SSDT web site.

Support specialist/technical writers also prepare training manuals to assist employees of the other ITCs to provide hands-on training for their local user organizations. Training is ongoing for the NWOCA users. Semiannual meetings are held to help users accomplish fiscal and year-end closing tasks and make users aware of other significant changes. Additional training is scheduled as necessary.   For minor changes, an e-mail describing the change is sent to users. In addition, the NWOCA personnel are responsible for answering user inquiries and helping to solve user problems.

Changes to Existing Applications or Systems

Program enhancements and modifications are initiated through the Software Performance Report/Request (SPR) tracking procedure. The SPR system utilizes SiteScape Forum, an HTTP based product, to allow for electronic conferencing about proposed software enhancements in a public forum. SiteScape Forum is available to any user with Internet access and a graphical web browser. All ITCs and most user organizations have access to Forum conferences, providing end-user participation in the program development process. Users who do not have Internet access may request their local ITC to post the SPRs for them.

When the SPR is initially entered through the SiteScape Forum, the keyword “_NEW” is added to the note or forum entry by a systems analyst. This indicates that the SPR has been received but has not been reviewed by the proper SSDT or ODE staff, and is awaiting an official response. Any SSDT staff member may add this keyword to any note or Forum entry they perceive as an enhancement request or problem report.

Forum entries accepted by the SSDT management will have a written response indicating the action to be taken by SSDT on the SPR. Upon approval of the SPR by SSDT management, the keyword “_NEW” is replaced with “_WO” to indicate that the request has been approved but is waiting to be converted to a JIRA issue. Depending upon the complexity of the task, additional design and specification information, estimates, and schedules may be prepared by the systems analyst before preparation of the JIRA issue. If the Forum entry is not considered a valid request, the

SSDT will prepare a response explaining why they are rejecting the SPR. The keyword "_REJECTED" is then added to the note replacing the prior keyword "_NEW". The "_PENDING" keyword is added to the note after a work order is created. Upon completion of the change and approval by SSDT management, the keyword "_COMPLETED" is added to show the work has been completed and has been released or is pending release.

COBOL program changes are performed through JIRA and follow a five-step process:

- Source files are reserved and copied into the assigned programmer's directory to make the program changes.
- Program changes are tested by the programmer assigned to the work order.
- Additional testing is performed by a "buddy" programmer; however, this step may be skipped, with the approval of the systems analyst, for small changes or emergency changes.
- Test documentation is reviewed by the systems analyst.
- Finally, beta-testing is performed by NWOCA user organizations for a minimum of two weeks before the changes are distributed to the other ITCs.

The SSDT utilizes the Code Management System (CMS) to control and monitor changes to COBOL source code. SSDT analysts must "reserve" a program from the CMS library. If multiple copies of the same program are requested, each program is assigned variant version numbers. Only one of the variant versions can be "replaced" on the direct line of descent per each version level. A history file is maintained by CMS which contains all direct line descendants of each program allowing for recovery in the event of an error with the current version.

Policies and procedures require the SSDT systems analysts to review test results and approve the JIRA issue before moving the program change back into CMS. Programmers move their own files into the CMS Source Library upon approval from the systems analyst. On a nightly basis, programs with source code changes logged in CMS are automatically recompiled into production object libraries. As a compensating control, the SSDT programming services director monitors changes to the source code library and may be able to detect unusual module changes. The SSDT programming services director and systems analysts review the SYSBUILD log which reports all recompiled programs. All object modules are recompiled from the source code each week and the SSDT programming services director reviews a weekly CMS Summary and Status report, which lists all modifications made during the week. The process of compiling and linking files is performed by an automated command procedure called SYSBUILD.

Emergency program changes are also processed through JIRA; however, the SPR system is bypassed. A JIRA issue is opened and assigned to either the SSDT systems analyst or a programmer and is placed back into production by the person making the change. The entire process is performed at the authorization of the SSDT systems analysts.

For JAVA applications, the JIRA issue tracking system is also used for change order management. In JAVA, a change order is referred to as a JIRA issue. A programmer selects their own assignments from JIRA issues and assigns them to themselves. JIRA maintains a list of outstanding issues that have been scheduled and prioritized by the team and systems analysts. Each programmer can select from this list without intervention from the systems analysts. The team leader is notified by JIRA via e-mail at each stage of the JIRA issue process:

- When a JIRA issue has been assigned to a team member.
- When the process begins.
- When the JIRA issue is marked as resolved.

A JIRA issue is not closed until a systems analyst or the SSDT programming services director reviews it.

Concurrent Versioning System (CVS) replaces CMS for the JAVA project. CVS is the code management system for open-source projects such as the JAVA project. CVS allows the users to “check out” a working copy of the source library, but does not reserve any of the files. When changes are made, “committed,” to the central CVS library, an e-mail will be sent to the SSDT staff. Each user then “updates” their working copy. The update process merges changes from the library into the programmer’s working copy. Therefore, programmers always have a current copy of all committed source files and they can be certain that their changes will work with other changes made to the system. CVS detects when multiple programmers make changes to the same file and automatically merges those changes, but only as long as the changes are not made to the same lines of code. If a change is made to the same lines of code, it is the responsibility of the programmer making the commit to resolve the conflict, re-test both changes, and commit the change. Log files are maintained by CVS and are automatically attached to the JIRA issues. This log contains the programmer name, date of change, description of change, and section of code that was changed.

Testing of the JAVA programs is performed by JUNIT. JUNIT is a part of the JAVA Open Source software and allows programmers to easily write tests for new and existing modules. The tests are added to CVS and become part of the source for the project. The tests run as part of a nightly build in the application Cruisecontrol. This replaced SYSBUILD_JAVA.COM. If a test fails, a report is generated and sent to the programming team.

The process for creating a production distribution is similar to how SSDT releases the COBOL applications. The following briefly describes the process:

- Tag the CVS versions to be released in CVS to freeze the code.

- Build (compile) the code using an Ant script. The Ant script compiles the classes, stamps the version and build number and build date. Then it produces JAR and WAR files, which are special zip files containing the JAVA application. Everything the ITCs need to install the application is in one or two WAR files.

- The resulting WAR file is installed in the NWOCA's production J2EE web container/Tomcat. Tomcat is a product that functions like an operating system and runs the J2EE web server application.

- After any final system testing, the WAR is released to the ITCs for installation. If any problems are found with either the software or the installation, the process restarts with the first step.

Documentation of programming and system changes is the responsibility of the SSDT. The SSDT Documentalist Handbook and the SSDT Programmers Handbook contain the following procedures and standards.

- System documentation – Programmer/analysts are required to document the source code. Comments are included for the following: beginning comment, variables, storage fields, tables, structures, section headers, report layouts, and screen layouts.

- User documentation – Support specialist/technical writers are required to prepare and maintain user manuals and help screen documentation. The manuals are stored electronically as part of the CMS program library. The user manuals include background information, purpose statement, theory behind the program, goals of the program, start-up, reference material, how/when the program should be used, and error conditions.

- Operations Documentation – Support specialist/technical writers are also required to prepare operations documentation. Operation instructions include how and when procedures, error messages, screen layouts, output layouts, storage fields, tables, and structure definitions.

In addition, program change files are maintained as part of the CMS system. All versions of program documentation are maintained under the CMS history files. The CMS history file maintains an accurate chronological record of the changes to the WOS, SPR and Documentalist systems.

For JAVA applications, program change files are maintained as part of the CVS system. CVS provides for full history tracking with comments, date stamp and user, revision tracking, and ‘freezing’ generations for releases.

Quarterly release presentations are available via webcast on the SSDT’s web site. These presentations discuss application program changes and updates to the user documentation. Release notes are also distributed with each quarterly release and are also available through the web site. Documentation is updated after the program is placed into production, but before the program is released to the ITCs.

All JIRA issues for COBOL applications, with the exception of EMIS changes, have the documentalist portion of the JIRA issue completed. EMIS documentation is now entered in a “Wiki” application that is not related to a JIRA issue. Any programmer with access is encouraged to update documentation.

Only vendor supplied changes are made to the operating systems and system software documentation. There is a formal agreement with the HP Computer Corporation to keep the system documentation current, now an online system. The SSDT puts the OpenVMS documentation on the OECN web site for the current version of the operating system. The NWOCA’s staff and all other ITCs have access to the documentation.

Significant changes to the OpenVMS operating system are first loaded to a test Alpha and then tested by processing simultaneously with the current applications (dual processing). Testing of changes to the system utilize at least one of the NWOCA’s user organizations. Once tests have been completed and data processing management is satisfied with the results, all of the ITC’s are informed to update to the new version. Once all of the ITC’s have upgraded to the new version, the changes are implemented on NWOCA’s HP Alpha.

The NBEC, who acts as the fiscal agent for this and other participating ITCs, has entered into a license under the Campuswide Software License Grant Program (CSLG) through the MCOECN, for acquiring and/or providing software maintenance services for a limited series of HP software packages.

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

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

- Provide telephone technical support to the participating ITCs’ technical staff for a limited series of HP software packages approved by the board of trustees of the MCOECN.

- Track and maintain an accurate listing of all HP hardware and software covered under the agreement.

- Provide periodic training and update sessions covering the policies and regulations governing this program as well as updating the ITCs' technical staff on the latest releases of HP software packages covered under the agreement.

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

- Read, sign, and comply with the rules and regulations of the CSLG Program and the Education Software Library (ESL) Program as operated by the NBEC on behalf of the MCOECN.

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

- Provide HP or MCOECN representatives, upon prior written notice, with physical access to computer facilities at reasonable times during normal business hours to inspect sites and system records for compliance with the terms of the CSLG and ESL Programs.

- Make payments to NBEC for services under the agreement within 30 days of the receipt of an invoice for said services.

IT Security

The NWOCA has a security policy that outlines the responsibilities of user organization personnel, the NWOCA personnel, and any individual or group not belonging to the user organization or the NWOCA. The security policy is accessible through the NWOCA website. In addition to the security policy, the NWOCA uses banner screens that are displayed before a user logs in 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 the computer system are subject to having their activities monitored by the NWOCA personnel.

The NWOCA 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 network/systems services director and no authorization form is used.

Users from the user organizations are granted access upon the receipt of authorization (e-mail or written) from the superintendent, treasurer or assigned technology coordinator. The director of planning and research or the network/systems services director will create, update, or delete the account and e-mail the appropriate user organization designee regarding the request made. A file of e-mail requests is maintained for about one year and then copied to microfiche. This policy was implemented in 2006, any user that had access granted before then will not have documentation on file. A listing of users within the user organization is sent once a year to the respective superintendents to confirm the present users on the system are properly authorized. The listing does not include user access privileges and the NWOCA does not confirm accounts of non-member district users.

Access to the Internet has been provided to the user organizations of the NWOCA. Access is provided through the OECN GOSIP network. Each user organization is responsible for creating its own Internet usage policies. NWOCA provided an Internet usage policy, which can be tailored and used by the user organizations. All of the member groups have some type of Internet acceptable use policy. All documentation is maintained at the local user organizations.

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

Security alarm messages are sent to an operator terminal that has been enabled to receive security event messages. Security audit messages are sent to the audit log file; alarms are sent to the operator log file. Access to the operator log and audit log is limited to data processing personnel. Critical events should be reported as both alarms and audits; less critical events can be written to a log file for later examination. The following security alarms and security audits have been enabled through OpenVMS to monitor any security violations on the NWOCA 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.

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 network/systems services director 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 NWOCA utilizes Sophos Anti-Virus software to scan all inbound and outbound e-mail. If a virus is found, the e-mail is quarantined and the recipient and support staff are sent e-mails detailing the infected e-mail.

Access to web based applications including USAS, USPS, and EMIS is authenticated through a secure XML interface with a valid OpenVMS username and password. Once authenticated, users are automatically given only those privileges assigned in each user’s default login security profile.

The NWOCA 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.

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the NWOCA. For user organizations which use the NWOCA system, UICs are for the most part, functionally assigned and therefore, multiple user organization users may share an individual UIC. UICs are assigned at the user organization’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 DCL. Such accounts must be set up as restricted accounts, not captive accounts. User accounts should be set with the RESTRICTED flag instead of the CAPTIVE flag if they need to use network applications like MAIL or network proxy accounts. The RESTRICTED and CAPTIVE flags are typically not used for administrative accounts (treasurers and their staff) because access to the DCL prompt is necessary for them to manipulate print queues. However all other users, such as teachers and students, are assigned the RESTRICTED and CAPTIVE flags respectively. The RESTRICTED flag allows access to MAIL, but because the CAPTIVE flag is also assigned the use of the SPAWN command to gain access to the DCL prompt is prohibited.

The system forces users to periodically change their passwords. The majority of accounts have password lifetimes in accordance with the standards established by NWOCA. The teacher and student accounts were setup so the password change interval corresponds with the school year. These accounts do not affect financially significant functions and are not able to access financial applications. Passwords are set to expire when a new user identification code is issued or when a user has forgotten his password. This parameter requires the user to change his password during the first logon procedure. Minimum password lengths have been set according to the standards established by NWOCA.

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

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

System parameter standards have been established through the use of HP established defaults. Any changes are logged and reviewed by the director of planning and research and network/systems services director.

A timeout program 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 reduces 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.

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

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

SYSTEM: Any of the following: (1) Users with a UIC group number between 1 and the MAXSYSGROUP number. (2) Users with system privileges. (3) Users with group privileges whose UIC group number matches the UIC group number on the object. (4) Users whose UIC matches the owner UIC of the volume on which the file is located.

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

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

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

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

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

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

To limit access to security files, the NWOCA has limited the WORLD access for the following:

- Authorization file – contains account information to identify which users are allowed access to accounts on the system.
- Proxy file – contains proxy account information to identify which remote users are allowed access to proxy accounts on the system.

- Rights file – contains names of the reserved system identifiers and identifiers for each user.

Access to the OECN software packages is controlled at the ITC level by a security mechanism called the OECN Security Authorization (OSA) utility. Access to specific packages is provided by granting the appropriate OpenVMS identifiers to authorized users. Each application package has a set of unique identifiers that permit access to programs. In addition to the standard identifiers for each package, a pass through identifier can be used to further customize access. OSA is used in conjunction with the OECN menu processor utility thus allowing the users to see only the items they are authorized to execute. UIC-based protection prevents WORLD WRITE or DELETE access to USAS, USPS, SAAS/EIS and EMIS application data files.

User organizations have been set up with sub-networks which have addresses not recognizable to the Internet. This is called a private internal network. Firewall equipment and additional routing devices deny all outbound traffic requests originating from the subnetwork. In addition, the firewalls and routing devices deny access to all inbound traffic unless the IP address originated from inside the network. Instead, the requests are routed to a proxy server located in each network segment which serves to filter all Internet access. The Internet filter service retrieves requests from the Internet for the typical user. Permission to bypass the proxy server requires management authorization. In addition, an e-mail message is automatically sent to the director of planning and research, the director of instructional services, the network/systems service director, and the district technology coordinators each time the proxy server is bypassed. The firewall also prevents all outside connections from accessing inside hosts or servers, unless the IP address originated from inside the network.

The data processing department is in an enclosed area which is secured by both key and combination locks. The servers reside in the data processing computer room. All doors are locked during off hours. During daytime hours the main door is unlocked; however, data processing personnel are present at all times. The computer room and adjoining programming area remain locked at all times and are secured by a combination key pad lock. The combination is known by the data processing staff (including programmers), and maintenance personnel. Motion detectors are in place throughout the building.

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

- Halon fire extinguishers.
- Liebert system to monitor temperature and humidity.
- Power cutoff device which will shut down power to the computer room if the temperature exceeds a preset level.
- 30 KVA power conditioner with a one second carryover.
- 40 KVA UPS.
- Raised floor.
- Backup generator running on natural gas.

Windows Active Directory Domains

NWOCA utilizes Windows 2000 and Windows 2003 operating systems to control access to the NWOCA network. The network consists of three domains; NWOCALAND, NBECLAND, and SSDTLAND. NWOCALAND is the primary domain that NWOCA and SSDT staff uses to log into the network. The NBECLAND trusts the NWOCALAND domain and encompasses the nwapfs, nwwebapps, nwnet, and SQL_DEV servers in addition to others. SSDTLAND trusts the NWOCALAND domain and is considered a resource domain encompassing SSDT development servers.

NWOCA also maintains other domains for housing applications served to user organizations. These are AVSLAND for anti-virus and DISTRICTLAND for district Exchange e-mail users.

Individual user profiles are used to grant secure access rights and privileges to the network. Access to various system functions are controlled through the assignment of groups, approximately 32 groups and 157 accounts. Each group contains specific parameters defining access levels to the network (i.e., to files, directories, system functions, etc.). Unique user IDs and passwords are used to authenticate users before granting them access to the system. Security parameters have been set to control and monitor sign-on attempts for the NWOCALAND domain.

IT Operations

Traditional computer operations procedures are minimal because users at the user organizations initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All NWOCA employees have access to a procedures manual, which provides directions and guidelines for most of the operational functions performed. In addition, all users, except students, have access to SiteScape Forum, which is a bulletin board that allows the NWOCA employees to communicate with users across the state. Users can post questions and/or comments to the NWOCA staff through this site.

Common problems, such as disk drive failures, terminal lockups and program crashes, are usually handled by the NWOCA service representatives over the phone and are logged on an error log through the CA Unicenter, a help desk software package. For hardware problems which cannot be handled by the hardware technicians, the NWOCA staff contact HP directly. The maintenance agreement with HP is based on two service levels, a HP Service and a Basic Service. The HP Service requires on-site service within four hours of the request and a continuous response is provided until the problem is resolved regardless of the time of day or day of week, providing the original call is logged during the normal service window. Basic Service requires HP to be on-site within eight hours of a request. HP also has online internal diagnostics that will automatically reveal hardware malfunctions.

If the user organizations need a modification to system data, a File Intervention Form is completed and submitted to the NWOCA staff. The director of planning and research and the assistant to director periodically review the forms to verify processing was not interrupted. The user organizations have the option of printing an "AUDIT" report that will show activity changes to their data files.

The NWOCA performs daily system maintenance through routine jobs. These operational maintenance tasks (i.e., system backups, source code rebuilds, log reports, and other maintenance directed at the whole system) are scheduled by two automated applications, DECScheduler and SUBMITALL. DECScheduler continually submits jobs, such as backups, cleanups, checkups, dumps and purges, on the Alpha system; whereas, the SUBMITALL command schedules several jobs, such as creating daily indexes and fiscal reports from NWOCA databases and purging prior day indexes and fiscal reports, to run once a night. When a job is setup to be scheduled to run through the SUBMITALL or the DECScheduler, the programmer who scheduled the job will configure the application to respond with an e-mail if an error occurs while the application is running.

The program called ANALYZE, which is run through DECScheduler, helps prevent failure or corruption of the Record Management Services (RMS) databases. All of the OECN State Software (USAS, USPS, EMIS, SAAS,) applications utilize RMS file structures to store application data. Implemented in the OECN State Software applications is a series of ISAM files that are multi-keyed and have an ODBC-enabled view that comprises the “database” for the application. Once a week, ANALYZE will scan all files to verify that all files are readable and have no bad blocks, sectors or chains. If a problem is found by ANALYZE, an e-mail is sent to the director of planning and research and the network/systems services director. The NWOCA staff is then responsible for resolving the problem (usually recovering or rebuilding the data files).

Network performance is monitored through the use of an application called WhatsUp Gold. As the application runs, it displays all the devices for the network and their status. WhatsUp Gold submits a continuous ping to each network device to determine if it is active. If a device is not active, the device will be highlighted in red on the application and an e-mail will be sent to the network/systems services director and the network technicians responsible for the device. The network technicians will prioritize the problem and schedule maintenance accordingly.

Network and Internet traffic is monitored with the use of Bess filtering software. The NWOCA uses the Bess reporting tools mainly for trouble shooting the routers and firewalls.

The NWOCA maintains documented backup procedures and schedules to guide the operators in backing up programs and data. They also have a service agreement with Cerdant for support of the E-Vault backup software. All servers except for NWOCA4 use the E-Vault software.

Five servers and/or systems at the NWOCA west location are backed up regularly:

(1) NWOCA4, which is used for OECN and SIS applications, is backed up on tape.
(2) NWAPFS, which is used for the front end of the Web-GAAP application, is backed up to external RAID drives located off-site via fiber connection to the SOCC in Columbus.
(3) NWWEBAPPS, which is used for the front end of the USAS, USPS, and EMIS web applications, is backed up to external RAID drives located off-site via fiber connection to the SOCC in Columbus.
(4) NWNET, which is used for the CSADM and Web-GAAP production databases, is backed up to external RAID drives located off-site via fiber connection to the SOCC in Columbus.
(5) SQLDEV, which is used for Web-GAAP and CSADM development databases, is backed up to external RAID drives located off-site via fiber connection to the SOCC in Columbus.
(6) EMPOWER, which is used for CVS-JAVA, is backed up to external RAID drives located off-site via fiber connection to the SOCC in Columbus.

Full system backups are performed daily, at least Monday through Friday on the NWOCA4, NWAPFS, NWWEBAPPS, NWNET, SQLDEV, and EMPOWER servers. A stand alone backup is done nightly for the NWOCA 4 server. There are 30 backup tapes (one for each night) for the NWOCA4 server. The tapes are dated and are rotated daily off-site to the Archbold location. Tapes are kept on a one month rotation cycle.

All backups are documented in a system backup log. The log will indicate if the backup was successful or in error, the number of files written and the size of the data backed up. For the NWOCA4 server, an e-mail containing the system backup log is sent daily to a SSDT programmer/analyst.

If an error occurs on the NWAPFS, NWWEBAPPS, NWNET, SQLDEV, and EMPOWER server backups, a SSDT programmer/analyst, the SSDT database administrator, the director of planning and research, the assistant to director, the executive director, and a few other key personnel will receive an e-mail containing the system backup log and detailing the error.

An additional backup of all state software, historical changes, source code, executable images, and programmer libraries is sent daily via fiber to off-site locations in Archbold and Perrysburg. The only backup tapes used are in the Datastor library off-site for NWOCA4. The off-site location for tapes is in Archbold. Backup tapes backups are periodically used to restore files, but are not tested.

Restoring from backups is a work saving option open to all NWOCA staff members. Restoring files from backups happens infrequently at NWOCA. Restores most commonly occur when programmers or NWOCA staff accidentally deletes test files or when user organization data is in error.

For some errors, it is easier to restore older data than to correct mistakes made at the user organization. These restores are always requested by NWOCA support staff on behalf of the user organization. Restore requests are usually received by e-mail. The SSDT programmer/analyst generally performs all restores; however, in the event the SSDT programmer/analyst is not available, the restore may be performed by the database administrator, the network/systems services director, or the director of planning and research. Procedures for using this data and restoring it to the user organization are handled by the requesting department at NWOCA.

FINANCIAL APPLICATION CONTROLS

Uniform School Accounting System (USAS), Release 6.1

The USAS is a budgetary accounting system designed to be used by user organizations and county educational service centers. The criteria used for the system's design is the Ohio Chart of Accounts as set forth by the Ohio Auditor of the State's Office. The Chart of Accounts involves a thirty-digit account number with nine distinct dimensions.

Overall, the application is largely user controlled with the user being responsible for ensuring the completeness and accuracy of data input, processing and output through various reports. Reports are printed by request. Programmed control procedures, such as reasonableness tests, limit tests, checks for incomplete data, and checks for numeric or alphanumeric data, have been implemented to ensure complete and accurate data entry. The system will also provide warning messages if appropriation or cash amounts are exceeded. However, whether these and other types of transactions are allowed can be determined by the user organization.

User interaction with the system is simple and straightforward, requiring only basic familiarity with the terminal device connecting the user to the main computer. Data entries include such items as vendor information, accounts, purchase orders, invoices, receipts, transfers, and refunds. The system checks all entries for accuracy, processes the correct data, and produces various reports to provide information for managing the financial affairs of the user organization.

The AUDITS function produces an audit trail of additions, deletions and modifications to certain key files. Users are unable to bypass the automatic audit logging features of this program. Reports can be produced using various sort options. The management of the user organizations can use this function to track all changes made to data and detect any unauthorized changes made.

Users can change account codes or fund and special cost codes. The user must enter the original code as well as the new code. The system will (1) prompt for each account field and display the entire code as entered and (2) request the user to confirm the accuracy of the code before updating the associated transactions.

The Account Balance Report compares the fiscal-to-date and month-to-date amounts on each budget and revenue account with the total of the transactions on these accounts for a given fiscal year. If the totals are not equal, an error message is printed on the report indicating a particular account is out of balance, and a separate error report is generated. Users can run this program on a nightly basis to reduce the possibility of being out of balance at the end of the month or other fiscal period.

The Financial Report (4502) of the board of education includes a cash reconciliation option which can be used in the month end closing procedures and can also be used to reconcile bank statements to cash accounts. Exhibits 2 and 3 of the 4502 are the combined statement of revenues, expenditures, and changes in fund balances for the user organization and summarize the detail transactions recorded in USAS.

The Monthly Report Archival (MONTHLYCD) provides the ITCs with the ability to archive month-end financial reports and make the reports available to registered users online via a secure web site. This option generates about 30 monthly reports in a *.txt and *.pdf format. Reports generated include various month-end appropriation, audit, balancing, billing, budget, check register, purchase order, and vendor reports. Additionally, at the end of the fiscal year the ITCs may archive the monthly reports to one or more CD-ROMs. These month-end procedures are optional and are at the discretion of each ITC. The MONTHLYCD procedure can only be used if the ITC has acquired and configured the proper hardware and has properly configured the users' systems.

Access to USAS is provided by granting the appropriate OpenVMS identifiers to authorized users. When a user logs onto the application, each USAS program will look up the OpenVMS identifier held by the current process. If the process holds the required identifier, the execution proceeds normally. If the current process' rights list does not contain the required identifier, an error message is displayed and the program aborts immediately. In addition, the OECN menu processor utility allows the users to see only the items they are authorized to execute.

The USAS standard identifier is OECN_USAS. This, when granted to a user, allows standard read/write access to the package. In addition, there are four suffixes that may be attached to the standard identifier. These identifiers provide access to requisition only functions (OECN_USAS_REQ), read only functions (OECN_USAS_RO), group manager functions(OECN_USAS_GM), or provide a mechanism for bypassing security at the program level(OECN_USAS_PT). These program level identifiers (OECN_USAS_PT) allow for further customization of access. In addition, the program module, USASEC, may be used to further restrict access related to requisition processing, PO processing, vendor maintenance, appropriation maintenance and certain report and lookup programs.

The following are the four main financial transactions input into the USAS application:

- Receipts
- Investments
- Budgets
- Purchase Requisitions/Purchase Orders

Receipts

The Accounts Receivable Facility (ARF), provides a complete billing-payment system, and allows the user organization to identify what amounts are owed to it at any point in time. It can be used to provide information needed for Generally Accepted Accounting Principles (GAAP) accounting. It is also useful for generating invoices and recording payments on a current time basis. ARF also contains options to post either a receipt or a reduction of expenditure directly to the user organization's USAS files.

The ARF data entry screen heading displays the total dollar value of the current invoice being created as well as all receipts entered or all billing invoices created in the run. These totals can be used to confirm the completeness and accuracy of billing data entered. Additionally, ARF provides other reports management may use to confirm the accuracy of accounts receivable update transactions.

The Receipts Processing subsystem (RCPROC) is used to process receipts, refunds of receipts, and reductions of expenditures. The total of all transactions, which reflects the sum of all receipt transactions entered in a run, is displayed on the screen and could be used by the user organization to confirm the completeness of receipt transactions. Required verification fields within the RCPROC program force the user to enter a receipt transaction number, date of the transaction, and revenue account codes before a transaction can be processed. As each receipt transaction is entered, the receipt data is displayed on the terminal screen and the user is asked to confirm its accuracy before online update occurs. The online validity edit checks help prevent or detect incorrect entry of receipt transaction number, date of transaction, and revenue account codes prior to processing. Account codes and vendors must be valid. After entry of the account code, the account description is displayed, and the user is asked to confirm the displayed account is correct.

The USASWeb receipts module may also be used to process receipt and reduction of expenditure transactions.

The Student Fees Payment program may be used to automate posting student fee payments, extracted from a student software system, as USAS receipts.

For receipt transactions, dates cannot be outside of the current processing month or fiscal year. Entry of an invalid date will generate an error message and cause the date prompt to reappear. The Receipt File Editing function (RECEDT) and USASWeb allow for modification of the source or description, issue date, or transaction number of a receipt transaction. These modifications would be logged by the AUDITS program. In addition, the receipt ledger report can be used to create a listing of receipt transactions, which may be used to confirm completeness.

After the processing of a transaction into the RCPROC or USASWeb program, the application automatically updates the corresponding revenue and cash account balances for the amount of the transaction.

Reports are available in USAS listing all receipt transactions processed. The reports have the option of printing receipts, reduction of expenditures, refunds of receipts, appropriation modifications, budget modifications, fund-to-fund transfers, supply distributions, corrections, void refunds of receipts, all transaction types, or transactions by fund/receipt code. The reports can be sorted by transaction date or transaction numbers, and for all funds, a single fund, alpha funds only, all except alpha funds, or bank or group of banks.

A user’s access rights to the various functions within the ARF program can be restricted by an appropriately authorized user at the user organization, such as the treasurer. This function can be used to prevent users from having access rights outside of their job duties. The options available include:

- May enter billings.
- May enter payments.
- May add/modify ledgers.
- May add/modify customers.
- May add/modify receipt codes.
- May delete billings.

Investment Income

USAS includes an Investment Processing subsystem (INVEST) that allows the user to add an investment, enter an investment maturity date, cancel an investment, or generate an investment report. Required verification fields force the user to enter an investment number, date of the investment, check number, and vendor numbers before investment transactions can be processed. In addition, investment transaction data is displayed on the user’s terminal, and the user is prompted to confirm the accuracy of the data prior to its being processed to prevent or detect incorrect entry of investment numbers, date of investment, fund, check number, and vendor prior to processing.

Entry of an investment reduces the current balance of the corresponding cash account to give the current available cash balance. Users have the option to create a check record and enter new vendor data from within the program. The system does not perform interest calculations. The actual interest received must be entered through RCPROC or USASWeb.

Reports are available in USAS listing all investment transactions processed through the INVEST program. The reports can be sorted by transaction sequence number or by fund number sequence. Reporting is available on all investments, active investments only, or investments by maturity date. Management can use these reports to confirm the completeness and accuracy of information entered, such as interest rates and maturity dates.

Use of INVEST’s Investment Maturity or Cancel options to end an investment at or before maturity automatically reduces the amount of investments for the corresponding fund and increases the current available cash balance of the fund.

Budgetary

Budget accounts provide a breakdown of appropriated and actual expenditures. Budget and appropriation accounts are linked, meaning the total dollar amount on the budget accounts equals the total amount on an associated appropriation account. Most of the processing programs will prompt the user for a budget account, not an appropriation account. The amount in the budget account is also applied to an appropriation account.

The Appropriation Maintenance Program’s (APPROP), NYPMNT, NYPMASS, or NYPLOAD options, are used to enter either temporary or permanent appropriations before closing for the fiscal year. This program updates a "Next Year Proposed" field on the account record and the Next Year Proposed amounts are moved to the "Initial Budget" or "Initial Revenue Estimate" after the ADJUST program is run to close for the fiscal year. The IABMNT, IABMASS, or IABLOAD options of APPROP are used to enter either temporary or permanent appropriations after closing the fiscal year. These options update the current fiscal year's "actual" fields on the account record. Users can enter an amount for each budget or revenue account, can utilize a mass change option to modify all accounts on a percentage basis, or load the amounts in from a comma separated or tab-delimited file.

Users can print a budget worksheet from the system to help them prepare budget and appropriation information for data entry. The APPROP programs will list all account codes used in the current year when setting up a budget for the following year to help ensure all account codes are included in the user organization’s new budget. During entry of appropriation data, the system will prompt the user for amounts for each successive account; however, accounts can remain blank or zero. Totals are calculated and displayed to be matched to pre-calculated totals to help users verify all amounts were input for processing.

If the user attempts to enter a transaction using a date outside of the current processing period (month or fiscal year), an error message will be generated and the date prompt will reappear. The system will always display a warning message if the appropriation will be exceeded by the encumbrance or expenditure and ask the user if he wants to proceed.

Amounts entered on the budgetary worksheets in the APPROP program are automatically updated to the user organization’s yearly budgets and recorded on the REVWRK, APPWRK, and BUDWRK reports.

The Account Modification function (ACTMOD) processes appropriation and budget modifications during the fiscal year.

The Accounts Master File Editing function (ACTSCN) can be used for the addition of budget and appropriation accounts during the year and to make changes for month-to-date and fiscal year-to-date additions and deductions. The USASWeb accounts module may also be used to perform these functions.

Changes to the actual fund or account codes can be made through the Change Account Codes (ACTCHG) or Changes Fund/SCC Combinations (FNDCHG) programs. In addition to permitting normal account maintenance, an account number may be changed through these programs. The user must enter the original code as well as the new code, and then the system will prompt for each account field and display the entire code as entered and then request the user to confirm the accuracy of the code before updating the associated transactions.

The ACTCHG and FNDCHG programs produce a report after each use. Changes are also logged in the AUDITS report for user verification.
The list of possible account code dimensions are stored in the USAS.IDX file. User organization users do not have access to update function, fund, object, instructional level, or receipt number of the account codes, which are stored in the USAS.IDX file.

Direct maintenance of account code balances is completed through the Accounts Screen function (USASCN/ACTSCN). It can be used for the addition of budget and appropriation accounts during the year and to make changes for month-to-date and fiscal year-to-date additions and deductions. Account changes can also be made to budget accounts through the USASWeb. Account changes made are also placed in the AUDITS report. Access to directly modify the balances of the account codes without processing a transaction is restricted to the OECN_SYSMAN identifier.

The ACTBAL program produces an Account Balance Report (ACTBAL) that can be used to review appropriation, budget, and cash account balance information. The ACTBAL report compares the fiscal-to-date and month-to-date amounts on each budget and revenue account with the total of the transactions on these accounts for a given fiscal year. Users can run this program on a nightly basis to reduce the possibility of being out of balance at the end of the month or other fiscal period. At NWOCA this program is run in a batch mode for all user organizations, and users are sent a notification e-mail message. An Error Listing is produced by the ACTBAL program when an out of balance condition exists between the transactions processed and the budget and revenue accounts. An error report is also produced by the BALCHK program when an out of balance condition exists between the revenue and cash accounts or between the appropriation, budget, and cash accounts. If the totals are not equal, an error is printed on a separate error report indicating that a particular account is out of balance. At NWOCA, ACTBAL errors are corrected by the NWOCA staff.

A variety of budget reports are available for confirmation of the accuracy and completeness of budget data input.

Purchasing

Purchase order (PO) processing can be performed using four different programs, Expense Processing (EXPROC), Purchase Order Processing (USASCN/POSCN), Automatic USAS Posting (AUTOPOST), and the USASWeb purchase order module. USASCN/POSCN, and the USASWeb purchase order module allow for the entry of requisitions and/or POs and allow for quick creation of POs from requisitions. EXPROC allows for the entry of a PO, invoice, and check all in one step and is meant to be used only with entries that do not require a PO before processing, such as for utility payments. Users must create a PO for all expenditures and have the option to print them. Vendors can be added to the vendor file during EXPROC, USASCN/POSCN and USASWeb. AUTOPOST allows posting of POs and payroll data from a spreadsheet or fixed format file. In addition, the Mass Convert Requisition program (USASCN/MASCNV) can be used to mass convert requisitions into POs by a range of dates or a range of requisition numbers. There is no automated approval process for requisitions within the USAS application. Controls related to the approval of requisitions are at the user organization’s discretion. For instance, the user organization could print a hardcopy report listing requisitions for manual approval prior to processing; configure user access and use the USAS identifiers to segregate the entry process from the approval process; or use a combination of both.

Required verification fields within the POSCN program force the user to enter a PO number, item quantity, date, vendor number, and budget account code before a PO can be processed. PO numbers must be seven unique and numeric characters. Budget and appropriation accounts must exist on the master files prior to processing. A user may create a PO that exceeds both the budget and appropriation balances; however, USAS will issue a warning message. POSCN utilizes an optional user security profile that allows the treasurer to prohibit postings that would cause negative unencumbered balances at either the budget or the appropriation level.

Each PO must be processed completely before going on to the next one. Duplicate PO numbers are not allowed. An error message will be generated if the user tries to use a date from a prior fiscal year. A warning message will be issued if the transaction date is from a prior month in the current fiscal year or from a future month or fiscal year. POs for a future month or fiscal year can be entered into the system and printed out, then held in a batch file for posting to encumbrances once the current month/year is closed.

Invoices can be processed using the Accounts Payable Entry (APE), Expense Processing (EXPROC), USASWeb, or Automatic Posting (AUTOPOST) functions. APE allows for processing of invoices as they are returned from the vendor. It allows for marking of items for inventory and for making full or partial payments on an invoice, cancellation of a PO item or an entire PO. APE does not actually expend the money for the PO, but prepares the order to be paid later in the Check Processing program (CKPROC). APE also allows a vendor number to be input for payment for purchase orders issued to a “multi-vendor” vendor number.

A warning message is displayed if a PO or invoice amount exceeds the available budget, appropriation, or cash balance. In addition, the system displays the data and prompts for confirmation of correctness after all PO or invoice data is entered before updating the file. All fields do not have to be reentered during invoice processing. The PO and invoice number must be entered, and the PO data will be displayed for confirmation or modification. The same invoice and PO numbers may not be entered together more than once.

Purchase orders, invoices, and checks entered into the POSCN, APE, and CKPROC programs or via the USASWeb interface automatically adjust the appropriate appropriation, budget, and cash account balances.

The user has the option of printing a variety of reports for management reporting and for confirmation of the completeness and accuracy of requisition and PO data entered, as follows:

- The PO Detail program (USARPT/PODETL) or the PO Summary program (USARPT/POSUMM) can be accessed to generate a detailed or summary PO register to confirm that all input POs are available for processing.

- The USARPT/PODETL can be used to generate an outstanding purchase order report for a user to investigate and resolve long outstanding open purchase orders.

- The Recreate Lost or Destroyed PO Forms program (POFORM) or POSCN program can be used to recreate POs.

- The PO Information Listing (POINFO) program may be used to generate a detailed purchase order report for verification of purchase orders entered or outstanding purchase orders.

- The Invoice Listing program (INVLST) can be used to print a listing of invoices for a user to review that all invoices received are input for processing.

Payments Made for Goods and Services

CKPROC allows for the posting of expenditures for the outstanding invoices on file and can create printed checks or be used for memo processing. A beginning check number and date must be entered by the user with each new check-processing run. Throughout the processing run, the program will consecutively number the checks. Disbursement data is not re-entered into the system, but taken from the invoice and PO data already on the system. Checks can only have a date in the current processing month to ensure recording in the proper period. The manual check option can be used to record individual checks on the system without generating a printable check file.

Checks can be printed for all invoices on file, only those invoices entered, or all invoices excluding those entered. To help prevent duplicate payments, the system requires that all payments have a PO, and that a payment cannot be made against a closed PO. There must be enough cash in the correct fund or a warning message will be issued and the associated checks may not be processed depending on whether or not the user organization has allowed for negative cash balances in its set up options.

Users can print summary information prior to printing checks to confirm all cash disbursements are processed. Check registers can be printed and can be used to investigate missing, duplicate or long outstanding checks.

Non-cash Reductions of Accounts Payable

Both USASWeb and APE allow for the cancellation of a purchase order item or an entire PO. In APE, the amount canceled for the PO, as well as the amount canceled for all invoices processed in the run, may be displayed and can be used by management to confirm completeness of input.

To cancel an item, the user will enter the invoice and purchase order numbers, and the program will proceed item by item through the purchase order. The user can compare the PO items to the invoice and identify which items to process. USASWeb and APE will return the encumbered funds to the available balance. USASWeb or RCPROC can be used for the reduction of an expenditure. The INVLST can be used to print a listing of invoices which may help the user to confirm all adjustments are input.

Encumbrances

The Purchase Order Requisition modules (USASCN/POSCN, USASCN/MASCNV, and USASWeb Purchase Order module) encumber in specific accounts.

Carryover encumbrances do not have to be reentered unless the user organization chooses to do so. Users have two options when entering initial budget amounts. One option will prompt the user for the budget amount and will subtract the Last Fiscal Year Carryover Encumbrances from the figure entered by the user and enter this calculated amount in the budget field. The other option records the actual amount entered into the budget field.

Warning messages are displayed when appropriation or cash account balances are being exceeded. An error message is generated if a date from a prior fiscal year is entered. A warning message is issued if the transaction date is within a prior month of the current fiscal year or in the future. Transactions for a future month or fiscal year can be entered into the system and printed out, then held in a batch file for posting to encumbrances once the preceding month/year is closed.

Invoices cannot be entered into the system without a corresponding PO. Purchase order processing programs encumber funds against accounts. Account codes entered for purchase orders must be valid account codes.

The USARPT/PODETL and USARPT/POSUMM programs can be used to generate a PO report that can be used to confirm all formal commitments were entered. In addition, these programs can be used to generate a list of outstanding POs.

Vendor data can be added, modified or deleted via the vendor file editing program (USASCN/VENSCN) or the USASWeb. Vendors cannot be deleted if there are any year-to-date or fiscal year-to-date expended amounts or if the last activity date is within the current fiscal year. Vendor deletions are recorded in the audit file providing an audit trail for these transactions. Duplicate vendor numbers are prohibited. The Vendor Listing program (VENLST) can be used to print a listing of vendors to confirm the accuracy of vendor data.

The Inactive Vendors program (DELVEN) can be used to create a report of inactive vendors.

The program USASDAT/USASEC is an optional application level security program that allows the user organizations to limit the users who can modify the vendor file to only those users that require it for their job responsibilities.

When invoices are processed, the related PO number must be entered, and the vendor information is displayed. Vendor data does not have to be reentered, thus helping to prevent entries to incorrect vendor accounts.

When checks are processed through CKPROC or EXPROC, expenditures in the budget accounts are automatically increased while the encumbrances are decreased.

USAS Data Export

USAS data export produces a GAAP_EXP file that is used by the WebGAAP application. Changes to account balances made through USAS are reflected in the GAAP_EXP file.

Uniform Staff Payroll System (USPS), Release 4.2

The USPS application is a payroll system designed to create the employee and deduction company checks by running a series of programs in a specific order. Besides generating payroll and deduction checks, reports and data files are also created to meet reporting requirements to the Ohio Department of Job and Family Services (ODJFS), School Employees Retirement System (SERS), State Teacher's Retirement System (STRS), and the Education Management Information System (EMIS). This system also provides the ability to do any of the following: track benefit information (sick, personal, vacation); support direct deposit; generate a printable W2 form file; produce salary notices and/or special forms; generate custom reports; track absence and attendance days; and support the STRS annual reporting.

Another feature of this payroll system is that it interfaces with the USAS. During the payroll cycle a file is created for USAS users to post payroll expenditures to the appropriate USAS accounts. In addition, USPS interfaces with EMIS to supply information necessary to meet the reporting requirements for classified and certified employees.

The USPS application consists of a number of programs. These programs can be segregated into the following broad categories:

Start Up Programs - Certain initial information must be input before entering data about the user organization employees. Five programs are run to accomplish this. These programs provide the system with information regarding the user organization name, address, what will be printed on check stubs, how benefits are tracked, the buildings and departments, and any deduction company names and addresses the employees plan to use. If direct deposit is used, the ITC will run another program to provide transit routing numbers and other information regarding the direct deposits.

Employee Data Programs – These are modules of the USPS file maintenance program. There are thirteen modules that contain information specific to each employee. Employee information can be added, deleted, modified, and retrieved through these modules.

Primary Check Processing Programs – For each payroll cycle, a set of check processing programs must be run. While some of these programs are optional, certain programs are key elements in the payroll cycle. This set of programs drives the actual issuance of both physical checks and direct deposit forms for the user organization employees.

The system provides two modes of processing payrolls. The first mode allows for the processing of only one payroll at a time, while the second mode allows for the processing of multiple simultaneous payrolls. Both modes use the same check processing programs. However, different menus and options will appear in these programs based on the mode chosen by the user organization.

Check Processing Follow-Up Programs – After each check processing run, various programs should be run to provide historical reports and perform other functions (e.g., reconciliation, verification) related to the payroll cycle. Deduction checks for taxes and retirement plans are normally created after each payroll. Other deductions may be paid on a monthly or quarterly basis. This set of programs performs a variety of functions including deduction reporting, check status reporting, voiding and reissuing checks, and the creation of checks for each deduction recipient.

Monthly or Demand Programs – Certain summary reports can be produced on a demand basis. These are usually done monthly and include the ability to print history information and provide estimates of outstanding obligations for wages and benefits. In addition, a leave projection program creates a posting file from which employee absences may be charged to the proper leave accounts.

Quarterly Programs – There are two programs that should be run quarterly. These programs generate reports and/or magnetic tapes that are used for IRS and ODJFS reporting purposes.

Annual Programs – These programs are run for year-to-date reporting purposes. They can also be used for generating W-2 forms and creating a report of the total amount of money already paid to the STRS for employees within the user organization. These programs create submissions files (i.e. W2TAPE.SEQ) and submission reports (i.e. STRS) as opted by the ITC.

USPS Report Programs – These programs produce several useful reports ranging from annual summary reports to detailed payroll registers.

The payroll programs must be run in the proper sequence. USPS internally tracks which programs have been run, and will issue error messages and will not allow the user to run the programs out of sequence.

For contract employees there are no required entries for payroll processing. INICAL, the Initialize Payroll Run program, is used to initialize the payroll run for all active status employee records for the pay groups and the pay dates specified. The INICAL program generates reports and displays initial processing totals that can be used to confirm the payroll run.

For other employees, time sheet data must be manually input into the system through UPDCAL_CUR, (Current Payroll Data Maintenance program), UPDCAL_FUT (Future Payroll Data Maintenance program), or a time sheet system may be used to feed USPS. Authorization for time sheet transactions is a manual control performed by user organization management.

USPS provides for online editing of data input. Dates, employee identification numbers (ID) and other USAS codes are edited for validity and completion. In addition, a pay report can be generated and displayed on the user's terminal to verify data entered. Any identified errors can be corrected at this point through UPDCAL_CUR.

Alternatively, users can utilize PAYSUM, the Pay Amount Summary Report program, to produce a Pay Amount Summary Report that summarizes the pay type, number of units and the pay amount by job for each active employee in the pay period. Grand totals by pay type are displayed at the bottom of the report. The totals reported for PAYSUM should balance to the INICAL totals plus any exceptions entered for the payroll. PAYSUM can be run after UPDCAL_CUR and before the CHKUPD, Check Update program. A balancing calculation can be verified by management at this point in the payroll process.

After this initial balancing, the CALCPAY, Calculation of Employee's Earnings, Deductions and Accounts program, is run. CALCPAY is the part of the payroll run sequence that handles the major portion of the calculation processing including deductions, net pay, tax calculations and totaling employee multiple contract amounts. An error report will automatically be printed if any errors were encountered during the run of CALCPAY. Pay, budget and deduction reports can be generated from CALCPAY and used by management to verify the accuracy of data.

The CHKUPD program, which is run after the check printing program, CHKPRT, updates the job, pay account and deduction amount data, generates reports for confirmation and the treasurer's signature, and creates a posting file to be used by a USAS program to actually perform the posting. The leave balances will be updated by CHKUPD if the USPSDAT/USPCON "deferred post" flag is answered "Y". This signifies a district is using the deferred posting method of absence posting. If this flag is answered "N" the employees' balances will be updated immediately when an absence entry is posted in USPSCN/ATDSCN. AUTOPOST allows for the delay of posting of payroll data. It also performs some validation checks of the data and will create an error report and reject the batch from posting if errors are identified.

Beginning and ending pay dates are entered in the INICAL initialization program. A warning message will be received if the user has not closed the quarter for SERS, STRS and ODJFS processing, however, the user can continue. These warnings will occur if a previous period is not closed, the current period is closed, or a future period is closed. However, the CHKUPD program, which actually updates the files and creates a posting file for the USAS accounting system, will not allow the update to occur until the closing is finished.

During the initial set up of a user organization on USPS, start up programs must be run prior to actually entering data about the user organization employees on the system. The following programs must run:

- USPSDAT/USPCON, User Organization Data Information - maintains user organization data, including, identification numbers such as federal and state employer ID numbers, period closing dates, benefit account flags, check information and payroll processing information.

- USPSDAT/PGRPED, Configuration and Pay Groups - used to establish payroll groups to enable mass changes by groups.
- USPSDAT/DEDNAM, Deduction Names - maintains deduction company information. Users can print a report to verify deduction company data.
- USPSDAT/BLDMNT, Building – creates a file of building codes.
- USPSDAT/DEPMNT, Departments – creates a file of department codes.

In addition, there are a variety of file maintenance program modules which are used to add modify or delete employee data. These include:

- BIOSCN, Biographical Data Maintenance - used for employee biographical information.
- DEMSCN, Demographical Data Maintenance - used for employee demographic data.
- BENSCN, Benefit Data Maintenance - used to enter leave data.
- JOBSCN, Job/Contract Data Maintenance - used for employee job/contract data.
- POSSCN, Position Data Maintenance - used for employee job/position data.
- PAYSCN, Pay Account Data Maintenance - used for payroll account data.
- DEDSCN, Deduction Data Maintenance - used for employee deduction record data.

Users can use EMPMST, Employee Master Listing program, to print employee data and verify the completeness and accuracy of data entered through the file maintenance program modules. Duplicate employee records are prevented through online edit checks.

The CHKLEV, Current Leave Usage and Balances, report tracks employees' current leave usage and balances.

The AUDRPT, USPS Change Tracking Report program, tracks the old values and new values entered in various USPS programs. It reports who made the change, the date and time, the record changed, and the old and new values. Two types of audit reports are available: Demand and Official. The demand report can be run at any time and shows the change activity that occurred on the file. The program provides for a variety of sort options. The official report contains all of the changes made to the USPS files since the previous official report was run. Each run of the report is sequentially numbered. Users are instructed to keep every copy of the official report for auditor review. Treasurers are instructed to review and sign the official report.

OpenVMS identifiers and user passwords prevent unauthorized access to USPS and thus payroll data. Standard USPS identifiers allow the ITC to grant a standard "USPS" or a "Personnel" identifier. The "USPS" identifier allows the user access to all fields in the system pertaining to the contract information, while the "Personnel" identifier would only allow the user to see fields that need to be maintained for reporting information for

EMIS and would exclude contract and other payroll information. If desired by the user organization, the ITC can customize identifiers to their needs. The OECN_PPS identifier for personnel users allows access to DEMSCN, and POSSCN and portions of BENSCN and ATDSCN. The payroll identifier, OECN_USPS, allows access to BIOSCN, JOBSCN, BENSCN, ATDSCN, PAYSCN, and DEDSCN. Although the personnel data more appropriately belongs to the superintendent and not the treasurer, users such as a treasurer may have both identifiers.

School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS), Release 2.1

The SAAS/EIS is a fixed asset accounting system for user organizations. The primary purpose of the system is to provide the necessary information for reporting in accordance with GAAP. The system also provides enhanced management reporting and values for insurance purposes.

User interaction with the system is simple and straightforward, requiring only basic familiarity with the terminal device connecting the user to the main computer. Data entries include such items as USAS invoice data, local codes, capitalization criteria, transaction records, and dates.

The system checks all entries for accuracy, processes the correct data and produces various reports that can help the user to manage the fixed asset records of the user organization.

The SAAS/EIS system is highly interactive. As user organizations enter data, the system checks the entered data through edit checks for validity. Codes that have incorrect data types or length are considered invalid, and are rejected by the system. The system has set predefined value types to minimize the possibility of an invalid code.

User organizations are responsible for preventing/detecting unauthorized changes to their inventory files. The EIS Audit Report program module can be used to track changes made to the inventory files. Either a “demand” audit report or an “official” audit report can be generated. The demand audit report can be run for a range of dates and has various sort and selection options. The official audit report is sequentially numbered and contains all additions, deletions, and modifications made since the previous official report. This report is used as the audit trail for annual audits and should be run at convenient times (i.e., monthly, quarterly, semiannually), depending on the volume of activity on the system.

User organizations can run various program reports to verify the completeness of data input:

- Schedule of Fixed Assets by Source – schedules of fixed assets used for GAAP reporting.
- Schedule of Fixed Assets by Function and Class – creates a schedule of fixed assets by function and class, by class, or a summary by function and class.
- Leased Asset Listing – listing of all leased items with the acquisition method “leased” or with a “lease vendor number.”
- Asset Listing by Grant/Source – generates a report listing acquisition transactions by source account code and/or by a grant identifier ID.
- Location Worksheet – generates a listing of inventory items by their location category and number, and is designed to aid in completing an inventory.
- Inventory Master Listing – master listing of all data relative to an inventory item.
- Brief Asset Listing – brief listing of all assets on the inventory file or a subset of these.
- Audit Report – generates a report to track changes made to the EIS files.
- Detailed Breakdown of EIS101 Report – detailed listing of fixed assets by source.

The SAAS/EIS software also interfaces with the USAS system to extract items from the USAS invoice file and add them to an EIS pending file. This interface reduces the work in obtaining the purchase order information needed on the item and acquisition transaction records. Flags may be set within the USAS program USASDAT. This flag allows transactions from the USASWeb and APE programs to be posted directly to the EIS pending file.

User organizations can also use the SAAS/EIS program EISPND to update fixed asset files. This program adds PO information for all items that contain an account object code of 600-699 or 700-799 and meet a certain threshold amount, to the pending file. This program will also show the number of records added and can be printed through the EISRPT program.

The SAAS/EIS has system level edit checks to verify entered data is acceptable. The system uses codes to verify valid data types are entered. For example, fund codes must be a four-character code consisting of letters or numbers. If the user does not enter exactly four characters, the system will respond with an error message. The ODE predefines some of these codes, such as the first two numbers in the asset class code. However, others are defined locally by the user organization. These include the following:

- Asset class codes (second two characters only).
- Item category codes.
- Condition codes.
- Configuration data.
- Disposition codes.
- Fund codes.
- Function/activity codes.
- Location codes.
- Organizational/department unit codes.

Each user organization can periodically print an inventory report to verify for accuracy. A commonly used report is the Location Worksheet, generated by the Report Program, EIS302. This report generates a listing of fixed assets by their location, category and tag number. This is a one-line per fixed asset worksheet designed to aid in completing an inventory and may be sorted in many ways to facilitate asset tracking. These can be used prior to or just after a physical inventory to check the accuracy of an appraisal company.

Location Worksheets may be given to the user organization staff member assigned to a particular area or room. Such persons update the inventory list for their specific work area. This approach allows user organizations to complete more accurate and cost-effective inventory updates.

Edit checks within the SAAS/EIS system, such as valid fund types, function codes or departmental codes, help to ensure databases are correctly appended. Data codes, set within the edit checks, prevent improper records from being entered into the SAAS/EIS system. Data codes for inventory listings are changed only by authorized user organization personnel.

User organizations are normally responsible for ensuring data is complete and accurate. The ITCs will provide assistance if the user organization is attempting a first year GAAP conversion for the SAAS/EIS system. Year end procedures are provided to user organizations to help ensure all databases have been backed up prior to closing the year through the EISCLS program.

The SAAS/EIS system has tools for closing the fiscal year and ensuring a smooth transition into subsequent years. Several year-end reports are suggested to be run before any major year-end changes are completed. Suggested reports include, Inventory Master Listing Report, Brief Asset Listing Report, Insurance Value Report, and EIS Audit Report. The user organizations may use these reports as an audit trail for documenting depreciation information; maintaining current replacement cost and/or insurable value of the inventory item records; and providing an official audit report of the SAAS/EIS system. Procedures to close fiscal years for SAAS/EIS are the same for GAAP and non-GAAP user organizations. Life-to-date depreciation is calculated automatically and updated by the EIS closing procedure.

Access to SAAS/EIS packages is provided by granting the appropriate OpenVMS identifiers to authorized users. When a user logs on to the application, each SAAS/EIS program will look up the OpenVMS identifier held by the current process. If the process holds the required identifier, then the execution proceeds normally. If the current process' rights list does not contain the required identifier, an error message is displayed and the program aborts immediately. The SAAS/EIS standard identifier is OECN_EIS. This, when granted to a user, allows standard read/write access to the package. In addition, the OECN menu processor utility allows the users to see only the items they are authorized to execute.

Education Management Information System (EMIS), Release 2.6

The overall purposes of the EMIS are to provide better accountability for tax dollars, to provide better policy understanding of school programs and accomplishments, and to help improve the local education system. The most significant information from this data is the enrollment data that ODE uses to calculate the Average Daily Membership (ADM) for each user organization. The ADM number is used to determine the amount of state funding each user organization will receive.

The majority of the information required for the EMIS databases can be found in the user organization’s already existing accounting, payroll, personnel and student information files. These files are created and maintained by the application software already in use by the user organization, whether it is state supported or third-party vendor software.

EMIS collects and reports information by performing data extractions, validations, corrections and aggregations. User organizations extract the information from their financial, payroll, personnel, and student files and transfer it to their respective ITC in accordance with the specifications and time lines established by the ODE. These time lines are referred to as EMIS processing cycles. During each EMIS processing cycle, data is extracted, transferred and loaded. User organizations are then notified of reports available for their review. It is the user organization’s responsibility to correct the errors and help ensure the validity of the information that is sent to the ODE.

The ITC will coordinate the collection, submission and aggregation of the data for all the user organizations who belong to the ITC. Each ITC will also play a consulting role to assist each of their user organizations in preparing the data for submission to the ODE. Each ITC will determine procedures for their districts submission of data to ODE. Each user organization is required to e-mail the ITC, before the processing deadline dated, in order for the ITC to submit their data to ODE. Not all user organizations submit data for each reporting period. Organizations using student information systems such as DASL and ESIS process their own data, and only require ITC intervention to submit their data. The ODE’s processing schedule and deadlines are available to all user organizations via the ODE website. In most cases, a request must come from the districts’ EMIS Coordinator or other approved district staff. NWOCA’s procedure is to copy the e-mail into the California Associates (CA) Unicenter application to create a help desk ticket. Alternatively, the user organizations may enter the request directly into the CA Unicenter application to request submission. After the user organizations approve their data for submission, the ITC will forward the data to ODE in the format required by the EMIS.

ODE processes each user organization's submission and returns additional reports to the district through the ITC that submitted the data. The district must review the reports and restart the process as needed.

A program called EMSRX is responsible for loading user organization data files and importing them into the EMIS system located at the ITC. The EMIS program EMSRX searches for duplicate keys and compares the batch file record length to the record length of the detail records in the file. Duplicate records cannot be created for a student ID number that is already on the EMIS files.

Edit checks within the software create assurance the file contains the proper number of records and accurate file layout. The primary means by which this is completed is with a verification of record counts. The file header and trailer contain a count and the process verifies the records read against this count.

Each file transmitted to an ITC must contain a header and a trailer record. The record length of the header and trailer records must equal the record length of the detail records in the file. The purpose of the record is to assist the designated ITC in identifying the reporting user organization and ensuring the processing is complete and valid. The record contains two checksum fields whose values are compared to ensure the entire file was extracted.

If all the records for a given batch file are properly extracted, the totals calculated by the EMSRX will equal the totals found in the fields of the trailer record listed above. If not, an error will appear in the EMSRX4 report.

Since the information which is input into the EMIS system comes from a variety of different application software packages, controls over what constitutes accurate input are flexible. In both the VMS interface and the EMIS Web application, online edit checks are used to verify the accuracy of entered data and warning messages are displayed when erroneous data is entered, however, the records will process with warnings. Various reports are generated by the application to identify incorrect information so that timely corrections can be made to data. The EMSRX program checks only a few key fields while extracting the information from the user organization's application files and loading into the EMIS database

The ITC or user organizations can run a program called EMSVLD against their data directly after loading into the EMIS database. This program validates the fields against the EMIS options file provide by the ODE. The accuracy of the values in each field is checked. Neither user organizations nor ITCs should run EMSVLD after the data is compiled for submissions. EMSVLD does not generate accurate validations on compiled data.

The aggregation programs (commonly called "The Aggs") are used by the ITCs and user organizations to compile the data loaded by EMSRX and its sub-programs. The data compile steps consist of reading the detail records loaded and creating new submission records and files that are to be sent to the ODE. Specifications for the format of the files are dictated by the ODE. These specifications are sent to the SSDT by the ODE. After the data is compiled, additional checking is completed for data integrity. Depending on the reporting cycle in process, the checking is different. The aggregation checks are defined by the ODE in documents provided by the SSDT. Various reports are generated by the aggregation routines. These reports are to be reviewed by user organization staff. The AGG5.TXT is one of the more important reports created. It lists fatal errors. The fatal errors prevent records from being included in submissions to ODE, in nearly all occurrences. The failure of records being sent to the ODE can be detrimental to the district.

EMSRDET is used in some of the EMIS reporting cycles for creating submission files to the ODE. The records being processed as a part of

EMSRDET are detail records. The detail loaded into EMIS is sent to ODE with no additional data compile as would occur in the aggregations. The records are checked for fatal errors and can be excluded in the same manner as the compiled records can be.
EMIS identifiers are assigned to limit access to EMIS menu screens to help prevent unauthorized changes to data. Each identifier has uniquely defined access levels. Identifier may be limited further by using suffixes such as “RO” for read-only access, or given additional access privileges with the “GM” for group-manager access. In addition, an EAUDRPT report can be used to detect unauthorized additions, deletions, and modifications to data. The report lists when changes are made, who made the change, and the original and modified values.

The ODE handles the distribution of the Information Retrieval Number (IRN) file. The ODE has assigned an IRN to each user organization and every school building within that user organization for the entire state. The EMIS program calculates record counts and checksums of IRNs to verify the completeness of the files being loaded.

The EMIS Options file establishes the correct values or ranges of values for the given fields within the EMIS databases. ODE makes the necessary changes to the Options file. SSDT personnel only modify the EMIS standing data contained in the Options file when an authorized options file is received from ODE. These changes are transmitted to the SSDT along with an e-mail describing the changes made, and transferred to a protected directory on the Ohio Education Computer Network (OECN). Upon receipt of the updated Options file, the SSDT prepares a JIRA issue to document the conversion and installation of the new Options file. An OpenVMS utility allows the SSDT to compare the updated file with the current file and then list the differences between the two. The SSDT examines the resulting report to determine whether the differences match the changes described in the EMIS Guide or in the e-mail notification. The SSDT then distributes the changes to the other ITCs.

The SSDT received other files maintained by the ODE. These are included in the distribution with the EMIS software. These other files include the count week file for both October and February, valid program codes, valid subject codes, valid assignment areas, test combination file, OEDS (Ohio Education Directory System) prefix files, general info for Voc Ed, ITC-IRN listing, valid credential IDs and the RFO-IRN (Reading First Ohio) file. The count week files are updated and distributed as needed when districts have been approved for waivers to the standard count week dates. The other files are generally updates once per reporting cycle and released accordingly.

Various reports provide information on the EMIS databases and can be examined by the user organization to confirm their content and identify incorrect information so that timely corrections can be made to the data.

- Detail Reports: Reports on detailed information within the database.
- Validation Report: Lists errors/warnings found in the database. Information in this report can be sorted in multiple ways.
- Look-Alike Reports: These reports look like the reports the ODE will generate from the user organization’s databases. The users examine these reports to determine if their data appears valid. Note: These look-a-like report formats are no longer updated, and are not considered official reports. Although they are not as useful to the districts as they once were, some continue to review these reports.
- Aggregation Reports: These reports aggregate the information in the EMIS databases and can show valid and invalid data found in the database.

Due to the continuous updating for EMIS, the information stored in the EMIS databases can always be modified if needed. Although, it is best practice for districts to update their source systems and reload their EMIS data, doing so is not always practical.

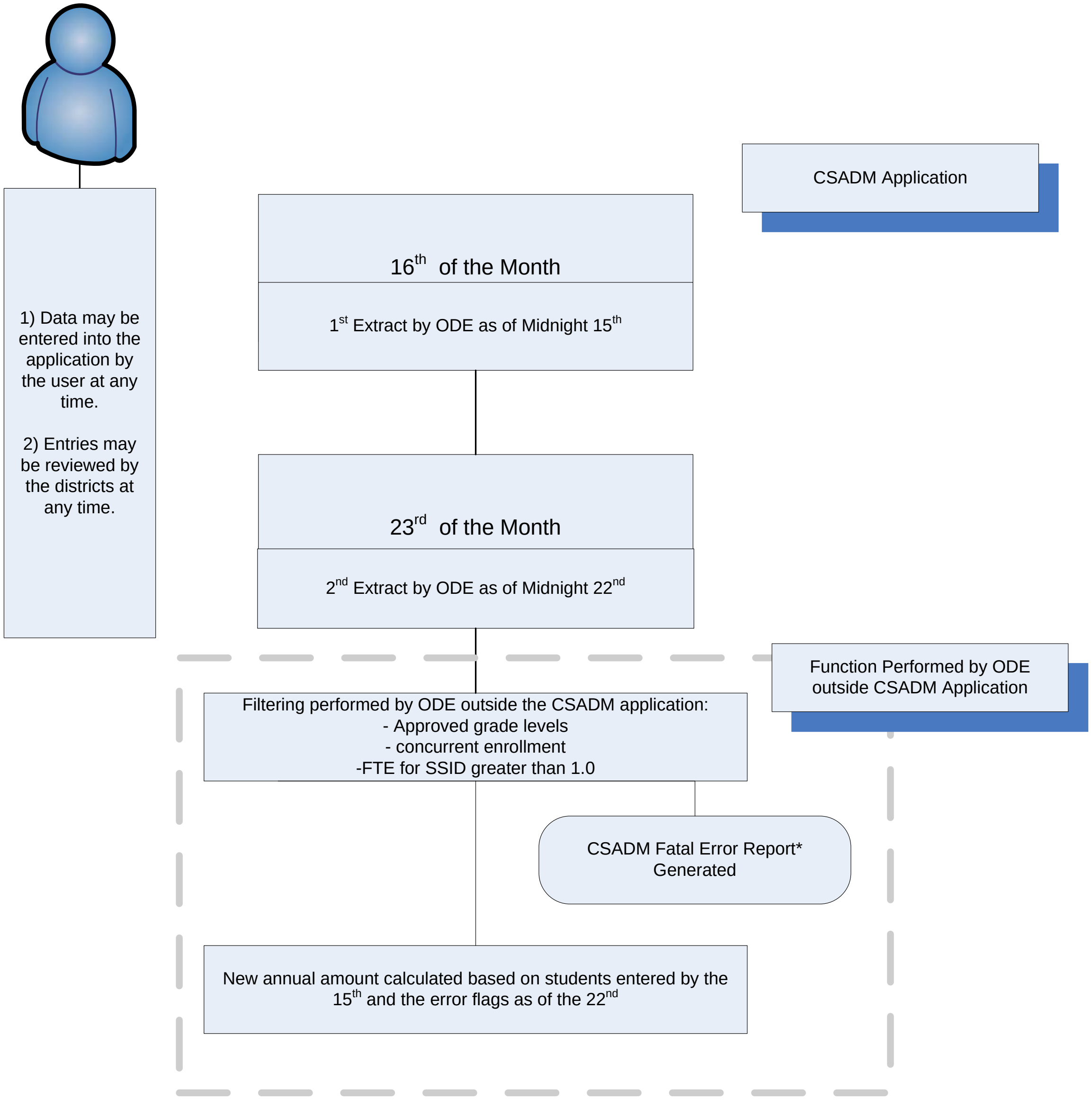
Validation reports are created when programs are run against the EMIS databases. Errors are detected and reported.

The ITC is responsible for ensuring that all EMIS data received and processed is secure and the data can only be accessed by the user organization’s designated employees. This is done by using the security features offered by the OpenVMS operating system.

Community School Average Daily Membership System (CSADM) Release 3.0-1

The CSADM application is a subsystem of the Education Management Information System (EMIS) which is used to drive funding for community schools. This web application is used by community schools and traditional public schools to maintain data used to flow funds to community schools. Community school personnel enter data in the CSADM system and traditional public school personnel review, and then verify or challenge the accuracy and validity of the data. The term, “resident school district” is used to refer to the traditional public school district where the student lives. The State Software Development Team (SSDT) performs limited duplicate checking using the Statewide Student Identifier System (SSID) assigned identification number. Additionally, the application performs various logic checks.

Users may enter data into the application at any time. The following illustration provides an overview of the processing of data maintained by the CSADM:


1) Data may be entered into the application by the user at any time.
2) Entries may be reviewed by the districts at any time.
CSADM Application
16th of the Month
1st Extract by ODE as of Midnight 15th
23rd of the Month
2nd Extract by ODE as of Midnight 22nd
Function Performed by ODE outside CSADM Application
Filtering performed by ODE outside the CSADM application:
- Approved grade levels
- concurrent enrollment
-FTE for SSID greater than 1.0
CSADM Fatal Error Report* Generated
New annual amount calculated based on students entered by the 15th and the error flags as of the 22nd

*The CSADM Fatal Error Report is not generated by the CSADM application. Rather the report is generated as a result of edit checks performed on the CSADM "snapshot" outside the application.

Note: Fatal error reports are available to the users through the Information Technology Center (ITC).

Access to the CSADM application is granted through one of two methods. In the first method a "CSADM Web Based System Access Form for Community Schools" or a "CSADM Web Based System Access Form for Traditional Public Schools" is completed and submitted to the Ohio Department of Education's (ODE) Office of Community Schools or Office of School Finance, respectively. ODE personnel create the profile, but do not have the ability to enable it. The inactive account is forwarded to the SSDT to be enabled. Alternatively, the admin user requests a new account be created in the CSADM application. The SSDT receives an automatically-generated form e-mail from the application requesting the new account be enabled, and the SSDT enables the account. Access forms are retained by ODE, and the e-mail requests are maintained by the SSDT.

Access to the CSADM application is restricted through Structured Query Language (SQL) security tables. The security in the application provides for the following five roles:

- Administrative User: A user assigned this role has the ability to create/modify/enable user profiles and create/modify entity profile information and does not have access to student information.

- Area Coordinator: A user assigned this role has read-only access to student information (not names). This role was created for ODE School Finance Coordinators to assist in resolving conflicts between the resident school district and the community schools.

- ODE Exec: A user assigned this role has the ability to update any entity or student information in the state database, review student information, and generate ODE snapshots for funding. This role can create new user profiles, but does not have the ability to enable the user.

- ODE User: A user assigned this role has the ability to create/modify entities, create new or modify existing user profiles; however, does not have the ability to enable the users. This role can perform the monthly snapshot for funding.

- District/School User: If assigned to a resident school district or JVS this role has the ability to review student information to set error flags, but not to create new or modify existing student information. If assigned to a community school this role has the ability to enter/modify student information; but not the ability to perform the student review and set error flags.

Each resident school district user role is further restricted to an entity and an access level. Access levels include Read-Only, Update, and Admin.

Each resident school district and community school's financial contact is assigned the 'Admin' access level. This gives the school admin rights to perform the following operations:

- Request a new user account for any school they administer. This new user requested must be enabled by the SSDT.
- Change the access level of users who have access to the school or entity they administer (change between read-only and update access).
- Remove user access from the school or entity they administer.
- Grant access to a school they administer to an existing user account.

A validation system has been implemented to help ensure the validity of user accounts. Three times each year, an e-mail is sent to all active

CSADM users asking them to validate their account. The user can validate their account either through clicking a link provided in the e-mail, or navigating to the CSADM website and entering the code provided in the e-mail.

Each time the user logs in after the e-mail has been sent and before their account has been validated, they will receive a warning that their account must be validated within 30 days, and they are prompted to correct their contact information and resend the validation e-mail. If the validation is not performed within 30 days of the original validation e-mail, the user account will become suspended. Suspended accounts cannot log into the application.

Accounts which have been suspended will still have the option to resend the validation e-mail and validate their account; however, they will not be able to make changes to their contact information prior to sending the validation. If their contact information needs to be updated, they will need to contact ODE to have this information updated and confirmed in order to have the confirmation re-sent.

Two types of information are retained for processing in the CSADM application: entity and student information.

Entity Information

Entity information consists of the following:

- *Entity type* (Community School, Resident School District, or Vocational/Career Center) – only ODE Exec, ODE User, and Administrative User profiles have the ability to modify or enter this information.
- *Entity Name* – only ODE Exec, ODE User, and Administrative User profiles have the ability to modify or enter this information.
- *IRN* – only ODE Exec, ODE User, and Administrative User profiles have the ability to modify or enter this information.
- *County* – must be selected from a “drop-down” menu.
- *Financial Contact* – optional text field.
- *Contact E-mail* – optional text field.
- *Contact Phone* – optional text field.
- *Fax Number* – optional text field.

In addition, Community Schools are required to enter the following entity information:

- *Annual Membership Units* – drop down menu, days or hours.
- *Total Annual Membership Days/Hours* – numeric field.
- *Kindergarten Program Type* – drop down menu.
- *First Day of Class.*
- *Last Day of Class.*
- *Days in Session.*
- *Instructional Hours Per day.*

Student Information

Student Information can be broken down into demographic, enrollment, and transportation information. Prior to accepting a record for entry, the CSADM application performs various edit checks to prevent erroneous information from being retained by the application. The information retained and associated edit checks by each area are as follows:

Demographic

- *First Name* - required field <cannot be blank>.
- *Last Name* – required field <cannot be blank>.
- *Middle Name* – optional field.
- *EMIS ID* – optional field.
- *SSID* – validated outside the application (NOTE: only student with valid, unduplicated SSIDs will be funded.) *REQUIRED*
- *Grade* – option to choose from “drop-down” menu <standing data>.
- *Grade Level Next Year* – option to choose from “drop-down” menu <standing data>.
- *Birth Date* – required field - must be logical (mm/dd/yyyy). Age is calculated from this date and must meet the following requirements:
    - if in kindergarten, be at least 5 years old on enrollment or must turn 5 by January 1st of the current school year.
    - be no older than 21 on the first day of school and may turn 22 anytime during the year.
    - cannot be 22 on or before the first day of school.
- *Gender* – required field – must be selected from a “drop-down” menu.
- *Ethnicity* – required field – must be selected from a “drop-down” menu.
- *Limited English Proficient (LEP)* – must be selected from a “drop-down” menu.
- *Disability Condition* – must be selected from a “drop-down” menu.
- *Special Ed Program* – must be selected from a “drop-down” menu.
- *Individualized Education Program (IEP) Date* – must be logical (mm/dd/yyyy).
- *Economic Disadvantaged* – checkbox.
- *Attend Last Oct* – must be selected from a “drop-down” menu <standing data>

Enrollment

- *From Effective Date* – must be logical (mm/dd/yyyy).
- *To Effective Date* – must be logical (mm/dd/yyyy).
- *Withdrawal Reason* – must be selected from a “drop-down” menu.
- *Guardian’s Name* – required field.
- *Student Address* – required field.
- *Total Days* – may not exceed the annual membership units entered in the Entity Profile.
- *Notes* – free form field (optional).

Transportation

- *Transported* – checkbox.
- *Distance* – must be selected from a “drop-down” menu <standing data>.
- *Days Transported* – series of 5 checkboxes.
- *Notes* – optional from form field.

Transportation information was added as an option during the audit period. Some community schools provide transportation for their students. This information is logged in the transportation screens in CSADM. This information does not affect the average daily membership calculations or community school funding.

When adding student demographic information certain fields are required before processing can occur. If the required fields are not populated an error message is returned and the student information is not updated. Certain fields within CSADM affect funding levels, and changes to these fields are tracked within the system. The ‘Added by’ and ‘Modified by’ function records who and when changes are made to specific student and enrollment information which can be used to assist in detecting unauthorized additions and modifications to student data. A change summary is available that documents the field changed, the old value, and the new value. The date and user making the change are stored in the audit table within the CSADM database.

Several fields are drop down fields and can only be populated with pre-defined/standing data. The only personnel with access to the SQL tables housing the “drop-down” information are SSDT personnel with direct access to the SQL Server. The data housed in the “drop-down” menus cannot be modified through the application.

A student demographic entry or enrollment entry cannot be deleted through the CSADM application, regardless of the user role assigned. To disable an entry, users update the effective to and from dates to be equal (e.g., “from” date = 1/13/1999 and “to” date = 1/13/1999), indicating removed enrollment information. This prevents users from deleting any previously entered enrollment information. Any deletions must occur directly through the SQL Database.

When a student residency record is created, the user must enter the number of units (hours or days) the student is living in that resident school district and attending the community school. The CSADM system automatically calculates the available number of units based on the from date entered, and either the to date or end of the school year (whichever is earlier). In order to prevent excessive units from being entered, the system will generate an error if the units entered exceed the maximum available units, and will not allow the record to be saved until the error is corrected. When a residency record is inactivated (i.e. from and to date are the same date), the total units are automatically reduced to zero.

ODE and Admin users have the ability to disable the year status. Changes cannot be made in a year that has been disabled in the CSADM ‘Year Maintenance’ screen.

The resident school district is the district a student lives in and would normally attend. The resident school district is responsible for reviewing the information in the CSADM for students assigned to their district to confirm the information is correct. The CSADM system has an edit check for preventing duplicate resident school districts with an overlapping or open date range in the enrollment period for the same student. Resident school district users are required to review student information entered by the community schools and set error flags for incorrect information. For example, if the student’s date of birth or address are incorrect, or if the student does not actually reside in the resident school district entered into

CSADM, the resident school district can challenge the information by setting an error flag so the community school can resolve the identified errors. Additionally, a flag can be set if the resident school district determines the student is attending the resident school district, and not the community school. The resident school district must provide evidence to support the challenge of information.

Beginning in FY08, the Auto Review Process was implemented. This process creates warning messages in the student enrollment records if a resident school district does not review the records in a timely manner.

According to the CSADM Manual, resident school districts are now required to review student records within 75 days of entry by the community school, or the student record becomes restricted. During these 75 days, warnings are provided to districts as notification of the upcoming review deadline, as follows:

- New records entered in the system between 8/15 and 10/1, or records from FY07 that were not reviewed by the district, will be noted with a “Review Caution” status if the resident school district does not review the records within 30 days.

- The “Review Caution” status will be changed to “Review Warning” 15 days after the initial warning; therefore, records not reviewed within 45 calendar days after the resident district is identified will be noted with a “Review Warning” status.
    - Student records that are in “Review Caution” or “Review Warning” status can still be reviewed by the resident school district and error flags may be set.

- The “Review Warning” status will be changed to “Review Restricted” 30 days after the “Review Warning” status is displayed; therefore, any record not reviewed within 75 calendar days after the resident district is identified will be noted with a “Review Restricted” status. This status prevents the district from placing any flags on the student record. Resident school districts must contact their Area Coordinator at ODE and provide adequate documentation in order to have a flag added once a record has become “Review Restricted.”

- The only users who can add a flag once the record is “Review Restricted” are the ODE Exec users. When the flag is added, the status changes to “reviewed with x errors,” effectively removing the restriction. The community school must address the error, putting it back to a modified status to be reviewed by the RD again.

Any time a student record is modified by the community school, the review status is reset. If a district flags a record and the community school modifies the record in order to remove the flag, the district has to review the record within the same guidelines. If the district does not review the record within 75 days of the modification, the record will also go to restricted status and the student will be funded at the community school, even though the student record is flagged.

The CSADM application performs edit checks to ensure all required data fields have been entered before processing a transaction. In addition, edit checks are in place to prevent duplicate student enrollment by resident school districts. The CSADM program performs edit checking to ensure duplicates are not permitted, data is in the correct format, and logical. All students assigned to a community school must have a unique SSID. The CSADM application does not allow entering a duplicate SSID at the same community school. The SSID for a student can be assigned to multiple resident district schools during one year; however, the date ranges for the schools cannot overlap for an SSID. Once data is extracted, ODE has procedures in place to detect and correct duplicate SSID’s in multiple community schools with over lapping date ranges.

ODE contracts with IBM to maintain a third-party file of SSID information. Users at the community schools and resident school districts enter students into the SSID system, and a unique SSID is automatically generated. This file is matched to CSADM data in order to validate the SSIDs being entered into CSADM.

NWOCA offers a web service to manually validate SSIDs before they are entered into CSADM. As SSIDs are saved within the CSADM application, they are compared to a file from IBM that contains valid SSIDs. If the SSID is not contained within the IBM file, the record cannot be saved. If an SSID is removed from the IBM file at any time, the SSID status shows as “INVALID” in the CSADM record and the Community School Report the next time the status is displayed.

Standing data in the CSADM application consists of information available through drop down menus. This information is only able to be modified through direct access to the SQL Database residing on the NWNET server. Only select SSDT personnel have access to the SQL Database. Access to the database is controlled through Windows authentication.

Community school users have the ability to modify student records in the application at any time. When a community school makes a change to a student record after it has been reviewed by the resident school district, the status of the record is changed to “Modified.” The status of the record will be “modified – errors” or “modified – no errors”.

The community school Full Time Equivalency (FTE) is automatically calculated by the system based on the total units (number of hours or days) assigned to the community school. The FTE is automatically calculated each time updates to student hours or days are made, and the recalculated FTE is extracted in the ODE snapshot.

The CSADM provides ODE the ability to perform a snapshot of all community schools’ data. The snapshot captures all student information for use in calculating the monthly funding payments. When a snapshot is performed, the ODE user has the option of performing a rebuild, which includes all modifications and additions since the last time the information was compiled for the snapshot. If the rebuild option is not selected, the snapshot information will include the same information as the previous snapshot, even if modifications or additions have been made. The snapshots are performed by ODE on the 16th and 23rd of each month.

The SSDT has retained/backed up final monthly builds since the inception of the CSADM application.

SECTION III - INFORMATION PROVIDED BY THE SERVICE AUDITOR

This section is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the NWOCA's internal control that may be relevant to user organization's internal control, and reduce the assessed level of control risk below the maximum for certain financial statement assertions.

The broad objectives of data processing controls should be achieved by a combination of the procedures that are employed in various segments of the transaction processing system, for example procedures performed at the NWOCA and procedures performed at user organizations that utilize the NWOCA.

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

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Development and Implementation of New Applications and Systems

The SSDT did not develop or implement new audit significant applications during the audit period. Control objectives for program maintenance are described and tested in the next section.

Development and Implementation of New Applications and Systems - *Control Objective:* **Project Management** – Project management should ensure appropriate control over the design and implementation of new applications or systems.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The Software Advisory Committee (SAC) meets quarterly to monitor current software development projects and discuss proposed projects.	Inspected the quarterly meeting minutes of the SAC.	No relevant exceptions noted
The NWOCA has an agreement with the Ohio Department of Education (ODE), Information Technology Office (ITO) to perform services as the State Software Development Team (SSDT) for the benefit of Ohio user organizations.	Inspected the Memorandum of Agreement between the NWOCA and the ODE.	The agreement is current.
A programmer's handbook and supplement detail steps to take in the development of new applications or systems.	Inspected the handbook for documented procedures.	No exceptions noted.

<table>
<tr><td colspan="3">**Development and Implementation of New Applications and Systems** - *Control Objective:*
Training and Documentation - Users and IT staff should receive appropriate training when their responsibilities are impacted by application or system development and implementation. In addition, technical documentation should be provided to support ongoing operations, problem resolution and future application or system maintenance.</td><td>**Control Objective Has Been Met**</td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>The SSDT provides training to all users for the web application releases through webcasts which are available online.</td><td>Inspected online training documents and presentations for the 2007-2008 releases</td><td colspan="2">Online training is available.</td></tr>
</table>

Changes to Existing Applications or Systems

<table>
<tr><td colspan="3">**Changes to Existing Applications or Systems** - *Control Objective:*
Change Requests - Requests for application program changes or system upgrades should be appropriately considered and processed.</td><td>**Control Objective Has Been Met**</td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>User requests for program changes are submitted through the Site Scape SSDT Forum for review by the SSDT or ODE staff.
If the request is accepted, it is assigned the _PENDING qualifier.
If it is rejected, it is assigned the _REJECTED qualifier and an e-mail describing why the request was rejected is sent to the person making the request.</td><td>Independently confirmed change request procedures with the SSDT programming services director, and the SSDT systems analysts.
Inspected the pending and rejected forum entries (SPR_Pending and SPR_Reject listings) for each of the audit significant applications.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

Changes to Existing Applications or 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:
The automated JIRA Issue Tracking System is used to track the progress of all application work orders.	Inspected a listing of all changes during the audit period (5/26/07 – 5/23/08) from the CMS library. Haphazardly selected 100 changes from the library and traced the change to the work order. Inspected JIRA for completion of key fields indicating the JIRA issues were used to track the progress and approval of each step.	No relevant exceptions noted.
The NWOCA participates in the CSLG/ESL program, which provides operating system support, upgrades, and related documentation.	Inspected the following items: • CSLG/ESL agreements between the ITCs and the NBEC. • Operating system software support invoice and payment. • Online system software documentation.	All agreements and payments were current. In addition, the NWOCA maintains the agreements for all ITCs on behalf of the NBEC.
The NWOCA has an agreement with the Ohio Department of Education (ODE), Information Technology Office (ITO) to perform services as the State Software Development Team (SSDT) for the benefit of Ohio user organizations. As part of the agreement, the SSDT provides updates to the state software that includes design, development, testing, implementation and support.	Inspected the Memorandum of Agreement between NWOCA and ODE.	The agreement is current.

Changes to Existing Applications or Systems - *Control Objective:* **Testing of Program Changes or System Upgrades -** Program changes and hardware system upgrades should be tested to ensure they achieve the business' requirements and do not negatively impact existing processing.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Testing is performed to help ensure that the updated applications function properly. Programmers approve the JIRA issues electronically to indicate completion of testing. When “buddy testing is performed, a second programmer or analyst also approves the JIRA issue.	Using the JIRA issues selected for previous testing, inspected them to confirm testing was performed.	No exceptions notes.
COBOL Applications: The CMS library monitors simultaneous reservations of the same source code to help prevent concurrent changes. Concurrent reservations are flagged as unusual transactions and included in the CMS reports for periodic review.	Inquired with the SSDT programming services director, about simultaneous reservation monitoring by the CMS library. Inspected the programmer's manual for documentation of the warning message which occurs when a file is reserved by another person. Inspected the CMS history log from 5/26/07 to 5/23/08 for concurrent reservations of the same file with changes made by programmers. Also, inspected the Weekly CMS Summary and Status report.	No exceptions noted.
Beta-site testing is performed by NWOCA's user organizations prior to the release of application updates.	Inquired with the SSDT programming services director about NWOCA user organization involvement in Beta-site testing.	No exceptions noted.
Web-Enabled – JAVA Applications: Testing is performed on the JAVA programs by a testing utility called JUNIT and the results of the tests are recorded reporting Cruisecontrol.	Inspected Cruisecontrol to confirm JUNIT testing is performed.	No exceptions noted.

<table>
<tr><td colspan="2"><b>Changes to Existing Applications or Systems</b> - <i>Control Objective:</i>
<b>Testing of Program Changes or System Upgrades -</b> Program changes and hardware system upgrades should be tested to ensure they achieve the business’ requirements and do not negatively impact existing processing.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>JAVA Applications
The CVS library monitors simultaneous reservations of the same source code to help prevent concurrent changes.</td><td>Inquired with the Programming Services Director about simultaneous reservation monitoring by the CVS library to confirm warnings are given to the programmers if they attempt to replace a program already modified by another programmer.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Changes to Existing Applications or Systems</b> - <i>Control Objective:</i>
<b>Transfer into the Live Environment</b> - The transfer of programs or system upgrades into the live environment should be appropriately controlled.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>A SSDT systems analyst or the SSDT programming services director reviews program changes and testing results prior to the release into the production environment.</td><td>Inspected the JIRA documentation for each application (USAS, USASWEB, USPS, USPSWEB, EMIS, EMISWEB, CSADM, and WEBGAAP) to confirm that all issues are approved by the systems analyst or programming services director before they are released into production.</td><td>28 of 46 USPS changes did not have final approval before the application was released.
No other exceptions noted.</td></tr>
<tr><td><b>COBOL Applications:</b> The CMS Summary and Status reports are reviewed weekly by a SSDT systems analyst.</td><td>Inspected the Weekly CMS Summary and Status reports.
Discussed the reports with the, SSDT programming services director and the SSDT systems analysts to confirm the code is monitored for possible unauthorized changes.</td><td>No exceptions noted.</td></tr>
</table>

Changes to Existing Applications or Systems - *Control Objective:* **Transfer into the Live Environment** - The transfer of programs or system upgrades into the live environment should be appropriately controlled.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Access to the CMS Library is restricted to SSDT staff.	Inspected the CMS Library of Directories and the SSDT Source Security ID listing for USAS, USPS, SAAS/EIS, and EMIS. Confirmed with the SSDT programming services director that only SSDT user organizations are listed on the SSDT Source Security ID listing.	Eight accounts had access to the CMS Library that was not required for the user's job responsibilities.
Web-Enabled – JAVA Applications: The SSDT staff maintains a concurrent versioning system (CVS) log for any transfers into the live environment. The log is sorted by date, programmer, section of code changed, and description of change.	Inspected the CVS logs for the following applications: • USAS Objects. • USAS Webapp. • EMIS Objects. • EMIS Webapp. • USPS Objects. • USPS Webapp. • CSADM. • WEBGAAP.	No exceptions noted.
Access the CVS library is restricted to SSDT staff.	Inspected the CVS user list and confirmed accounts with the programming services director.	No exceptions noted.

<table>
<tr><td colspan="2"><b>Changes to Existing Applications or Systems</b> - <i>Control Objective:</i>
<b>Documentation and Training -</b> Technical documentation should be updated to reflect program changes and system upgrades. When changes to applications and system upgrades affect user procedures, documentation should be updated accordingly. Likewise, users and IT staff should receive appropriate training when their responsibilities are impacted by application changes or system upgrades.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Program documentation is updated or created when application changes are made.</td><td>Inspected the JIRA issues selected for previous testing to confirm documentation was created and/or updated when changes were made to applications.</td><td>No exceptions noted.</td></tr>
<tr><td>Release Notes are provided to the ITC's and user organizations.</td><td>Inspected the release notes for the most current release for USAS, USASWEB, USPS, USPSWEB, EMIS, EMISWEB, SAAS, and CSADM.</td><td>No exceptions noted.</td></tr>
<tr><td>The SSDT provides training to users for supported software through web casts, which are available online.</td><td>Inspected online training documents and presentations.</td><td>Online training is available.</td></tr>
<tr><td>The SSDT provides manuals for users on the SSDT web site. User Guides, reference manuals and system manager manuals are available.</td><td>Inspected online manuals.</td><td>Online manuals are available.</td></tr>
</table>

IT Security

IT Security - Control Objective: **Security Management** - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The NWOCA has established a data system security policy that outlines user responsibilities regarding computer security and access. The policy is maintained on NWOCA's website and is accessible by the user organizations.	Inspected the security policy on the NWOCA website. Inspected the data system security policy to confirm user responsibilities are documented.	No exceptions noted.
Administrators for each user organization are required to sign an acknowledgement, signifying acceptance of the NWOCA Security Policy.	Inspected security policy acknowledgement forms from all user organizations. Confirmed procedures for allowing user access to the NWOCA network with the assistant to the director.	6 of 90 user organizations did not sign and return the security policy.
Authorization from the appropriate level of management is required before setting up a user account on the Alpha server.	Identified new user accounts with access to USAS, USPS, EMIS, and/or SAAS/EIS. Sampled 30 usernames from the population of new users and inspected the corresponding authorization e-mail or service desk ticket to confirm access was authorized and the access on the Alpha matched the request. Inquired with the help desk technician to confirm the process for authorizing access to the Alpha.	No exceptions noted. Note: Only new users have authorization for their access on the Alpha. Anyone that had access granted before 2006 would not have a form on file.
User organizations are required to confirm user accounts and associated access privileges annually with a positive confirmation to NWOCA. NWOCA tracks the status of the confirmation and performs any necessary follow-up communication to facilitate a response from the user organization.	Inspected confirmation documentation, including communication between NWOCA and the user organizations and the verification checklist used to track the status of verification requests.	37of 37 member user organizations responded to the confirmation request. Confirmations are not required for non-member user organizations and confirmations do not verify the accuracy of user access privileges.

<table>
<tr><td colspan="2"><b>IT Security -</b> Control Objective:
<b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Banner screens indicating users’ consent to NWOCA’s user policies are displayed before and after a user logs on the OpenVMS operating system. The banner screen text is included in the startup process for the OpenVMS operating system.</td><td>Inspected the banner screens displayed prior and subsequent to login into the OpenVMS systems.
Inspected the startup process for OpenVMS.</td><td>No exceptions noted.</td></tr>
<tr><td>Detection control alarms are enabled through OpenVMS to track security related events, such as break-in attempts and excessive login failures, and are logged to audit journals for monitoring of potential security violations.</td><td>Inspected the enabled security alarms and audits for the OpenVMS system.
Inspected the listing of audit journals for the OpenVMS system.</td><td>No exceptions noted.</td></tr>
<tr><td>Security violations are extracted, compiled into summary and detailed security reports, and e-mailed to the director of planning and research and network/systems services director nightly through OpenVMS command procedures on the OpenVMS system. Daily, the reports are reviewed for login failures, breakins, and changes to the user authorization file. The command procedures are automatically resubmitted to the system daily.</td><td>Inspected the following information for the OpenVMS system relating to the security monitor reports:
• Example of a Security Monitor report.
• Command procedure used to generate the report.
• SUBMITALL.COM command procedure and listing.
• SUBMIT_ALL.DAT listing of batches to be run by SUBMIT_ALL.COM.
Inquired with the network/systems services director to confirm violations are reviewed on a daily basis.</td><td>No exceptions noted.</td></tr>
<tr><td>Anti virus software is installed on a Windows 2000 server that primarily scans all inbound and outbound e-mail. Definitions are updated automatically, and infected items are deleted to help prevent and detect computer viruses.</td><td>Inspected the anti-virus update information from the Sophos scheduling settings, from the Sophos on-access scan screen, and the virus notification.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>IT Security -</b> Control Objective:
<b>Security Management</b> - Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td colspan="4"><b>User Control Considerations</b>:
Confirm that user organization management has made users aware of the NWOCA security policies and that the users should take precautions to confirm passwords are not compromised.

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

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

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

Confirm that user organization management is retaining signed copies of the authorization form for new user accounts and changes to existing accounts.</td></tr>
</table>

IT Security - Control Objective: **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Individual user profiles are used to grant access rights and privileges for the OpenVMS system. The user profiles on the OpenVMS system do not consist of an excessive number of inactive or disabled profiles.	Using security analysis tools extracted the following information from the user authorization file: • Inactive user accounts. • DISUSERED user accounts. Inspected the generated information and inquired with the network/systems services director regarding the purpose and appropriateness of the account settings.	No relevant exceptions noted.
Use of wild card characters in proxy accounts is restricted to ensure proxy accounts do not permit blanket access.	Inspected the network proxy listing for wild card characters.	No relevant exceptions noted.
Access to the operating system command line (DCL) is restricted to authorized users.	Using a security analysis tool, extracted user accounts that do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER or RESTRICTED flags set. Inspected the results of the extracted information and inquired with the NWOCA projects manager regarding the appropriateness of these accounts.	No relevant exceptions noted.

<table>
<tr><td colspan="2"><b>IT Security -</b> Control Objective:
<b>System Level Access Controls -</b> Access to the computer system, programs, and data should be appropriately restricted.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Password parameters are in place to aid in the authentication of user access to the OpenVMS system. Passwords used by individual profiles agree to password policies established by the NWOCA and profiles with pre-expired passwords are not excessive on the OpenVMS system.</td><td>Extracted password information from the user authorization file. Inspected user's account password parameters and compared accounts to policy-defined standards as follows:
• Passwords lengths must be greater than or equal to the minimum established value.
• User Accounts have a password lifetime equal to or shorter than the established value.
• The number of user accounts with pre-expired passwords is minimal.
Inspected the above exception reports to identify relevant exceptions. Inquired with the network/systems services director regarding the appropriateness of the listed accounts.</td><td>Passwords are not forced to be changed every 90 days or less.</td></tr>
<tr><td>Login parameters have been set to control and monitor sign-on attempts.</td><td>Inspected the login parameter settings.</td><td>No exceptions noted.</td></tr>
<tr><td>A program, HITMAN, constantly monitors terminal activity and logs off inactive users. The program is part of the startup command ensuring the program is consistently executed at startup.</td><td>Inspected the HITMAN parameters to confirm they were set to automatically logoff inactive users.
Inspected the start up file to confirm the HITMAN utility is part of the startup procedures.</td><td>No exceptions noted.</td></tr>
<tr><td>Access to production data files and programs is restricted to authorized users.</td><td>Using a security analysis tool, identified and inspected production data files with WORLD access and executables files with WORLD WRITE and/or DELETE access.</td><td>No relevant exceptions noted.</td></tr>
</table>

IT Security - Control Objective: **System Level Access Controls** - Access to the computer system, programs, and data should be appropriately restricted.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
A private internal network and firewall are used to control Internet traffic and maintain a logical segregation between user organizations.	Inspected the firewall configuration for evidence that Internet traffic is restricted through the firewall. In addition, confirmed the existence of a private internal network.	No relevant exceptions noted.
Security parameters are in place to control access to the NWOCALAND domain.	Using a security analysis tool, extracted information from the security profile. Inspected users' account password parameters and compared accounts to policy-defined standards as follows: • Password lengths must be greater than or equal to the minimum established value. • User accounts have a password lifetime equal to or shorter than the established value. • User accounts are locked-out after a defined number of failed access attempts. Inspected accounts that have not logged into the system in over 180 days.	No relevant 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:
Security parameters are in place to control access to the NBECLAND domain.	Using a security analysis tool, extracted information from the security profile. Inspected users' account password parameters and compared accounts to policy-defined standards as follows: • Password lengths must be greater than or equal to the minimum established value. • User accounts have a password lifetime equal to or greater than the established value. • User accounts are locked-out after a defined number of failed access attempts. Inspected accounts that have not logged into the system in over 180 days.	Password minimum length, password history and lockout parameters do not comply with minimum standards.
Access to the NWWEBAPPS, NWNET, and NWGAP server directories are restricted to appropriate personnel.	Inspected group printouts and directory listings for access rights to each directory. Using a security analysis tool, extracted information about network servers to confirm no access to shared files on the NWWEBAPPS, NWNET, and NWGAP servers.	No exceptions noted.
Access to accounts on the Linux servers is restricted to authorized personnel.	Inspected the ECT/Passwd and ECT/Shadow files to confirm user access.	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.	Using security analysis tools, extracted OpenVMS accounts containing USAS, USPS, SAAS/EIS, and/or EMIS OECN identifiers from the user authorization file. Inspected the reports generated for evidence of the use of identifiers to segregate access to the applications. Inquired with the network/systems services director regarding the OSA utility and the process used to assign application identifiers.	No exceptions noted.
Access to the USAS, USPS, SAAS/EIS, and EMIS application systems is authorized by user management.	Identified new user accounts with access to USAS, USPS, EMIS, and/or SAAS/EIS. Sampled 30 usernames from the population of new users and inspected the corresponding authorization e-mail or service desk ticket to confirm access on the Alpha matched the request.	No exceptions noted.
User Control Consideration: User Identification Codes (UICs), passwords and access privileges should only be issued to authorized users who need access to computer resources to perform their job function.		

IT Security - Control Objective: **System Software and Utilities Access Controls** - Use of master passwords, powerful utilities, and system manager facilities, should be appropriately controlled.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
WORLD access to “key” system files is restricted.	Used security analysis tools to extract files from the system directories. Inspected the list of files with WORLD Write or Delete access. Inspected the file protection masks on the security files.	No exceptions noted.
System level UICs are restricted to authorized personnel. UICs belonging to the system group are determined by the parameter value for MAXSYSGROUP. UICs less than the MAXSYSGROUP value have system level privileges.	Inspected the MAXSYSGROUP value for the Alpha server. Inspected the list of accounts with a UIC less than the MAXSYSGROUP value.	No exceptions noted.
Use of an alternate user authorization file is not permitted.	Inspected the value of the user authorization alternate parameter for the OpenVMS system. Inspected the system directory listings for an alternate user authorization file.	No exceptions noted.
Remote access to the firewall is restricted through password protection.	Inspected the firewall configuration. Observed a remote access attempt to the firewall. Inspected the results of invalid attempts to access the firewall.	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 appropriately controlled.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The OECN_SYSMAN identifier and BYPASS privilege that grant all access privileges for all state developed applications are restricted to authorized users.	Inspected the accounts with the OECN_SYSMAN identifier and the BYPASS privilege. Inquired with the network/systems services director to confirm the functionality of the OECN_SYSMAN identifier and BYPASS privilege.	No exceptions noted.
The user profiles on the OpenVMS system do not consist of an excessive number of high-privileged profiles.	Using security analysis tools extracted accounts with elevated privileges from the user authorization file.	Users had high privileged access to the Alpha that are no longer employed by the SSDT or no longer need that access.
High-level access on the NWOCALAND and NBECLAND domains is restricted to appropriate NWOCA and SSDT personnel.	**NWOCALAND domain** Using a security analysis tool, extracted information from the security profile file. Inspected network user and group information to confirm whether the server was adequately protected from unauthorized access. **NBECLAND domain and NWAPFS & NWWEBAPPS servers** Inspected the domain, NWAPFS, and NWWEBAPPS server group accounts to confirm appropriateness of the administrative accounts.	The administrator account is shared by multiple users.

<table>
<tr><td colspan="2"><b>IT Security -</b> Control Objective:
<b>Physical Security</b> - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Physical access to the computer room and its contents is restricted to authorized personnel.</td><td>Observed the use of keypad entry devices throughout the period of fieldwork. Observed motion detection devices in the computer room.
Through inquiry with the network systems services director confirmed the access codes are periodically changed.</td><td>No exceptions noted.</td></tr>
<tr><td>Environmental controls are in place to protect against and/or detect fire, water, humidity, or changes in temperature.</td><td>Inspected the computer room with the network/systems services director to confirm the existence of the environmental controls.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Considerations:</b>
PCs and terminals should be protected against damage or misuse by having separate areas, either independent rooms or sections of rooms that restrict access to only authorized individuals.
Communication lines, junctions and modems should be secured in an area that restricts access to only authorized individuals.</td></tr>
</table>

IT Operations

IT Operations – Control Objective: **System Administration and Maintenance** - Appropriate procedures should be established to ensure the system is properly maintained and monitored.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The NWOCA performs certain routine jobs for system maintenance through the scheduling programs, SUBMITALL and DECScheduler.	Inspected the DECScheduler listing of jobs to confirm that routine system maintenance jobs are automatically scheduled. Confirmed the purpose of the various system maintenance jobs with the network/systems services director. Inspected the operating system startup printout to confirm that DECScheduler was initialized during the startup of the system.	No exceptions noted.
The ANALYZE system utility is run weekly to help prevent file failure or corruption of the RMS (record management services) databases.	Inspected the DECScheduler listing of jobs to confirm the ANA_SIERRA job is being executed to run the ANALYZE system utility weekly. Inspected the ANA_SIERRA log (created on 5/4/08) obtained from the network/systems services director and inquired about the functions of the ANALYZE system utility. Inspected OpenVMS system startup printout (“SYSTARTUP_VMS” command procedure) to confirm the DECScheduler was initialized during the startup of the system.	No exceptions noted.
A service agreement with HP covers maintenance and failures of the computer hardware.	Inspected the hardware maintenance agreement to confirm hardware is covered and the period of coverage with the help desk technician and the NWOCA treasurer.	No exceptions noted.

<table>
<tr><td colspan="2"><b>IT Operations –</b> Control Objective:
<b>System Administration and Maintenance -</b> Appropriate procedures should be established to ensure the system is properly maintained and monitored.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>WhatsUp Gold software monitors network performance and alerts staff of hardware failures and system problems.</td><td>Made inquiries with the network/systems services director regarding the functions of the WhatsUp Gold utility.
Inspected the WhatsUp Gold Device View, Ping Report, and Active Monitor Report for documentation of server status.</td><td>No exceptions noted.</td></tr>
<tr><td>Help Desk personnel log operational failures in Unicenter Service Guide upon notification by users or operation staff.</td><td>Observed the Unicenter Service Plus Service Desk application. Additionally, inspected the ticket reports for the following:
• Request Number
• Status
• Modified Date
• Parent Group
• Contacts
• Open and closed ticket listings.</td><td>No exceptions noted.</td></tr>
</table>

IT Operations - Control Objective: **Backup** - Up-to-date backups of programs and data should be available in emergencies.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Backups of programs and data are automated and scheduled. Backup logs are generated and are available for review.	Inspected the backup procedures for the NWOCA production servers (NWOCA4) and inquired with network/systems services director regarding procedures and review of logs. Inspected example system backup logs for the NWOCA production servers (NWOCA4, NWAPFS, NWNET, and SQLDEV). Inspected the DECScheduler (NWOCA4), EVault InfoStage CentralControl (NWAPFS, NWNET, and SQLDEV) backup parameters to confirm backups are automatically scheduled. Inspected the OpenVMS system startup printout (“SYSTARTUP_VMS” command procedure) to confirm that DECScheduler was initialized during the startup of the system.	No relevant exceptions noted.
Backups are either stored on tape in a secure on-site location or are stored on external RAID drives off-site.	Inquired about the backup tape storage procedures with the SSDT programmer/analyst and the network/systems services director.	No relevant exceptions noted.
A service agreement with Cerdant covers maintenance and failures of the E-Vault backup software.	Inspected the Cerdant maintenance agreement for documentation of coverage.	No exceptions noted.
Backup tapes are stored off-site in a physically and environmentally secure location.	Inquired with the network/systems services director regarding backup tape storage procedures with and inspected the storage of off-site backup tapes to confirm the backups are adequately secured.	No exceptions noted.

<table>
<tr><td colspan="3"><b>IT Operations -</b> Control Objective:
<b>Backup</b> - Up-to-date backups of programs and data should be available in emergencies.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td colspan="4"><b>User Control Considerations:</b>
The user organization should retain source documents for an adequate period to ensure data can be re-entered in the event that data files are destroyed prior to being backed up and rotated off-site.
The user organization should establish and enforce a formal data retention schedule with their ITC for the various application data files.</td></tr>
</table>

FINANCIAL APPLICATION CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Uniform School Accounting System (USAS), Release 6.1

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Authorization:</b> Information entered into the entity’s computer application represents valid data approved by the entity’s management.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Overall:</b> USAS identifiers are used to limit user access to those USAS menu items necessary to perform their job responsibilities or assigned duties. Each identifier has uniquely defined access levels.</td><td>Inspected the USAS Menu Hierarchical Chart that defined all of the available menu items for use.
Accessed all available menu items for a user granted the following identifiers:
• OECN_USAS
• OECN_USAS_RO
• OECN_USAS_GM
• OECN_USAS_REQ
• OECN_AR
• OECN_AR_RO
• OECN_AR_GM
Observed how menu options differed among identifiers.
In addition, selected a privileged menu item (ACTMOD – Account Modifications) restricted to the OECN_USAS and the OECN_USAS_GM identifier, and attempted to access it with a lesser privileged profile, OECN_USAS_RO.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Authorization:</b> Information entered into the entity’s computer application represents valid data approved by the entity’s management.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Overall:</b> The AUDITS program automatically generates an audit trail, which can be used to help detect unauthorized additions, deletions and modifications to data.</td><td>Observed the SSDT systems analyst create three AUDITS reports using the following sort options:
• Date (4/15/08).
• Fund (572).
• Program (ACCTXML)
In both the USAS Web and USAS VMS interface, observed the SSDT systems analyst post an addition, deletion and modification transaction. Confirmed the observed addition, deletion, and modification transactions were reported on an AUDITS report.</td><td>No exceptions noted.</td></tr>
</table>

Uniform School Accounting System – *Control Objective:* **Authorization:** Information entered into the entity’s computer application represents valid data approved by the entity’s management.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Overall: The USASEC program is an optional program to restrict user access at the application level.	Inspected the USASEC setup screen for the access flags and account code filters available to restrict individual users at the application level. Observed the functionality of the access flags set at Y and N for each of the following: • Add or Modify Vendors. • Modify Invoice-to Address. • Allow Negative Budget. • Allow Negative Appropriation. Confirmed results in both the USAS Web and USAS VMS interface were consistent with the USASEC flag settings. Also observed the systems analyst set filters that restricted access to all funds other than 500. Observed the systems analyst successfully post to fund 516 and was denied access to post to fund 001. For an example user organization, inspected a SECUR report showing the users and their application level access rights.	No exceptions noted.

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Authorization:</b> Information entered into the entity’s computer application represents valid data approved by the entity’s management.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Overall:</b> The account coding available for use in the USAS application adheres to the standards established by the Ohio Auditor of the State’s Office.</td><td>Compared the list of account codes available for use in the USAS application (USAS.IDX) to the list of mandated account codes in the AOS USAS User Manual.
In addition, with the assistance of the SSDT systems analyst, attempted to enter two account codes not specified on the USAS.IDX (funds 040 and 412) into the CASHSCN screen.
Inspected the error message to confirm warning/error messages were produced when not using established account codes.</td><td>No relevant exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Considerations</b>:
User organizations should create an employee's USAS access to mirror the segregation of duties established by user organization management. Identifiers should limit employee’s access to only those USAS functions they need to perform their job. For larger user organizations, the program module, USASEC, may be used to further restrict access related to requisition processing, PO processing, vendor maintenance, appropriation maintenance and certain report and lookup programs.
The AUDITS report may be used by the user organization to confirm data entry or to detect unauthorized transactions that may have occurred. These reports are available as an option to help the users detect errors that could not be otherwise identified through existing controls. The AUDITS report can be sorted in a variety of ways.</td></tr>
</table>

Uniform School Accounting System – *Control Objective:* **Completeness of Input:** All authorized transactions are input and accepted for processing by the application.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Investment Income: Required verification fields within the INVEST program force the user to enter an investment number, date of the investment, fund number, amount to be invested, check number, and vendor numbers into the appropriate fields before the transaction can be processed. Errors occur when these fields are left blank and prohibit the user from processing the investment until the errors are resolved.	With the assistance of the SSDT systems analyst, attempted to leave all fields in the INVEST program blank. Inspected error messages to confirm error/warning messages were produced when fields were not completed.	No exceptions noted.
Investment Income: A report is available in USAS listing all investment transactions processed through INVEST.	With the assistance of the SSDT systems analyst, processed an investment through INVEST. Ran a report in the INVESTMENT PROCESSING program of all investments processed for all dates. Inspected the report for inclusion of the newly created investment.	No exceptions noted.
Receipts: Required verification fields within the RCPROC program force the user to enter a receipt transaction number, date of the transaction, and revenue account codes into the appropriate fields before the transaction can be processed. Errors occur when these fields are left blank and prohibit the user from processing the receipt until the errors are resolved.	With the assistance of the SSDT systems analyst, attempted to leave all fields in the RCPROC program blank. Inspected screens of error messages to confirm error/warning messages were produced when fields were not completed.	No exceptions noted.

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Completeness of Input:</b> All authorized transactions are input and accepted for processing by the application.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Receipts:</b> Required verification fields within the USAS Web receipt module force the user to enter the date of the transaction and revenue account codes into the appropriate fields before the transaction can be processed.
Errors occur when these fields are left blank and prohibit the user from processing the receipt until the errors are resolved.</td><td>With the assistance of the SSDT systems analyst, attempted to leave all fields in the USAS Web receipt module blank.
Inspected error messages to confirm error/warning messages were produced when fields were not completed.</td><td>No exceptions noted.</td></tr>
<tr><td><b>Receipts:</b> A report is available in USAS listing all receipt transactions processed through RCPROC and the USAS Web receipt module.</td><td>With the assistance of the SSDT systems analyst, processed a receipt through RCPROC with a date of 04/30/2008.
With the assistance of the SSDT systems analyst, processed a receipt through the USAS Web receipt module with a date of 04/30/2008.
Using RECLED, generated a report in USAS of all receipts processed on 04/30/2008. Inspected the report for inclusion of the newly created receipts.</td><td>No exceptions noted.</td></tr>
<tr><td><b>Budgetary:</b> The APPROP programs include all account codes used in the current year when setting up a budget for the following year.</td><td>With the assistance of the SSDT systems analyst, attempted to enter a Next Year Proposed Maintenance (NYPMNT) appropriation for a selected user organization to confirm account codes are automatically included.</td><td>No exceptions noted.</td></tr>
</table>

Uniform School Accounting System – *Control Objective:* **Completeness of Input:** All authorized transactions are input and accepted for processing by the application.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Purchasing: Required verification fields within the POSCN program force the user to enter a purchase order number, item quantity, date, vendor number, and budget account codes into the appropriate fields before the transaction can be processed. Errors occur when these fields are left blank and prohibit the user from processing the purchase order until the errors are resolved.	With the assistance of the SSDT systems analyst, attempted to leave all fields in the POSCN program blank. Inspected error messages to confirm error/warning messages were produced when fields were not completed.	No exceptions noted.
Purchasing: Required verification fields within the USAS Web purchase order module force the user to enter an item quantity, date, vendor number, and budget account codes into the appropriate fields before the transaction can be processed. Errors occur when these fields are left blank and prohibit the user from processing the purchase order until the errors are resolved.	With the assistance of the SSDT systems analyst, attempted to leave all fields in the USAS Web purchase order module blank. Inspected error messages to confirm error/warning messages were produced when fields were not completed.	No exceptions noted.
Purchasing: A report is available in USAS listing all purchase order transactions processed through POSCN and the USAS Web purchase order module.	With the assistance of the SSDT systems analyst, processed a purchase order through POSCN with a date of 04/30/2008. With the assistance of the SSDT analyst, processed a purchase order through the USAS Web purchase order module with a date of 04/30/2008. Using PODETL, generated a report of all purchase orders processed on 04/30/2008. Inspected the report for inclusion of the newly created POs.	No exceptions noted.

Uniform School Accounting System – *Control Objective:* **Completeness of Input:** All authorized transactions are input and accepted for processing by the application.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
USAS Data Export: USAS data export produces a GAAP_EXP file that can be used in the WebGAAP application. Changes to account balances made through USAS are reflected in the GAAP_EXP file.	With the assistance of the SSDT systems analyst, used the USAS Data Export program and produced the GAAP_EXP file. With the assistance of the SSDT systems analyst, changed the budget balance for an account code. Using USAS Data Export program, generated a new GAAP_EXP file, and inspected the file for inclusion of the updated budget balance.	No exceptions noted.
User Control Considerations: Through the investment-processing program (INVEST), users can run reports which may be used to confirm all investment transactions have been completely and accurately input. Users are given the capability to run reports, which may be used to confirm all receipt transactions have been completely and accurately input. Users are given the capability to run reports, which may be used to confirm all purchase order transactions have been completely and accurately input.		

Uniform School Accounting System – *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Overall: The AUDITS program automatically generates an audit trail, which can be used to help detect unauthorized additions, deletions, and modifications to data.	Observed the SSDT systems analyst create three AUDITS reports using the following sort options: • Date (4/15/08). • Fund (572). • Program (ACCTXML) In both the USAS Web and USAS VMS interface, observed the SSDT systems analyst post an addition, deletion and modification transaction. Confirmed the observed addition, deletion, and modification transactions were reported on an AUDITS report.	No exceptions noted.

Uniform School Accounting System – *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Investment Income: Online validity edit checks in the INVEST program prevent or detect incorrect entry of investment numbers, date of investment, fund, check number, and vendor prior to processing. Error messages are posted for erroneous data and further processing is prohibited until the errors are resolved.	With the assistance of the SSDT systems analyst, entered the following data into the INVEST program and inspected the system's response: • Entered invalid data into the numeric investment number field. • Entered invalid dates and months into the date field. • Inspected a listing of valid funds from which investments can be made for the selected user organization. Entered two funds that were not defined in the fund listing into the investment fund field. • Entered the highest check number already processed and on file and a string containing an alphabetic character into the numeric check number field. • Inspected a listing of valid vendors from which investments can be made for the selected user organization. Entered two vendors that were not registered on the vendor list into the vendor number field.	No exceptions noted.

Uniform School Accounting System – *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Receipts: Online validity edit checks in the RCPROC program prevent or detect incorrect entry of receipt transaction number, date of transaction, and revenue account codes prior to processing. Error messages are posted for erroneous data and further processing is prohibited until the errors are resolved.	With the assistance of the SSDT systems analyst, entered the following data into the RCPROC program and observed the system's response: • Entered the highest receipt transaction number already processed and on file and a string containing an alphabetic character into the numeric receipt transaction number field. • Entered invalid dates and months into the date field. • Inspected a listing of valid revenue account codes from which receipts can be made for the selected user organization. Entered two revenue account codes not defined in the listing into the revenue account code field.	No exceptions noted.

Uniform School Accounting System – *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Receipts: Online validity edit checks in the USAS Web Receipt module prevent or detect incorrect entry of receipt transaction number, date of transaction, and revenue account codes prior to processing. Error messages are posted for erroneous data and further processing is prohibited until the errors are resolved.	With the assistance of the SSDT systems analyst, entered the following data into the USAS Web Receipt module. Observed the system's response or validation error: • Entered the highest receipt transaction number already processed and on file and a string containing an alphabetic character into the numeric receipt transaction number field. • Entered invalid dates and months into the date field. • Inspected a listing of valid revenue account codes from which receipts can be made for the selected user organization. Entered a revenue account code not defined in the listing into the revenue account code field.	No exceptions noted.

Uniform School Accounting System – *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Purchasing: Online validity edit checks are in the POSCN program to prevent or detect incorrect entry of purchase order numbers, date of purchase orders, vendors, and budget account codes prior to processing. Error messages are posted for erroneous data and further processing is prohibited until the errors are resolved.	With the assistance of the SSDT systems analyst, entered the following data into the POSCN program and observed the system's response: • Used the POSCN programs 'Find' option to find an existing purchase order number already processed and on file. Entered the existing purchase order number. Also entered a string containing an alphabetic character into the numeric purchase order number field. • Entered invalid dates and months into the date field. • Inspected a listing of valid vendors for the selected user organization. Entered two vendors that were not registered on the vendor list into the vendor number fields. • Inspected a listing of valid budget account codes for the selected user organization. Entered two budget account codes not defined in the listing into the budget account code fields.	No exceptions noted.

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Accuracy of Input:</b> Authorized transactions are accurately recorded and in the proper period.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Purchasing:</b> Online validity edit checks are in the USAS Web Purchase Order module to prevent or detect incorrect entry of purchase order numbers, date of purchase orders, vendors, and budget account codes prior to processing.
Error messages are posted for erroneous data and further processing is prohibited until the errors are resolved.</td><td>With the assistance of the SSDT systems analyst, entered the following data into the USAS Web Purchase Order option. Observed the system’s response or validation error:
• Entered an existing purchase order number. Also, entered a string containing an alphabetic character into the numeric purchase order number field.
• Entered invalid dates and months into the date field.
• Inspected a listing of valid vendors for the selected user organization. Entered two vendors not registered on the vendor list into the vendor number fields.
• Inspected a listing of valid budget account codes for the selected user organization. Entered two budget account codes not defined in the listing into the budget account code fields.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Considerations</b>:
The AUDITS report may be used by the user organization to confirm data entry or to detect unauthorized transactions that may have occurred. These reports are available as an option to help the users detect errors that could not be otherwise identified through existing controls. The AUDITS report can be sorted in a variety of ways.</td></tr>
</table>

Uniform School Accounting System - *Control Objective:* **Cutoff of Transactions:** All activity is posted in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Receipts: Online validity edit checks in the RCPROC program prevent entry of a transaction date outside of the current processing month. An error message is posted for erroneous data and further processing is prohibited until the error is resolved.	With the assistance of the SSDT systems analyst, entered a transaction date outside of the current processing month into the RCPROC program and observed the system's response. Utilizing a third party software tool (ACL), AOS performed data integrity procedures on user organization USAS data files, including the summarization of the number of transactions by month and day for the year.	No relevant exceptions noted.
Receipts: Online validity edit checks in the USAS Web Receipt module prevent entry of a transaction date outside of the current processing month. An error message is posted for erroneous data and further processing is prohibited until the error is resolved.	With the assistance of the SSDT systems analyst, entered a transaction date outside of the current processing month into the USAS Web Receipt module and observed the system's response. Utilizing a third party software tool (ACL), AOS performed data integrity procedures on user organization USAS data files, including the summarization of the number of transactions by month and day for the year.	No relevant exceptions noted.
Purchasing: Online validity edit checks in the POSCN program warn users of processing transactions in a future processing period. A warning message is displayed for POs outside the processing period.	With the assistance of the SSDT systems analyst, entered a purchase order date outside of the current processing year into the POSCN program and observed the system's response. Utilizing a third party software tool (ACL), AOS performed data integrity procedures on user organization USAS data files, including the summarization of the number of transactions by month and day for the year.	No relevant exceptions noted.

Uniform School Accounting System - *Control Objective:* **Cutoff of Transactions:** All activity is posted in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Purchasing: Online validity edit checks in the USAS Web Purchase Order module warn users of processing transactions in a future processing period. A warning message is displayed for POs outside the processing period.	With the assistance of the SSDT systems analyst, entered a purchase order date outside of the current processing year into the USAS Web Purchase Order option and observed the system's response. Utilizing a third party software tool (ACL), AOS performed data integrity procedures on user organization USAS data files, including the summarization of the number of transactions by month and day for the year.	No relevant exceptions noted.

Uniform School Accounting System - *Control Objective:* **Transaction Classification:** All activity is coded to the proper account classification.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Overall: The account coding available for use in the USAS application adheres to the standards established by the Ohio Auditor of the State's office.	Compared the list of account codes available for use in the USAS application (USAS.IDX) to the list of mandated account codes in the AOS USAS User Manual. Also, with the assistance of the SSDT systems analyst, attempted to enter two account codes not specified on the USAS.IDX (funds 040 and 412) into the CASHSCN screen. Inspected the error message to confirm warning/error messages were produced when not using established account codes	No relevant exceptions noted.

Uniform School Accounting System - *Control Objective:* **Transaction Classification:** All activity is coded to the proper account classification.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Receipts: A report is available in USAS listing all receipt transactions processed through RCPROC and the USAS Web receipt module. This report can be used to confirm that receipt transactions have been coded to the proper accounts.	With the assistance of the SSDT systems analyst, processed a receipt through RCPROC with a date of 04/30/2008. With the assistance of the SSDT systems analyst, processed a receipt through the USAS Web receipt module with a date of 04/30/2008. Using RECLED, generated a report of all receipts processed on 04/30/2008. Inspected the report for inclusion of the newly created receipts.	No exceptions noted.
Purchasing: A report is available in USAS listing all purchase order transactions processed through POSCN and the USAS Web purchase order module. This report can be used to confirm that purchase order transactions have been coded to the proper accounts.	With the assistance of the SSDT systems analyst, processed a purchase order through POSCN with a date of 04/30/2008. With the assistance of the SSDT analyst, processed a purchase order through the USAS Web purchase order module with a date of 04/30/2008. Using PODETL, generated a report of all purchase orders processed on 04/30/2008. Inspected the report for inclusion of the newly created POs.	No exceptions noted.
User Control Consideration: Users are given the capability to run reports, which may be used to confirm all receipt transactions have been completely and accurately input. Users are given the capability to run reports, which may be used to confirm all purchase order transactions have been completely and accurately input.		

Uniform School Accounting System - *Control Objective:* **Transaction Occurrence:** All recorded activity occurred and is not fictitious. Duplicate activity is not recorded.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Investment Income: Online validity edit checks in the INVEST program prevent the entry of a duplicate check number. An error message is posted for erroneous data and further processing is prohibited until the error is resolved.	With the assistance of the SSDT systems analyst, entered the highest check number already processed and on file into the numeric check number field of the INVEST program and inspected the system's response.	No exceptions noted.
Receipts: Online validity edit checks in the RCPROC program prevent the entry of a duplicate receipt transaction number. An error message is posted for erroneous data and further processing is prohibited until the error is resolved.	With the assistance of the SSDT systems analyst, entered the highest receipt transaction number already processed and on file into the numeric receipt transaction number field of the RCPROC program and observed the system's response.	No exceptions noted.
Receipts: Online validity edit checks in the USAS Web Receipt module prevent the entry of a duplicate receipt transaction number. An error message is posted for erroneous data and further processing is prohibited until the error is resolved.	With the assistance of the SSDT systems analyst, entered the highest receipt transaction number already processed and on file into the USAS Web Receipt module and observed the system's response.	No exceptions noted.
Purchasing: Online validity edit checks in the POSCN program prevent the entry of a duplicate purchase order number. An error message is posted for erroneous data and further processing is prohibited until the error is resolved.	With the assistance of the SSDT systems analyst, used the POSCN program's 'Find' option to find an existing purchase order number already processed and on file. Entered the existing purchase order number into the POSCN program and observed the system's response.	No exceptions noted.

Uniform School Accounting System - *Control Objective:* **Transaction Occurrence:** All recorded activity occurred and is not fictitious. Duplicate activity is not recorded.			**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:	
Purchasing: Online validity edit checks in the USAS Web Purchase Order module prevent the entry of a duplicate purchase order number. An error message is posted for erroneous data and further processing is prohibited until the error is resolved.	With the assistance of the SSDT systems analyst, entered an existing purchase order number into the USAS Web Purchase Order option and observed the system's response.	No exceptions noted.	

Uniform School Accounting System – *Control Objective:* **Integrity of Standing Data:** Changes to standing data are authorized and accurately input.			**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:	
Overall: User organization users do not have access to update the function, fund, object, instructional level, or receipt number of the account codes, which are stored in the USAS.IDX file. Changes to the USAS.IDX file are made through the program change process and access to update the USAS.IDX file is limited to SSDT personnel.	With the assistance of the SSDT systems analyst, attempted to access the USAS.IDX file through the REVEDT program with the access privileges of the OECN_SYSMAN. Inspected the program change log for the addition of fund 71 during the FY year Inspected the USAS.IDX file privileges. Confirmed users with full access were limited to SSDT staff.	Eight of the accounts that had access to the USAS.IDX file did not need the access to perform their job functions, two of the eight accounts were disusered during fieldwork. No other relevant exceptions noted.	

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Integrity of Standing Data:</b> Changes to standing data are authorized and accurately input.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Overall:</b> The AUDITS program automatically generates an audit trail, which can be used to help detect unauthorized additions, deletions, and modifications to data.</td><td>Observed the SSDT systems analyst create three AUDITS reports using the following sort options:
• Date (4/15/08).
• Fund (572).
• Program (ACCTXML)
In both the USAS Web and USAS VMS interface, observed the SSDT systems analyst post an addition, deletion and modification transaction. Confirmed the observed addition, deletion, and modification transactions were reported on an AUDITS report.</td><td>No exceptions noted.</td></tr>
</table>

Uniform School Accounting System – *Control Objective:* **Integrity of Standing Data:** Changes to standing data are authorized and accurately input.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Purchasing: The USASEC program is an optional program that can restrict user access to modify the user organization’s vendor file. The SECUR report contains the users and their access to update the vendor file.	Inspected the USASEC setup screen for the access flags and account code filters available to restrict individual users at the application level. Observed the functionality of the access flags set at Y and N for each of the following: • Add or Modify Vendors. • Modify Invoice-to Address. • Allow Negative Budget. • Allow Negative Appropriation. Confirmed results in both the USAS Web and USAS VMS interface were consistent with the USASEC flag settings. Also observed the systems analyst set filters that restricted access to all funds other than 500. Observed the systems analyst successfully post to fund 516 and was denied access to post to fund 001. For an example user organization, inspected a SECUR report showing the users and their application level access rights.	No exceptions noted.
Purchasing: Duplicate vendor numbers are prohibited from being entered into the USAS application for each user organization. Error messages are displayed and further processing is prohibited until the errors are resolved.	With the assistance of the SSDT systems analyst, used the VENSCN program’s ‘Find’ option to find an existing vendor number already on file. Entered the existing vendor number (100) into the VENSCN program and observed the system’s response.	No exceptions noted.

Uniform School Accounting System – *Control Objective:* **Integrity of Standing Data:** Changes to standing data are authorized and accurately input.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Purchasing: Duplicate vendor numbers are prohibited from being entered into the USAS Web application for each user organization. Error messages are displayed and further processing is prohibited until the errors are resolved.	With the assistance of the SSDT systems analyst, entered the existing vendor number (100) in USAS Web and observed the system's response.	No exceptions noted.
User Control Consideration: User organization personnel should regularly inspect changes to account codes, fund codes, and vendor information. The Account Change Report, the Fund Change Report, and the AUDITS report may be used to detect any unauthorized changes to standing data. The AUDITS report may be used by the user organization to confirm data entry or to detect unauthorized transactions that may have occurred. These reports are available as an option to help the users detect errors that may not be otherwise identified through existing controls. The AUDITS report can be sorted in a variety of ways. User organizations may use the USASEC program to restrict access to the user organization's vendor file to a select group of designated individuals.		

Uniform School Accounting System – *Control Objective:* **Completeness and Accuracy of Updating:** Updates, modifications and/or additions to information already on the application’s files or database are accurately entered.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Overall: Access to directly modify the balances of the account codes without processing a transaction is restricted to users with the OECN_SYSMAN identifier.	In both the USAS VMS and USAS Web interfaces and with the assistance of the SSDT systems analyst, accessed the account balance of the General Fund. Attempted to modify the account balances with the OECN_SYSMAN identifier and the OECN_USAS_GM identifier.	No exceptions noted.
Receipts: The receipts and refunds processes automatically update the appropriate revenue and cash accounts.	With the assistance of the SSDT systems analyst, processed a receipt and confirmed the corresponding revenue and cash account balances were updated. Also, processed a refund and confirmed the corresponding revenue and cash account balances were updated.	No exceptions noted.
Receipts: The receipts and refunds processes automatically update the appropriate revenue accounts in USAS Web.	With the assistance of the SSDT systems analyst, processed a receipt and confirmed the corresponding revenue account balance in USAS Web was updated. Processed a refund and confirmed the corresponding revenue account balance in USAS Web was updated and corresponding cash balances were updated in the USAS VMS interface.	No exceptions noted.

Uniform School Accounting System – *Control Objective:*
Completeness and Accuracy of Updating: Updates, modifications and/or additions to information already on the application's files or database are accurately entered.

Control Objective Has Been Met

Control Procedures:	Test Descriptions:	Test Results:
Budgetary: Amounts entered on the budgetary worksheets in the APPROP program automatically update the user organizations' yearly budgets and are recorded on the REVWRK, APPWRK, and BUDWRK reports.	With the assistance of the SSDT systems analyst, processed amounts on a user organization's budgetary worksheets in APPROP. Inspected the REVWRK, APPWRK, and BUDWRK reports to confirm the proposed accounts were reflected.	No exceptions noted.
Purchasing: The purchase order, invoice, and check processes automatically update the appropriate appropriation, budget, and cash accounts.	With the assistance of the SSDT systems analyst, processed the following transactions. • A purchase order. • An invoice. • A check. Inspected the corresponding appropriation, budget, and cash accounts to confirm the account balances were updated.	No exceptions noted.
Purchasing: The purchase order, invoice, and check processes automatically update the appropriate budget accounts in USAS Web.	With the assistance of the SSDT systems analyst, processed the following transactions. • A purchase order through USAS Web • An invoice through USAS Web • A check through USAS CKPROC (VMS) Inspected the corresponding budget accounts in USAS Web to confirm account balances were updated.	No exceptions noted.

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Completeness and Accuracy of Updating:</b> Updates, modifications and/or additions to information already on the application’s files or database are accurately entered.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Purchasing:</b> AUTOPOST is available to post automatically USPS payroll data or any other externally formatted file into USAS.</td><td>With the assistance of the SSDT systems analyst, inspected a USPS payroll file that was created and stored on a user organization’s server.
Inspected the account balances of the associated budget, appropriation, and cash accounts. Validated the file using the AUTOPOST program and inspected the corresponding report and error listing. Then, based on the error listing, resolved all errors and processed the file using AUTOPOST.
Inspected the updated account balances of the associated budget, appropriation, and cash accounts.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Uniform School Accounting System</b> – <i>Control Objective:</i>
<b>Completeness and Accuracy of Accumulated Data</b>: The integrity of accumulated data is preserved.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td><b>Overall:</b> USAS detail transactions are accurately reported on Exhibits 2 and 3 of the 4502 report.</td><td>Utilizing a third party software tool (ACL), AOS performed data integrity procedures on user organization USAS data files. AOS recalculated exhibits 2 and 3 of the 4502 report from the USAS data files, and compared to the user organization prepared exhibits 2 and 3.</td><td>No relevant exceptions noted.</td></tr>
<tr><td><b>Overall:</b> The ACTBAL program produces an Account Balance report that can be used to review appropriation, budget, and cash account balance information.</td><td>With the assistance of the SSDT systems analyst, created and inspected the ACTBAL report for Pettisville Local Schools using test data.</td><td>No exceptions noted.</td></tr>
</table>

Uniform School Accounting System – *Control Objective:* **Completeness and Accuracy of Accumulated Data**: The integrity of accumulated data is preserved.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Overall: An Error Listing is produced by the ACTBAL program when an out of balance condition exists between the transactions processed and the budget and revenue accounts.	With the assistance of the SSDT systems analyst, created an out of balance condition on the account master file and then ran the ACTBAL program to generate an error listing. Inspected the account balance and error listing for inclusion of the out of balance condition.	No exceptions noted.
Overall: The BALCHK program produces an error report when an out of balance condition exists between the revenue and cash accounts or between the appropriation, budget, and cash accounts.	With the assistance of the SSDT systems analyst, created an out of balance condition on the account master file and then ran the BALCHK program to generate an error listing. Inspected the error listing for inclusion of the out of balance condition.	No exceptions noted.
User Control Consideration: User organizations should regularly inspect USAS reports so that errors or out of balance conditions can be addressed on a timely basis. These reports are available as an option to help the users detect errors and may be used to complement existing controls.		

Uniform School Accounting System - *Control Objective:* **Restricted Access to Assets and Records:** Only authorized personnel have access to the USAS data.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Overall: USAS identifiers are used to limit user access to those USAS menu items necessary to perform their job responsibilities and assigned duties. Each identifier has uniquely defined access levels.	Inspected the USAS Menu Hierarchical Chart that defined all of the available menu items for use. Accessed all available menu items for a user granted the following identifiers: • OECN_USAS • OECN_USAS_RO • OECN_USAS_GM • OECN_USAS_REQ • OECN_AR • OECN_AR_RO • OECN_AR_GM Observed how menu options differed among identifiers. In addition, selected a privileged menu item (ACTMOD – Account Modifications) restricted to the OECN_USAS and the OECN_USAS_GM identifier, and attempted to access it with a lesser privileged profile, OECN_USAS_RO.	No exceptions noted.

Uniform School Accounting System - *Control Objective:*
Restricted Access to Assets and Records: Only authorized personnel have access to the USAS data.

Control Objective Has Been Met

Control Procedures:	Test Descriptions:	Test Results:
Overall: The USASEC program is an optional program to restrict user access at the application level.	Inspected the USASEC setup screen for the access flags and account code filters available to restrict individual users at the application level. Observed the functionality of the access flags set at Y and N for each of the following: • Add or Modify Vendors. • Modify Invoice-to Address. • Allow Negative Budget. • Allow Negative Appropriation. Confirmed results in both USAS Web and USAS VMS were consistent with the USASEC flag settings. Also observed the systems analyst set filters that restricted access to all funds other than 500. Observed the systems analyst successfully post to fund 516 and was denied access to post to fund 001. For an example user organization, inspected a SECUR report showing the users and their application level access rights.	No exceptions noted.

User Control Consideration:
User organizations should have manual controls in place to reasonably ensure open requisitions are approved by the appropriate level of management prior to processing.

User organizations should create an employee's USAS access to mirror the segregation of duties established by user organization management. Identifiers should limit employee’s access to only those USAS functions they need to perform their job. For larger user organizations, the program module, USASEC, may be used to further restrict access related to requisition processing, PO processing, vendor maintenance, appropriation maintenance and certain report and lookup programs.

Uniform Staff Payroll System (USPS), Release 4.2

<table>
<tr><td colspan="3"><b>Uniform Staff Payroll System</b> - <i>Control Objective:</i>
<b>Authorization:</b> Information entered into the entity’s computer application represents valid data approved by the entity’s management.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>The CHKUPD program produces reports that can be used to confirm that all payroll funds have been properly allocated. A summary report option in the check update program (CHKUPD) contains a signature block for the treasurer.</td><td>Inspected the Payroll Account Distribution Summary for the May 30, 2008 payroll from the payroll test system. Inspected the payroll account distribution report to confirm the total of all funds agrees to the check amount on the payroll account distribution summary.
Also inspected the report to confirm the Treasurer’s Certificate was produced. In addition, the report was inspected for flags indicating allocation errors.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>USPS identifiers have uniquely defined access levels to help prevent unauthorized changes to data.</td><td>Inspected the USPS Menu Hierarchical Chart that defines all of the available menu items.
Observed while the SSDT systems analyst modified user access to the following:
• OECN_PPS_RO
• OECN_USPS
Observed how access rights to the menu options changed when assigned different identifiers.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

Uniform Staff Payroll System - *Control Objective:*
Authorization: Information entered into the entity’s computer application represents valid data approved by the entity’s management.

Control Objective Has Been Met

Control Procedures:	Test Descriptions:	Test Results:
The AUDRPT program automatically generates an audit trail, which can be used to detect unauthorized additions, deletions, and modifications to standing data. Two reports, the Demand Audit Report and the Official Audit Report, provide the same audit-trail information. The Official Report shows all changes made since the last Official Report was run. This report also has a signature and date line for the treasurer to indicate approval of the changes made.	Observed the SSDT systems analyst make changes to the test data via the employee maintenance screens. Inspected the Demand Audit Report, the Official Audit Report, and the summary report to confirm that the changes made by the SSDT systems analyst appeared on the reports.	No exceptions noted.

User Control Consideration:
User organization treasurers should be authorizing and approving the payroll for each processing period. A summary report option in the check update program (CHKUPD) contains a signature block for the treasurer. Confirm the treasurer signs the “Treasurer Certificate” to certify the amount required for payroll obligations is available.

User organizations should create an employee's USPS access to mirror the segregation of duties established by management. Identifiers should limit employee’s access to only those USPS functions they need to perform their job.

The User organization treasurer should inspect and approve the Official Audit Report (AUDRPT) to confirm changes made to an employee’s standing data.

Uniform Staff Payroll System - *Control Objective:* **Completeness of Input:** All authorized transactions are input and accepted for processing by the application.		**Control Objective** **Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Online edit checks are used to verify that data for all required fields is entered before an employee record is accepted for input.	With the assistance of the SSDT systems analyst, performed the following tests of the edits: • Attempted to process an employee record while leaving the social security number, employee ID, state, hire date, and direct deposit fields blank. • Entered a valid SSN, but left employee ID, state, hire date, and direct deposit blank. • Entered a valid SSN and state, but left the hire date, direct deposit, and employee ID blank. Inspected the resulting errors/warning messages.	No exceptions noted.

Uniform Staff Payroll System - *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective** **Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Online edit checks are used to verify that data entered is accurately recorded during payroll processing. Error messages are displayed for erroneous data, and further processing is prohibited until the errors are resolved.	Observed the SSDT systems analyst enter valid and invalid data for selected fields within selected USPS programs. Inspected the warnings and error messages that were displayed when invalid data was entered.	No exceptions noted.

Uniform Staff Payroll System - *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The INICAL program generates reports that can be used to verify the accuracy of payroll transactions.	Observed the SSDT systems analyst enter test data forcing errors to occur in the payroll application. Inspected the resulting INICAL Error Report for errors.	The error listing displayed the errors created from erroneous data; however, processing was allowed to continue. No other relevant exceptions noted.
Online edit checks are used to prevent duplicate employee records from being entered. Error messages are posted with each entry of erroneous data and further processing is prohibited until the errors are resolved.	Observed as the SSDT systems analyst attempted to add an employee in both the USPS Web application and VMS interface who was already on the system. • Using a duplicate SSN. • Using a valid SSN and duplicate employee ID. Observed the system for warning messages and a halt to processing.	No exceptions noted.
Online edit checks are used in the USPS Web application to verify that data entered is accurately recorded during payroll, or drop down boxes are provided to prevent the entry of erroneous data. Error messages are displayed for erroneous data, and further processing is prohibited until the errors are resolved.	Observed the SSDT systems analyst enter invalid data for the edit fields and verified drop down boxes were available to select accurate data within the USPSWeb application. Inspected warnings and error message that were displayed when invalid data was entered.	No exceptions noted.
User Control Consideration: User organizations should have established procedures to inspect and follow up on errors identified on the USPS Initial Processing Totals (INICAL) report.		

Uniform Staff Payroll System - *Control Objective:* **Cutoff of Transactions:** Employee services are recorded in the proper period.	**Control Objective Has Been Met**

<table>
<tr><td colspan="2"><b>Uniform Staff Payroll System</b> - <i>Control Objective:</i>
<b>Cutoff of Transactions:</b> Employee services are recorded in the proper period.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Online validity edit checks in the INICAL program prevent incorrect entry of a transaction date outside of the current processing month.</td><td>Utilizing a third party software tool (ACL), AOS performed data integrity procedures on user organization USPS data files, including the summarization of the number of transactions by month and day for the current year as compared to the prior year.</td><td>No relevant exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Consideration</b>:
User organizations should have established procedures to inspect the INICAL.TXT report to help ensure the proper dates are reflected in payroll processing.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Uniform Staff Payroll System</b> - <i>Control Objective:</i>
<b>Transaction Classification:</b> Payroll transactions relate to the employee’s position and duties performed.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The CHKUPD program produces reports that can be used to confirm that all payroll funds have been properly allocated.</td><td>Inspected the Payroll Account Distribution Summary for the May 30, 2008 payroll from the payroll test system. Inspected the payroll account distribution report to confirm the total of all funds agrees to the check amount on the payroll account distribution summary.
Also inspected the report to confirm that the Treasurer’s Certificate was produced. In addition, the report was inspected for flags indicating allocation errors.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="3">**Uniform Staff Payroll System** - *Control Objective:*
Transaction Classification: Payroll transactions relate to the employee’s position and duties performed.</td><td>**Control Objective Has Been Met**</td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>Stop and start dates defined by the employee’s job (JOBSCN) are used by the system to include only appropriate jobs within the current payroll.</td><td>Verified that an employee without a contract stop date defined in their JOBSCN was included in the current payroll (UPDCAL_CURRENT).
Observed as the SSDT systems analyst changed the employee’s contract stop date to a date prior to the payroll start date and confirmed the employee was removed from the payroll.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td colspan="4">**User Control Consideration**:
User organizations should have established procedures to inspect and follow up on any errors in the BUDPRO report.</td></tr>
</table>

<table>
<tr><td colspan="3">**Uniform Staff Payroll System - Control Objective:**
Transaction Occurrence: Payroll transactions are not duplicated nor fictitious.</td><td>**Control Objective Has Been Met**</td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>Online edit checks are used to prevent duplicate employee records from being entered.
Error messages are posted with each entry of erroneous data and further processing is prohibited until the errors are resolved.</td><td>Observed as the SSDT systems analyst attempted to add an employee in both the USPS Web application and VMS interface who was already on the system.
• Using a duplicate SSN.
• Using a valid SSN and duplicate employee ID.
Observed the system for warning messages and a halt to processing.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td colspan="4">**User Control Consideration**:
User organizations should have established procedures to inspect and follow up on any errors in the BUDPRO report.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Uniform Staff Payroll System</b> - <i>Control Objective:</i>
<b>Integrity of Standing Data:</b> Changes to standing data are authorized and accurately input.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The AUDRPT program automatically generates an audit trail, which can be used to detect unauthorized additions, deletions, or modifications to standing data.
Two reports, the Demand Audit Report and the Official Audit Report, provide the same audit trail information. The Official Report shows all changes made since the last Official Report was run. This report also has a signature and date line for the treasurer to indicate approval of the changes made.</td><td>Observed the SSDT systems analyst make changes to the test data via the employee maintenance screens. Specifically, changed the vacation benefits and the direct deposit option.
Inspected the Demand Audit Report, the Official Audit Report, and the summary report page to confirm that the changes made by the SSDT systems analyst appeared on the reports.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Consideration</b>:
The user organization treasurer should inspect and approve the Official Audit Report (AUDRPT) to confirm changes to the employees' standing data.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Uniform Staff Payroll System</b> - <i>Control Objective:</i>
<b>Completeness and Accuracy of Updating:</b> Updates, modifications and/or additions to information on the payroll files or database are accurately entered and properly update the payroll and general ledger database.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The CURPAY.INI file internally tracks USPS programs to prevent them from being run out of sequence.</td><td>Inspected the programs contained in the CURPAY.INI file and the USPS processing flags used to track the program run sequence. Observed while the SSDT systems analyst attempted to run the CHKPRT program out of sequence, i.e., prior to running the CALCPAY program.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Uniform Staff Payroll System</b> - <i>Control Objective:</i>
<b>Completeness and Accuracy of Updating:</b> Updates, modifications and/or additions to information on the payroll files or database are accurately entered and properly update the payroll and general ledger database.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The CHKLEV report, Current Leave Usage and Balances, tracks current leave usage and balances.</td><td>Inspected employees’ leave balances (i.e., CHKLEV report) prior to making any additions to employees’ leave balances. Observed while the SSDT systems analyst entered 1 day of personal leave to one employee. Recalculated the leave balance and compared it to the Check Leave Report for the selected employee.</td><td>No exceptions noted.</td></tr>
<tr><td>The CHCKUPD program creates the Projected Payroll Account Distribution Summary and a batch file for posting to USAS.</td><td>Compared the BUDPRO (Projected Payroll Account Distribution Summary) report to the batch file created from the test payroll system on May 30, 2008 to confirm that BUDPRO mirrors the batch file.</td><td>No exceptions noted.</td></tr>
<tr><td>Detail payroll transactions are posted to USAS and recorded within USPS for complete and accurate fiscal year-end reporting.</td><td>Utilizing a third party software tool (ACL), AOS performed data integrity procedures on user organization USPS data files. AOS compared USPS and USAS payroll totals and compared two USPS check files to confirm the completeness and accuracy of the USPS data files.</td><td>No relevant exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Consideration</b>:
The Projected Payroll Account Distribution Summary (BUDPRO) should be compared to the payroll expenditures updated to the USAS to confirm payroll expenses were updated accurately and completely to the general ledger. This comparison should be performed after each payroll period is complete.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Uniform Staff Payroll System</b> - <i>Control Objective:</i>
<b>Completeness and Accuracy of Accumulated Data</b>: The integrity of accumulated data is preserved.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The CHKUPD program produces reports that can be used to confirm that all payroll funds have been properly allocated.</td><td>Inspected the Payroll Account Distribution Summary Report, which is generated by the CHKUPD program.</td><td>No exceptions noted.</td></tr>
<tr><td>The USPS programs track the individual payroll records and accurately rolls them up to a summary report.</td><td>Inspected the biweekly payroll report for pay date 05/30/08. Recalculated the fields for net pay (*NET*), adjusted gross (*ADJ GROSS*), total deductions (*TOTAL*), and total annual deductions (*TOTANN*).   In addition, recalculated biweekly report pay group totals and check stub totals.
Inspected the Projected Payroll Account Distribution Summary for pay date 05/30/08 and traced the total for all funds expended totals to the total gross on the biweekly payroll report for pay date 05/30/08.
Inspected the Deduction Total Report and the Deduction Detail Report and traced the totals from the detail report to the total report. Verified the deduction reports matched the recalculated biweekly reports totals.
Also agreed the pay total from the Biweekly Payroll report to the Payroll Distribution Summary totals as of 5/30/08.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Consideration</b>:
The Projected Payroll Account Distribution Summary (BUDPRO) should be compared to the payroll expenditures updated to the USAS to confirm payroll expenses were updated accurately and completely to the general ledger. This comparison should be performed after each payroll period is complete.</td></tr>
</table>

Uniform Staff Payroll System - *Control Objective:* **Restricted Access to Assets and Records:** Only authorized personnel have access to the payroll and personnel data.		**Control Objective** **Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
USPS identifiers limit user access to those USPS menu items necessary to perform their job responsibilities. Each identifier has uniquely defined access levels.	Inspected the USPS Menu Hierarchical Chart that defined all of the available menu items for use. Observed while the SSDT systems analyst modified user access to the following: • OECN_PPS_RO • OECN_USPS Observed how access rights to the menu options changed when assigned different identifiers.	No exceptions noted.
User Control Consideration: User organizations should create an employee's USPS access to mirror the segregation of duties established by user organization management. Identifiers should limit employee’s access to only those USPS functions they need to perform their job.		

School Asset Accounting System/Equipment Inventory Subsystem (SAAS/EIS), Release 2.1

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Authorization:** Information entered into the SAAS/EIS represents valid data approved by the User organization's management.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
SAAS/EIS identifiers are assigned to help prevent unauthorized changes to data. Each identifier has uniquely defined access levels.	Inspected the SAAS/EIS Menu Hierarchical Chart that defined all of the available menu items. Observed while the SSDT systems analyst modified user access for each of the following identifiers: • No SAAS/EIS identifier. • OECN_EIS_RO. • OECN_EIS. Observed how menu items changed when assigned different identifiers.	No exceptions noted.
An audit trail is automatically generated by the EISSCN program to help detect unauthorized additions, modifications, and deletions to inventory data.	Observed while the SSDT systems analyst performed the following functions: • Added a new fixed asset record. • Changed an existing fixed asset record. • Deleted a fixed asset record. Inspected the EIS Demand Audit Report to confirm the changes made appeared on the report.	No exceptions noted.
User Control Consideration: The user organization treasurer should inspect and approve the EIS Official Audit Report (EIS801) to confirm changes made to SAAS/EIS standing data. User organizations should create an employee's SAAS/EIS access to mirror the segregation of duties established by user organization management. Identifiers should limit employee's access to only those SAAS/EIS functions they need to perform their job.		

<table>
<tr><td colspan="3"><b>School Asset Accounting System/Equipment Inventory Subsystem</b> - Control Objective:
<b>Completeness of Input:</b> All authorized transactions are input and accepted for processing by SAAS/EIS.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>The EISSCN program has online edit checks to verify that data for all required fields is entered before a new asset record is added.

Errors occur when these fields are left blank and prohibit users from processing the record until the errors are resolved.</td><td>With the assistance of the SSDT systems analyst, attempted to enter a new fixed asset and left the following required fields blank:

• Account code.
• Acquisition amount.
• Location code.
• Asset class.
• Function number.
• Fund number.
• Acquisition method.
• Depreciation method.
• Tag number.
• Depreciation beginning date.

Inspected the errors/warning messages that were received when the required fields were left blank.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>School Asset Accounting System/Equipment Inventory Subsystem</b> - Control Objective:
<b>Accuracy of Input:</b> Authorized SAAS/EIS transactions are accurately recorded and in the proper period.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>The EISSCN program provides online edit checks to verify the accuracy of entered data.

Error messages are displayed with each entry of erroneous data, and further processing is prohibited until the errors are resolved.</td><td>Observed the SSDT systems analyst enter invalid data for the following fields within the EISSCN program to confirm the edit checks prevented users from entering inaccurate data:

• Account code - transaction indicator.
• Vendor number.
• Acquisition date.
• Purchase date.
• Fund.
• Item status.
• Depreciation method.

Inspected the warnings/error messages that were received when invalid data was entered.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>The EISSCN program has online edit checks to prevent the entering of a duplicate fixed asset tag number.</td><td>Observed while the SSDT systems analyst attempted to enter a new fixed asset using an existing tag number.

Inspected the warnings/error messages that were received to confirm duplicate tag numbers cannot be entered.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Cutoff of Transactions:** Transactions are recorded in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
When entering new items, the acquisition date must be within the fiscal year the school is currently working in, or the item cannot be added.	Observed while the SSDT systems analyst attempted to enter a new fixed asset with an acquisition date outside of the current fiscal year. Inspected the warnings/error messages that were received to confirm transactions entered must be in the audit period.	No exceptions noted.

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Transaction Classification:** Transactions are recorded to the proper accounts.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The EISSCN program provides online edit checks to verify the accuracy of entered data. Error messages are displayed with each entry of erroneous data, and further processing is prohibited until the errors are resolved.	Observed the SSDT systems analyst enter invalid data for the following fields within the EISSCN program to confirm the edit checks prevented users from entering inaccurate data: • Account code - transaction indicator. • Fund. Inspected the warnings/error messages that were received when invalid data was entered.	No exceptions noted.

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Transaction Occurrence:** Recorded transactions occurred, are not fictitious, and duplicates are prevented from occurring.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The SAAS/EIS system interfaces with the USAS system to extract items from the USAS invoice file and add them to an EIS pending file.	Observed the SSDT systems analyst enter a purchase order in the USASWeb and process and then invoice the purchase order. Inspected the EIS pending file for the invoiced item from USAS.	No exceptions noted.
The EISSCN program has online edit checks to prevent the entering of a duplicate fixed asset tag number.	Observed while the SSDT systems analyst attempted to enter a new fixed asset using an existing tag number. Inspected the warnings/error messages that were received to confirm duplicate tag numbers cannot be entered.	No exceptions noted.

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Integrity of Standing Data:** Changes to standing data are authorized and accurately input.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
An audit trail is automatically generated by the EISSCN program to help detect unauthorized additions, modifications, and deletions to inventory data.	Observed while the SSDT systems analyst performed the following functions: • Added a new fixed asset record. • Changed an existing fixed asset record. • Deleted a fixed asset record. Inspected the EIS Demand Audit Report to confirm the changes made appeared on the report.	No exceptions noted.

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Integrity of Standing Data:** Changes to standing data are authorized and accurately input.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The original cost field is only modifiable with the addition of an acquisition transaction within the current fiscal year.	Observed while the SSDT systems analyst attempted to update the original cost of an item in ITMSCN to confirm it is not a modifiable field. Attempted to add an acquisition record with an acquisition date outside the current fiscal year, and inspected the error message that was received to confirm the original cost can only be updated with an acquisition record during the current fiscal year.	No exception noted.

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Completeness and Accuracy of Update:** Updates, modifications and/or additions to information already on the SAAS/EIS database are accurately entered.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The EISSCN program issues messages informing the user of the update that has occurred.	Inspected the EIS Demand Audit Report to confirm that added, modified, and deleted records were documented.	No exceptions noted.
The EISSCN mass change program automatically generates an audit trail of mass changes made to data on the inventory file.	Observed the SSDT systems analyst enter a mass change for the location category and location number fields. Inspected the "Actual Mass Change Audit Trail" report to confirm the mass change was documented.	No exceptions noted.

<table>
<tr><td colspan="3"><b>School Asset Accounting System/Equipment Inventory Subsystem</b> - Control Objective:
<b>Completeness and Accuracy of Update:</b> Updates, modifications and/or additions to information already on the SAAS/EIS database are accurately entered.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>Life-to-date (LTD) depreciation is calculated automatically and updated when the fiscal year is closed.</td><td>Obtained and inspected the Book Value Report (EIS305) and recalculated the depreciation value for 12 of the 80 items with a remaining life.

Observed the SSDT systems analyst close the EIS fiscal year 2008, then reran the Book Value Report and verified the remaining life was reduced by one year and the LTD depreciation was increased to reflect another year of depreciation. In addition, verified the LTD depreciation amount was increased in ITMSCN for the 12 items selected for testing.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td colspan="4"><b>User Control Consideration</b>:
The SAAS/EIS application provides the user with the option of either running a projection only report or updating the files with the mass changes. The user organization should run and review a “Projected Mass Change Audit Trail” report before updating the files.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>School Asset Accounting System/Equipment Inventory Subsystem</b> - Control Objective:
<b>Completeness and Accuracy of Accumulated Data</b> – <i>The integrity of accumulated data is preserved.</i></td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>Capitalized assets cannot be deleted outside the current fiscal year.</td><td>Observed the SSDT systems analyst attempt to delete a capitalized asset added during a prior fiscal year.

Inspected the error message to ensure prior year capital assets cannot be deleted.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

School Asset Accounting System/Equipment Inventory Subsystem - Control Objective: **Restricted Access to Assets and Records:** Only authorized personnel have access to the SAAS/EIS data.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
SAAS/EIS identifiers are assigned to help prevent unauthorized changes to data. Each identifier has uniquely defined access levels.	Inspected the SAAS/EIS Menu Hierarchical Chart that defined all of the available menu items. Observed while the SSDT systems analyst modified user access for each of the following identifiers: • No SAAS/EIS identifier. • OECN_EIS_RO. • OECN_EIS. Observed how menu items changed when assigned different identifiers.	No exceptions noted.
User Control Consideration: User organizations should create an employee's SAAS/EIS access to mirror the segregation of duties established by user organization management. Identifiers should limit employee’s access to only those SAAS/EIS functions they need to perform their job.		

Education Management Information System (EMIS), Release 2.6

<table>
<tr><td colspan="2"><b>Education Management Information System</b> - <i>Control Objective:</i>
<b>Authorization:</b> Information entered into the entity’s computer application represents valid data approved by the entity’s management.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>EMIS identifiers are assigned to limit access to EMIS menu screens to help prevent unauthorized changes to data. Each identifier has uniquely defined access levels.</td><td>Inspected the EMIS Menu Hierarchical Chart that defined all of the available menu items for use.
Observed while the SSDT systems analyst modified user access to the following:
• OECN_EMIS_FIN.
• OECN_EMIS_SFU.
• OECN_EMIS_STF.
• OECN_EMIS_STU.
• OECN_EMIS_GEN.
• OECN_EMIS.
Observed how menu options changed with each identifier.</td><td>No exceptions noted.</td></tr>
<tr><td>The EAUDRPT automatically generates an audit trail, which can be used to detect unauthorized additions, deletions and modifications to data.</td><td>Observed while the SSDT systems analyst changed the credentials ID for a staff member in the test environment.
Inspected the resulting EMIS audit report to confirm an audit trail is generated to track additions, deletions, and modifications to data.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Consideration</b>:
User organizations should create an employee's EMIS access to mirror the segregation of duties established by user organization management. Identifiers should limit employee’s access to only those EMIS functions they need to perform their job.
The EMIS Audit Report (EAUDRPT) may be used by the user organization to confirm data entry or detect inaccurate changes or deletions that may have occurred.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Education Management Information System</b> - <i>Control Objective:</i>
<b>Completeness of Input:</b> All authorized transactions are input and accepted for processing by the application.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The EMIS program EMSRX searches for duplicate keys and compares the batch file record length to the record length of the detail records in the file.</td><td>For a user organization, created the following scenarios:
• Attempted to load and add a file of student data that contained the same information already on file.
• Modified the file layout and attempted to load the file.
• Removed several records and attempted to load the file.
Inspected the resulting EMSRX Program Error Summary report to confirm the errors were detected.</td><td>No exceptions noted.</td></tr>
<tr><td>Duplicate records cannot be created for a student ID number that is already on the EMIS files.</td><td>Observed while the student services supervisor attempted to add a new record for a student by entering the same EMIS ID as another student that was already on file in the EMIS Web application and VMS interface.
Inspected the resulting error message and confirmed processing was prohibited until the error was resolved.</td><td>The EMIS Web application did not prevent adding a student with a duplicate EMIS ID.
No other relevant exceptions noted.</td></tr>
<tr><td>The EMIS Web program performs edit checks to ensure all required data fields have been entered before processing a transaction.</td><td>Observed while the SSDT systems analyst attempted to add a student record in the EMIS Web application while leaving all fields blank to verify the student ID and IRN fields were required.
Inspected the error messages and confirmed the record could not be saved until the errors were resolved.</td><td>No exceptions noted.</td></tr>
</table>

Education Management Information System - *Control Objective:* **Completeness of Input:** All authorized transactions are input and accepted for processing by the application.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
User Control Consideration: The EMIS Audit Report (EAUDRPT) may be used by the user organization to confirm data entry or detect in accurate changes or deletions that may have occurred.		

Education Management Information System - *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Online edit checks are used to verify the accuracy of entered data. Error messages are displayed when erroneous data is entered.	Observed while invalid data was entered into the EMIS VMS interface for the student status, birth date, user organization IRN, and grade level. Inspected the warnings/error messages that were received when invalid data was entered. Observed while invalid data was entered into the EMIS Web application for the birth date, admission date, special education exit date, and grade level fields. Inspected the warnings/error messages that were received when invalid data was entered. Inspected the EMIS standard validation report to confirm errors were detected in the validation process.	No exceptions noted.

Education Management Information System - *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Reports are generated by the application to identify incorrect information so that timely corrections can be made to data.	Observed while invalid data was entered into the student ID and grade level fields. Inspected the Aggregation Validation and Aggregation Exclusion reports for a user organization to confirm potential errors are detected by the application and flagged. Observed while a student was withdrawn in EMIS, and inspected the Aggregation Exclusion and Validation reports to confirm the withdraw status was detected by the application and flagged.	No exceptions noted.
User Control Consideration: EMIS data, submitted by the user organization to the ODE, is primarily compiled from the user organization’s other software applications including accounting, payroll, personnel and student information systems. Controls should exist to confirm the validity of EMIS data during data entry for these other applications. The process of submitting EMIS data to the ODE should include an inspection and reconciliation of the following reports for financial and staff data: Standard Validation (EMSVLD), Aggregation Validation (EMSAGG5), Aggregation Exclusion (EMSAGG6), and EMSRDET Validation (EMSRDET).		

Education Management Information System - *Control Objective:* **Transaction Occurrence:** *Recorded transactions occurred, are not fictitious, and duplicates are prevented from occurring.*		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The EMIS program EMSRX searches for duplicate keys and compares the batch file record length to the record length of the detail records in the file.	For a user organization, created the following scenarios: • Attempted to load and add a file of student data that contained the same information already on file. • Modified the file layout and attempted to load the file. • Removed several records and attempted to load the file. Inspected the resulting EMSRX Program Error Summary report to confirm the errors were detected.	No exceptions noted.
Duplicate records cannot be created for a student ID number that is already on the EMIS files.	Observed while the student services supervisor attempted to add a new record for a student by entering the same EMIS ID as another student that was already on file in the EMIS Web application and VMS interface. Inspected the resulting error message and confirmed processing was prohibited until the error was resolved.	The EMIS Web application did not prevent adding a student with a duplicate EMIS ID. No other relevant exceptions noted.

<table>
<tr><td colspan="2"><b>Education Management Information System</b> - <i>Control Objective:</i>
<b>Integrity of Standing Data:</b> Changes to standing data are authorized and accurately input.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>SSDT personnel only modify the EMIS standing data contained in the options file when an authorized updated options file is received from ODE.</td><td>Inspected the EMSOPC procedures from the SSDT Programmer’s Handbook, the history of the options file (EMSLCEN.IDX) in the CMS Library, and the associated JIRA issues for the changes made to the options file during the audit period to confirm that changes made were authorized by the ODE.</td><td>No exceptions noted.</td></tr>
<tr><td>Access to the options file is limited to the appropriate SSDT staff.</td><td>Inquired with the SSDT systems analyst regarding access to the directories where the options file is saved.
Inspected the directory/file permissions of the TWILLIAMS directory and the EMSLCE.IDX file privileges. Confirmed users with full access were limited to SSDT staff and that WORLD access is limited to Read and/or Execute.</td><td>Eight of the accounts that had access to the EMSLCE.IDX file did not need the access to perform their job functions, two of the eight accounts were disusered during fieldwork.
No other relevant exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Education Management Information System</b> - <i>Control Objective:</i>
<b>Completeness and Accuracy of Updating:</b> Updates, modifications and/or additions to information already in the EMIS database are accurately entered.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Reports are generated by the application to identify incorrect information so that timely corrections can be made to data.</td><td>Observed while invalid data was entered into the student ID and grade level fields.
Inspected the Aggregation Validation and Aggregation Exclusion reports for a user organization to confirm that potential errors are detected by the application and flagged.
Observed while a student was withdrawn in EMIS, and inspected the Aggregation Exclusion and Validation reports to confirm the withdraw status was detected by the application and flagged.</td><td>No exceptions noted.</td></tr>
<tr><td colspan="3"><b>User Control Consideration</b>:
The process of submitting EMIS data to the ODE should include an inspection and reconciliation of the following reports for financial and staff data: Standard Validation (EMSVLD), Aggregation Validation (EMSAGG5), Aggregation Exclusion (EMSAGG6), and EMSRDET Validation (EMSRDET).</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Education Management Information System</b> - <i>Control Objective:</i>
<b>Completeness and Accuracy of Accumulated Data:</b> The integrity of accumulated data is preserved.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Validation reports are created when programs are run against the EMIS databases. Errors are detected and reported.</td><td>Observed while invalid staff data was entered in the credentials ID field, and invalid student data was entered in the date of birth and grade level fields.
Inspected the EMIS EMSRDET Validation Report for staff errors and the EMIS Standard Validation Report for student errors to confirm the errors carried forward to the reports.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="3">**Education Management Information System** - *Control Objective:*
Completeness and Accuracy of Accumulated Data: The integrity of accumulated data is preserved.</td><td>**Control Objective Has Been Met**</td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td colspan="4">**User Control Considerations**:
The process of submitting EMIS data to the ODE should include an inspection and reconciliation of the following reports for financial and staff data: Standard Validation (EMSVLD), Aggregation Validation (EMSAGG5), Aggregation Exclusion (EMSAGG6), and EMSRDET Validation (EMSRDET).

The user organization superintendent and treasurer should be signing the EMIS Data Accuracy Summary Report and sending a copy to the ODE each reporting period certifying the completeness and accuracy of the reported information.</td></tr>
</table>

<table>
<tr><td colspan="3">**Education Management Information System** - *Control Objective:*
Restricted Access to Assets and Records: Only authorized personnel have access to the EMIS standing data and the individual user organization’s EMIS database.</td><td>**Control Objective Has Been Met**</td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td>EMIS identifiers are used to limit user access to those EMIS menu items necessary to perform their job responsibilities. Each identifier has uniquely defined access levels.</td><td>Inspected the EMIS Menu Hierarchical Chart that defined all of the available menu items for use.

Observed while the SSDT systems analyst modified user access to the following:

• OECN_EMIS_FIN.
• OECN_EMIS_SFU.
• OECN_EMIS_STF.
• OECN_EMIS_STU.
• OECN_EMIS_GEN.
• OECN_EMIS.

Observed how menu options changed when assigned a different identifier.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td colspan="4">**User Control Consideration**:
User organizations should create an employee's EMIS access to mirror the segregation of duties established by user organization management. Identifiers should limit employee’s access to only those EMIS functions they need to perform their job.</td></tr>
</table>

Community School – Average Daily Membership system (CSADM), Release 3.0-1

Community School – Average Daily Membership - *Control Objective:* **Authorization:** Information entered into the entity's computer application represents valid data approved by the entity's management.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
User access to the CSADM application menus is segregated by assignment of user security roles.	Inspected CSADM menus accessible by each role in the development system to confirm user roles segregated access to the application.	No exceptions noted.
The "Added by" and "Modified by" function records who and when changes are made to specific student and enrollment information, which can be used to assist in detecting unauthorized additions and modifications to student data.	Inspected the pseudo code to determine the fields that would trigger documenting a change to a student record. Made changes to the SSID, Disability Condition, First and Last Name, Date of Birth, Enrollment From and To Dates, Guardian Name, Address, City, and Postal Code fields of a test student in the development system. Inspected the creation of the Change Summary in the review menu subsequent to making changes to the student data. Inspected the "Added by" note in the student record subsequent to creating a new student to confirm the username, date and time were included in the note. Inspected the audit table in the CSADM database to determine whether the application logged the date and person making the change.	No exceptions noted.
User security roles are used to restrict administrative rights to authorized SSDT staff at the application level.	Inspected the user profile table using third-party software for users and access levels, and users' assigned administrative access. Confirmed with the senior programmer/analyst the account composition was reasonable and the administrative users were appropriate.	No exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Authorization:** Information entered into the entity's computer application represents valid data approved by the entity's management.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The SSDT requires a request from an authorized ODE representative or a School Admin user for new accounts to be activated.	Sampled 35 out of 331users created after 5/25/07 and obtained the access request e-mails to confirm the requests came from authorized personnel.	No exceptions noted.
Three times each year, the NWOCA sends an e-mail to each CSADM user to validate their account. If the validation is not performed within 30 days of the original validation e-mail, the user account is suspended.	Inspected the e-mail verification job in the Currently Scheduled Jobs menu of the CSADM application to ensure it is scheduled to run three times a year. With the assistance of the senior programmer/analyst, observed the confirmation process and confirmed the user was notified of the confirmation requirement and required to enter the information upon next logon, and the account would be suspended if not validated within 30 days. Obtained a query of all CSADM users and their validation status to identify the users that had completed the quarterly account review for the audit period. Attempted to sign in to the CSADM Application with an account that was suspended to confirm the user is notified of account status and procedures to validate the account.	No relevant exceptions.

User Control Considerations:
User access forms should be required for all users requesting access to the CSADM.

User management should review users, user roles, assigned entities, and access levels at least annually to ensure users are current employees and require the granted access to perform their job responsibilities.

User organization personnel should respond to the account confirmation requests from the NWOCA.

<table>
<tr><td colspan="2"><b>Community School – Average Daily Membership</b> - <i>Control Objective:</i>
<b>Completeness of Input:</b> All authorized transactions are input and accepted for processing by the application.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The CSADM program performs edit checks to ensure all required data fields have been entered before processing a transaction.</td><td>With the assistance of the senior programmer/analyst attempted to process a student transaction while leaving the following required fields blank:

Student Information:
• Last Name.
• First Name.
• Birth Date.
• Ethnicity.
• Gender.
• SSID.
Residency Information:
• From Date.
• Guardian Name.
• Address.
• City.
• State.
• Postal Code.
• Withdraw Code (only required when a to date is entered).

Inspected error messages returned to confirm the fields are required and an error/warning message is produced when fields were left blank.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Community School – Average Daily Membership</b> - <i>Control Objective:</i>
<b>Completeness of Input:</b> All authorized transactions are input and accepted for processing by the application.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The CSADM program performs edit checking to ensure duplicates are not permitted, data is in the correct format, and logical.</td><td>To confirm error/warning messages were produced when fields were invalid, attempted to enter the following:
• A new student with an SSID already used at the community school.
• An SSID at more than one community school for the same time period.
• An incorrectly formatted SSID.
• An incorrectly formatted date (in the effective date, birth date, and IEP date fields).
• A birth date to cause a student to be outside the 5 to 21 year range.
• A from date greater than 30 days before the student was added.</td><td>The CSADM application was not designed with an edit to prevent a student from being enrolled at more than one community school for the same time period.
No other exceptions noted.</td></tr>
<tr><td>A student demographic or enrollment entry cannot be deleted through the CSADM application, regardless of the user role assigned. Deletions must occur directly through the SQL Database.</td><td>With the assistance of the senior programmer/analyst attempted to delete a student record and enrollment record from the application using the ODE Exec and User roles.</td><td>No exceptions noted.</td></tr>
<tr><td>The CSADM system has an edit check for preventing duplicate student enrollment by resident schools.</td><td>With the assistance of the senior programmer/analyst, attempted to add a new resident school for a student with an overlapping effective date range of the same resident school to confirm the application would not accept two enrollments with overlapping effective dates.
Attempted to add another resident school district while the current resident school district had an open effective date range.</td><td>No exceptions noted.</td></tr>
</table>

Community School – Average Daily Membership - *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The CSADM program performs edit checks to ensure all required data fields have been entered before processing a transaction.	With the assistance of the senior programmer/analyst attempted to process a student transaction while leaving the following required fields blank: Student Information: • Last Name. • First Name. • Birth Date. • Ethnicity. • Gender. • SSID. Residency Information: • From Date. • Guardian Name. • Address. • City. • State. • Postal Code. • Withdraw Code (only required when a to date is entered). Inspected error messages returned to confirm the fields were required and an error/warning message is produced when fields were left blank.	No exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The CSADM program performs edit checking to ensure duplicates are not permitted, data is in the correct format, and logical.	To confirm error/warning messages were produced when fields were invalid, attempted to enter the following: • A new student with an SSID already used at the community school. • An SSID at more than one community school for the same time period. • An incorrectly formatted SSID. • An incorrectly formatted date (in the effective date, birth date, and IEP date fields). • A birth date to cause a student to be outside the 5 to 21 year range. • A from date greater than 30 days before the student was added.	The CSADM application was not designed with an edit to prevent a student from being enrolled at more than one community school for the same time period. No other exceptions noted.
The CSADM application automatically calculates the maximum total units allowed to be entered for a residency record based on the effective from date and the available days in the school year. When a student enrollment is set to “Inactive,” the CSADM application automatically reduces the total units to zero.	With the assistance of the senior programmer/analyst, attempted to enter a residency record with the total days exceeding the available days in the school year, and the total hours exceeding the available hours in the school year to confirm the system did not allow excessive units to be entered. Observed while the senior programmer/analyst set an enrollment record to “Inactive” and confirmed the total units were reduced to zero.	The system allowed entering hours that exceeded the time the student was enrolled. No other exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Cutoff of Transactions:** Students are recorded in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The CSADM system has an edit check for preventing duplicate student enrollment by resident school districts.	With the assistance of the senior programmer/analyst, attempted to add a new resident school for a student with an overlapping effective date range of the same resident school to confirm the application would not accept two enrollments with overlapping effective dates. Attempted to add another resident school district while the current resident school district had an open effective date range.	No exceptions noted.
Changes cannot be made in a year that that has been disabled in the CSADM 'Year Maintenance' screen.	With the assistance of the senior programmer/analyst, disabled the 2005-2006 school year in the test environment. Attempted to modify student demographic information for the 2005-2006 school year to confirm the data could not be modified	No exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Cutoff of Transactions:** Students are recorded in the proper period.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The Auto Review process creates warning messages in the student enrollment record if a resident school district does not review the records in a timely manner. After 30 days, the status changes to "Review Warning"; after 45 days, the status changes to "Review Caution"; after 75 days, the status changes to "Review Restricted" and the district cannot review the student record and set error flags.	Inspected the CSADM manual to determine the timing requirements for resident districts to review records. With the assistance of the senior programmer/analyst, attempted to review a student in the development system with a status of "Review Restricted" to determine whether flags could be set. Obtained a snapshot of CSADM data from the senior programmer/analyst. Using a third-party software tool (ACL), calculated 75 days from the last community school modification date, and verified the record status was "Review Restricted" when the last review date was 75 or more days prior to the date of the "snapshot."	No exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Transaction Classification:** Students are assigned to the proper resident school district.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The CSADM system has an edit check for preventing duplicate student enrollment by resident schools districts.	With the assistance of the senior programmer/analyst, attempted to add a new resident school for a student with an overlapping effective date range of the same resident school to confirm the application would not accept two enrollments with overlapping effective dates. Attempted to add another resident school district while the current resident school district had an open effective date range.	No exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Transaction Classification:** Students are assigned to the proper resident school district.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Resident school district users are required to review student information entered by the community schools. Additionally, resident school district management have the ability to set error flags.	With the assistance of the senior programmer/analyst, performed a review of a community school student as a resident school district manager and checked error flags and added notes to the ‘Resident District Review’ screen. Then, inspected the community school student as a resident school district, community school user, and coordinator to confirm the error flags and notes were visible and the status was updated accordingly. Inspected the “Community Schools Report” to confirm student information including error flags was documented.	No exceptions noted.
User Control Consideration: Resident school districts should routinely review student information in the CSADM application to identify errors or questions on a timely basis. Community schools should review the Community Schools Report “Review Status” field to determine whether the resident school district is reviewing student information entered by the community schools.		

Community School – Average Daily Membership - *Control Objective:* **Transaction Occurrence:** Students recorded are attending the school and are not fictitious		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
The CSADM program performs edit checking to ensure duplicates are not permitted, data is in the correct format, and logical.	To confirm error/warning messages were produced when fields were invalid, attempted to enter the following: • A new student with an SSID already used at the community school. • An SSID at more than one community school for the same time period. • An incorrectly formatted SSID. • An incorrectly formatted date (in the effective date, birth date, and IEP date fields). • A birth date to cause a student to be outside the 5 to 21 year range. • A from date greater than 30 days before the student was added.	The CSADM application was not designed with an edit to prevent a student from being enrolled at more than one community school for the same time period. No other exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Transaction Occurrence:** Students recorded are attending the school and are not fictitious		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
NWOCA offers a web service to manually validate SSIDs before they are entered into CSADM. As SSIDs are saved within the CSADM application, they are compared to a file from IBM that contains valid SSIDs. If the SSID is not contained within the IBM file, the record cannot be saved. If an SSID is removed from the IBM file at any time, the SSID status shows as “INVALID” in the CSADM record and the Community School Report the next time the status is displayed.	Entered a valid SSID, invalid SSID, and incorrectly formatted SSID into the SSID web service to confirm a manual validation process was in place for SSID checking. With the assistance of the senior programmer/analyst, entered a student into CSADM with an invalid SSID and confirmed the record could not be saved. Inspected a student record to confirm an invalid SSID was flagged as “INVALID” the next time the record was accessed. Inspected the Community School Report to confirm the SSID was identified as invalid. Inspected a snapshot of CSADM data from the senior programmer/analyst to confirm students with invalid SSIDs were included in the snapshot as required by ODE.	No exceptions noted.
User Control Consideration: User organizations should routinely review student information in the CSADM application to identify errors on a timely basis. Community schools should run the Community Schools Report and select the options that would include student errors and either a “BLANK” or an “INVALID” SSID status.		

Community School – Average Daily Membership - *Control Objective:* **Integrity of Standing Data:** Changes to standing data are authorized and accurately input.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Standing data cannot be modified through the CSADM application. Only SSDT personnel have access to the CSADM database to make changes to the standing data.	Inspected the listing of windows users with access to the CSADM database and confirmed the appropriateness of users with access to the CSADM database with the senior programmer/analyst.	No exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Integrity of Standing Data:** Changes to standing data are authorized and accurately input.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
Resident school district users are required to review student information entered by the community schools. Additionally, resident school district management has the ability to set error flags.	With the assistance of the senior programmer/analyst, performed a review of a community school student as a resident school district manager and checked error flags and added notes to the 'Resident District Review' screen. Then, inspected the community school student as a resident school district user, community school user, and coordinator to confirm the error flags and notes were visible and status was updated accordingly. Inspected the "Community Schools Report" to confirm student information, including error flags, was documented.	No exceptions noted.
The "Added by" and "Modified by" function records who and when changes are made to specific student and enrollment information, which can be used to assist in detecting unauthorized additions and modifications to student data. .	Inspected the pseudo code to determine the fields that would trigger documenting a change to a student record. Made changes to the SSID, Disability Condition, First and Last Name, Date of Birth, Enrollment From and To Dates, Guardian Name, Address, City, and Postal Code fields of a test student in the development system. Inspected the creation of the Change Summary in the review menu subsequent to making changes to the student data. Inspected the "Added by" note in the student record subsequent to creating a new student to confirm the username, date and time were included in the note. Inspected the audit table in the CSADM database to determine whether the application logged the date and person making the change.	No exceptions noted.

<table>
<tr><td colspan="2"><b>Community School – Average Daily Membership</b> - <i>Control Objective:</i>
<b>Integrity of Standing Data:</b> Changes to standing data are authorized and accurately input.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td colspan="3"><b>User Control Consideration</b>:
Resident school districts should routinely review student information in the CSADM application to identify errors or questions on a timely basis. Community schools should review the Community Schools Report “Review Status” field to determine whether the resident school district is reviewing student information entered by the community schools.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Community School – Average Daily Membership</b> - <i>Control Objective:</i>
<b>Completeness and Accuracy of Updating:</b> Updates, modifications and/or additions to information already on the application’s files or database are accurately entered.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>Resident school district users are required to review student information entered by the community schools. Additionally, resident school district management have the ability to set error flags.</td><td>With the assistance of the senior programmer/analyst, performed a review of a community school student as a resident school district manager and checked error flags and added notes to the ‘Resident District Review’ screen. Then, inspected the community school student as a resident school district user, community school user, and coordinator to confirm the error flags and notes were visible and status was updated accordingly.

Inspected the “Community Schools Report” to confirm the student information including error flags was documented.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Community School – Average Daily Membership</b> - <i>Control Objective:</i>
<b>Completeness and Accuracy of Updating:</b> Updates, modifications and/or additions to information already on the application’s files or database are accurately entered.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td>Test Results:</td></tr>
<tr><td>The “snapshot” is automatically calculated by the application and includes student information entered subsequent to the last “snapshot” when the rebuild option is selected.</td><td>In the test system, using a demo community school, performed the following procedures in the following sequence:
• Obtained and inspected all student information.
• Performed a “snapshot” of the student information.
• Updated the student information.
• Obtained and inspected all student information.
• Performed a “snapshot” of the student information without selecting the “rebuild” option.
• Performed a “snapshot” of the student information selecting the “rebuild” option.
Using a third-party software tool (ACL), compared the student information to the “snapshots” before and after the changes to the student information to confirm:
• The “snapshot” represented the proper student information in the database and the information was compiled accurately and completely.
• When the “rebuild” was not selected for the “snapshot” the “snapshot” did not include the changes to the student information since the last “snapshot”.
• When the “rebuild” was selected for the “snapshot,” the “snapshot” included all current student information.</td><td>No exceptions noted.</td></tr>
</table>

Community School – Average Daily Membership - *Control Objective:* **Completeness and Accuracy of Updating:** Updates, modifications and/or additions to information already on the application's files or database are accurately entered.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
User Control Consideration: Resident school districts should routinely review student information in the CSADM application to identify errors or questions on a timely basis. Community schools should review the Community Schools Report "Review Status" field to determine whether the resident school district is reviewing student information entered by the community schools.		

Community School – Average Daily Membership - *Control Objective:* **Completeness and Accuracy of Accumulated Data**: The integrity of accumulated data is preserved.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
A student demographic entry or enrollment entry cannot be deleted from the CSADM application, regardless of the user role assigned. Deletions must occur directly through the SQL database.	With the assistance of the senior programmer/analyst, attempted to delete a student record and enrollment record from the application using the ODE Exec and User roles.	No exceptions noted.
The community school Full Time Equivalency (FTE) is automatically calculated by the system based on the total units assigned to the community school.	Using a third-party software tool (ACL), recalculated the community school FTEs for test entities from an ODE snapshot to confirm the FTE amount was computed accurately.	No exceptions noted.

Community School – Average Daily Membership - *Control Objective:* **Restricted Access to Assets and Records:** Only authorized personnel have access to the CSADM data.		**Control Objective Has Been Met**
Control Procedures:	Test Descriptions:	Test Results:
User access to the CSADM application menus is segregated by assignment of user security roles.	Inspected CSADM menus accessible by each role in the development system to confirm user roles segregated access to the application.	No exceptions noted.
The CSADM database is restricted to programmers only. Access to the database requires specific user ID and password.	Inspected the listing of windows users with access to the CSADM database and confirmed the appropriateness of users' access with the senior programmer/analyst.	No exceptions noted.

<table>
<tr><td colspan="3"><b>Community School – Average Daily Membership</b> - <i>Control Objective:</i>
<b>Restricted Access to Assets and Records:</b> Only authorized personnel have access to the CSADM data.</td><td><b>Control Objective Has Been Met</b></td></tr>
<tr><td>Control Procedures:</td><td>Test Descriptions:</td><td colspan="2">Test Results:</td></tr>
<tr><td colspan="4"><b>User Control Consideration:</b>
User management should review users, user roles, assigned entities, and access levels at least yearly to ensure users are current employees and require the granted access to perform their job responsibilities.</td></tr>
</table>

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

INFORMATION TECHNOLOGY CENTER PROFILE
OHIO EDUCATION COMPUTER NETWORK

SITE DATA

Site Name:	Northwest Ohio Computer Association (NWOCA)
Site Number:	7
Node Name:	NWOCAC
Site Chairperson:	John R. Kaylor Superintendent Northwest Ohio ESC
Fiscal Agent:	Northern Buckeye Education Council
Site Administrator:	John R. Mohler Executive Director NWOCA
Address:	22-900 SR 34 Archbold, OH 43502
Telephone:	419-267-5565
FAX:	419-267-5248
Website	www.nwoca.org

OTHER SITE STAFF

Catherine Aldrich	Database administrator, SSDT
Andrea Bachman	Network/system support specialist
Duane Baker	Director of planning and research
Jodi Becher	Programmer/analyst, SSDT
Eric Bell	Technical projects manager
Andrea Boehm	Support specialist/technical writer, SSDT
Jason Bolbach	Hardware technician
Lori Burcham	Student services coordinator
Tammy Butler	Assistant to treasurer
Matthew Calmes	Systems analyst, SSDT
Julie Dicesare	Programmer/analyst, SSDT
Melissa Diemer	Systems analyst, SSDT
Michelle Drewes	Support specialist/technical writer, SSDT
Darren Estelle	Student services supervisor
Joseph Ferrall	Sr. programmer/analyst, SSDT
Debra Follett	Insurance programs specialist
Deborah Ford	Fiscal services coordinator
Cynthia Francis	Programmer/analyst, SSDT
Samuel Freeborn	EMIS/student services coordinator
Robin Fronk	Programmer/analyst
Sara Glore	Support specialist/technical writer, SSDT
Cory Goldfuss	Network/system support specialist
Carolyn Graf	NWOCA projects manager
Andy Hoiles	Programmer/analyst, SSDT
Dan Holden	Director of instructional services
Sandy Houck	MCOECN project coordinator
Kristen Hughes	Educational technologist
Jill Jacoby	Assistant to director
Ezequiel Juarez	Sr. programmer/analyst, SSDT
John Kern	Hardware technician
Jason Klinger	Programmer/analyst, SSDT
Karen Koch	Insurance programs clerk
Tami Kunesh	Student services coordinator, SSDT
Mike Kwiatkowski	Network/system support specialist
Eric Lammers	Project manager – eSIS/SPED
Julianne Lange	Educational technology specialist
Jean Lee	Student services coordinator
John Mansel-Pleydell	Educational technologist
Jennifer McCreight	Administrative assistant
Crystal Meyer	Insurance programs administrator
Kyle Miller	Programmer/analyst, SSDT
Lori Miller	Support specialist/technical writer, SSDT
Scott Mitchey	Programmer/analyst, SSDT
Mark Near	Database administrator
Angie Nofziger	Helpdesk technician
Kim Olson	Programmer/analyst, SSDT
John Overberg	Programmer/analyst, SSDT
Michelle Pfrogner	eSis implementation consultant
Robin Pfund	Assistant treasurer, NBEC/NWOCA
Linda Pohto	Student services coordinator, SSDT
Joe Prchlik	Network/systems services director
Dennis Reinhart	EMIS/student services coordinator
Tim Remster	Regional consultant, SSDT
Wendy Root	Sr. programmer/analyst, SSDT
Amy Jo Rouleau	Part-time systems analyst, SSDT
Travis Sheaffer	Network/system support specialist
Ryan Shively	EMIS/student services coordinator
Robert Slater	Programmer/analyst, SSDT
Dave Smith	Programming services director, SSDT
Lucas Swartz	Hardware technician
Judy Swerline	INFOHIO/educational technologist
Sean Taylor	EMIS/student services coordinator
Teresa Williams	Systems analyst, SSDT

HARDWARE DATA

Central Processors and Peripheral Equipment

CPU Unit 1

Model Number		Installed		Capacity/Density/Speed	
CPU:	HP Alpha Server ES45	Lines/Ports:	N/A	Memory Installed:	32.0 GB
Disk:	RZ1DF-VW	Units:	4	Total Capacity:	36.4 GB
Disk:	RZ1ED-VW	Units:	24	Total Capacity:	36.4 GB
Disk:	251872-002	Units:	40	Total Capacity:	1.45 TB
Tape Unit:	TZ891	Units:	1	Max Density:	N/A
Tape Unit:	TZ87	Units:	1	Max Density:	N/A
Printer:	HP8150	Units:	6	Print Speed:	32 PPM
Printer:	LG06	Units:	1	Print Speed:	600 LPM
Printer:	LG05	Units:	1	Print Speed:	500 LPM

CPU Unit 2

Model Number		Installed		Capacity/Density/Speed	
CPU:	HP Proliant DL560	Lines/Ports:	N/A	Memory Installed:	4.0 GB
Disk:	SCSI	Units:	2	Total Capacity:	300 GB
Tape Unit:	N/A	Units:	N/A	Max Density:	N/A
Printer:	N/A	Units:	N/A	Print Speed:	N/A

MEMBER USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
146706	Ayersville LSD	Defiance	X	X	X	X
046714	Central LSD	Defiance	X	X	X	X
043839	Defiance CSD	Defiance	X	X	X	X
045419	Hicksville EVSD	Defiance	X	X	X	X
046722	Northeastern LSD	Defiance	X	X	X	X
047043	Archbold-Area LSD	Fulton	X	X	X	X
047050	Evergreen LSD	Fulton	X	X	X	X
047068	Gorham Fayette LSD	Fulton	X	X	X	X
124297	Northwest Ohio ESC	Fulton	X	X	X	X
047076	Pettisville LSD	Fulton	X	X	X	X
047084	Pike-Delta-York LSD	Fulton	X	X	X	X
047092	Swanton LSD	Fulton	X	X	X	X
045641	Wauseon EVSD	Fulton	X	X	X	X
050963	Four County Career Center	Henry	X	X	X	X
047571	Holgate LSD	Henry	X	X	X	X
047589	Liberty Center LSD	Henry	X	X	X	X
044438	Napoleon CSD	Henry	X	X	X	X
047597	Patrick Henry LSD	Henry	X	X	X	X
048207	Anthony Wayne LSD	Lucas	X	X	X	X
048199	Lucas County ESC	Lucas	X	X		X

MEMBER USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
044362	Maumee City	Lucas	X	X	X	X
044602	Oregon City	Lucas	X	X	X	X
048215	Ottawa Hills LSD	Lucas	X	X	X	X
048223	Springfield LSD	Lucas	X	X		X
044875	Sylvania LSD	Lucas	X	X	X	X
048231	Washington LSD	Lucas	X	X		X
043679	Bryan CSD	Williams	X	X	X	X
050617	Edgerton LSD	Williams	X	X	X	X
050625	Edon-Northwest LSD	Williams	X	X	X	X
050633	Millcreek-West Unity LSD	Williams	X	X	X	X
045526	Montpelier EVSD	Williams	X	X	X	X
050641	North Central LSD	Williams	X	X	X	X
050658	Stryker LSD	Williams	X	X	X	X
049866	Lake LSD	Wood	X	X		X
050724	Otsego LSD	Wood	X	X	X	X
051359	Penta Co. JVS	Wood	X	X		X
050666	Wood County ESC	Wood	X	X		X
			37	37	31	37

OTHER USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
000613	Heir Force Community School	Allen	X	X		X
000825	Horizon Science Academy of Springfield	Lucas				X
000417	Buckeye Online School of Success	Columbiana	X	X		X
133900	Academy of Cleveland	Cuyahoga				X
000560	Apex Academy	Cuyahoga				X
133215	The Intergenerational School-Cleveland	Cuyahoga	X	X		X
009150	Lakeside College Preparatory Academy	Cuyahoga				X
000677	New Day Academy	Cuyahoga				X
000543	Pinnacle Academy	Cuyahoga				X
143610	The Arts and College Preparatory-Columbus	Franklin	X	X		X
000343	Chase Academy for Communication Art	Franklin				X
000779	Educational Academy for Boys & Girls	Franklin	X	X		X
000777	Educational Academy at Linden	Franklin	X	X		X
133413	Electronic Classroom of Tomorrow	Franklin	X			X
000780	Midnimo Cross Cultural Community	Franklin	X	X		X
008281	South Scioto Academy	Franklin				X
143636	W. C. Cupe	Franklin	X	X		X
009154	Cincinnati Leadership Academy	Hamilton				X
143602	Hamilton County Mathematics & Science	Hamilton	X			X

OTHER USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
000576	King Academy	Hamilton	X	X		X
000559	Orion Academy	Hamilton				X
134262	Academy of Business & Technology-Toledo	Lucas				X
000139	The Alliance Academy of Cincinnati	Hamilton				X
133447	Alliance Academy of Toledo	Lucas				X
134148	Aurora Academy-Toledo	Lucas	X	X		X
143297	The Autism Academy of Learning	Lucas	X	X		X
000843	Bennett Venture Academy	Lucas				X
009162	Bridge Academy of Ohio	Lucas				X
009164	Central Academy of Ohio	Lucas				X
143552	Eagle Academy-Toledo	Lucas				X
008289	Eagle Learning Center	Lucas	X			X
142976	Englewood Peace Academy	Lucas	X	X		X
000143	George A. Phillips Academy	Lucas				X
000131	Glass City Academy	Lucas	X	X		X
009147	Great Lakes Environmental Academy	Lucas				X
000338	Horizon Science Academy of Toledo	Lucas				X
143503	Lake Erie Academy	Lucas				X
000770	Maritime Academy of Toledo	Lucas	X	X		X
134171	Meadows Choice Community School-Toledo	Lucas	X	X		X

OTHER USER ORGANIZATION SITE DATA

IRN	USER ORGANIZATION	COUNTY	USAS	USPS	SAAS	EMIS
134122	MODEL Community School-Toledo	Lucas	X	X		X
148973	Paul Laurence Dunbar Academy	Lucas				X
133926	Performing Arts School of Metro Toledo	Lucas				X
000743	Pschtecin Public	Lucas	X	X		
009171	Star Academy of Toledo	Lucas				X
133975	Toledo Academy of Learning	Lucas	X	X		X
143545	Toledo Accelerated Academy-Toledo	Lucas				X
133942	Toledo School for the Arts	Lucas	X	X		X
000140	Victory Academy	Lucas	X	X		X
000222	Wildwood Environmental Academy	Lucas				X
000546	Winterfield Academy	Lucas				X
000855	Stambaugh Academy	Mahoning				X
133918	Academy of Dayton	Montgomery				X
000577	Emerson Academy of Dayton	Montgomery				X
143529	North Dayton School of Discovery-Dayton	Montgomery				X
000138	Pathway School of Discovery	Montgomery				X
TOTALS:			**21**	**20**	**0**	**52**

Mary Taylor, CPA
Auditor of State

NORTHWEST OHIO COMPUTER ASSOCIATION
(NWOCA)

HENRY 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
AUGUST 7, 2008