



JIM PETRO
AUDITOR OF STATE

STATE OF OHIO

TABLE OF CONTENTS

I	REPORT OF INDEPENDENT ACCOUNTANTS	1
II	ORGANIZATION'S DESCRIPTION OF CONTROLS	3
	CONTROL OBJECTIVES AND RELATED CONTROLS	3
	OVERVIEW OF OPERATIONS	3
	RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND	
	MONITORING	3
	Control Environment.....	3
	Risk Assessment.....	5
	Monitoring.....	5
	INFORMATION AND COMMUNICATION	5
	GENERAL EDP CONTROLS.....	6
	Development and Implementation of New Applications and Systems	6
	Changes to Existing Applications and Systems	6
	IT Security	7
	IT Operations.....	11
III	INFORMATION PROVIDED BY THE SERVICE AUDITOR	14
	GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING	
	EFFECTIVENESS.....	15
	Changes to Existing Applications or Systems.....	15
	IT Security	17
	IT Operations.....	29
IV	OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION	34
	DATA ACQUISITION SITE PROFILE	34

This Page Intentionally Left Blank



STATE OF OHIO
OFFICE OF THE AUDITOR

JIM PETRO, AUDITOR OF STATE

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

REPORT OF INDEPENDENT ACCOUNTANTS

Board of Directors
Southeastern Ohio Voluntary Education Cooperative (SEOVEC)
221 North Columbus Road, P.O. Box 1250
Athens, OH 45701

To Members of the Board:

We have examined the accompanying description of controls of the Southeastern Ohio Voluntary Education Cooperative (SEOVEC) 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), and Education Management Information System (EMIS). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the SEOVEC's controls that may be relevant to a member school district's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and member school districts applied the internal controls contemplated in the design of the SEOVEC's controls; and (3) such controls had been placed in operation as of April 26, 2002. The control objectives were specified by the SEOVEC management for the processing of USAS, USPS, SAAS/EIS, and EMIS with the assistance of the Ohio Department of Education. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of the SEOVEC's controls that had been placed in operation as of April 26, 2002. 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 member school districts applied the controls contemplated in the design of the SEOVEC'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 19, 2001 to April 26, 2002. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to member school districts of the SEOVEC and to their auditors to be taken into consideration along with information about the internal control at member school districts, when making assessments of control risk for member school districts. In our opinion, 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 19, 2001 to April 26, 2002.

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

The information in Section IV describing the data acquisition site is presented by the SEOVEC to provide additional information and is not part of the SEOVEC's description of controls that may be relevant to a user organization's internal control. Such information has not been subjected to the procedures applied in the

examination of the description of the controls applicable to the processing of transactions for member school districts and, accordingly, we express no opinion on it.

The description of controls at the SEOVEC is as of April 26, 2002, and information about tests of the operating effectiveness of specified controls covers the period from May 19, 2001 to April 26, 2002. 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 SEOVEC 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 SEOVEC, its member school districts, and the independent auditors of its member school districts.

A handwritten signature in black ink, appearing to read "Jim Petro", with a large, stylized flourish at the end.

JIM PETRO
Auditor of State

April 26, 2002

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The SEOVEC'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 SEOVEC's description of controls.

OVERVIEW OF OPERATIONS

The SEOVEC is a computer service organization whose primary function is to provide information technology services to its member school districts with major emphasis being placed on accounting, payroll and inventory control services. The SEOVEC is a council of governments (COG) which exists to foster cooperation among its member school districts in all areas of educational service. Currently, there are 30 member school districts in the Ohio counties of Athens, Gallia, Hocking, Jackson, Meigs, Morgan, Perry and Washington. The SEOVEC is located in Athens, Ohio.

The SEOVEC is one of 23 not-for-profit computer service organizations serving more than 600 public school districts and county educational service centers in the State of Ohio. Throughout the remainder of this report, any reference to member school districts will also include the county educational service centers. These service organizations, known as Data Acquisition Sites (DA Site) and their member school districts 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 school districts. Funding for this network and for the SEOVEC is derived from the State of Ohio and from user fees.

Per section 3301.075 of the Ohio Revised Code, each DA Site must be organized in accordance with either section 3313.92 or Chapter 167 of the Revised Code. The SEOVEC was organized in accordance with Chapter 167, and is required to have a board of education serve as its fiscal agent to receive State network funds and make equipment purchases from these funds. For this reason, the Logan-Hocking Local School District of Hocking County serves as fiscal agent for the SEOVEC and performs certain functions that might otherwise be performed by the council in order to verify receipt of funds from the OECN. Essentially, these functions are to apply for and maintain the DA Site permit for the central data processing equipment purchased with state monies and to hold legal title to this equipment.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

Operations are under the control of the Director of Computer Services, Chief Executive Officer and the SEOVEC Authorized Representatives. The SEOVEC is a council of governments which exists to foster cooperation among its member school districts in all areas of educational service.

The Authorized Representatives is the legislative body of the SEOVEC and consists of the superintendent or designee from each member school district. They meet once a year, and other times if necessary, to estimate program costs, to approve annual appropriations, to select officers and other members of the council and to approve other matters as determined to require approval. The Authorized Representatives elect the Governing Board, which is the governing body of SEOVEC, from amongst their members.

The Governing Board meets bi-monthly and is composed of one superintendent from each of the Counties of Athens, Gallia, Hocking, Jackson, Meigs, Morgan, Perry, and Washington, the SEOVEC Director of Computer Services and the SEOVEC Chief Executive Officer. The Board elects a Chairperson and Vice-Chairperson to serve as officers of the SEOVEC and preside at meetings of the Authorized Representatives, in addition to the meetings of the Governing Board. The Board has established several operating sub-committees. These committees work along with the Governing Board and the Director of Computer Services to provide oversight and planning for the organization.

The SEOVEC employs a staff of 14 individuals and consists of 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 district needs additional assistance for a period of time. Also provides support in all aspects of the InfoOhio program.
- 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.
- Network/Systems Support:* Supports the SEOVEC 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 Computer Services.

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

The SEOVEC follows personnel policies and procedures as outlined in the SEOVEC-COG Handbook. When necessary, additional SEOVEC policies are developed and approved by the Governing Board to address concerns of SEOVEC. Detailed job descriptions exist for all positions. The SEOVEC is constantly re-evaluating its need for personnel to provide for the increasing range of services provided. The reporting structure and job descriptions are periodically updated to create a more effective organization.

The SEOVEC hiring practices place an emphasis on the hiring and development of skilled information technology professionals. Most positions within the organization require some type of college degree or experience in a computer-related field, and all the SEOVEC 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. All the SEOVEC staff members are permitted and encouraged to attend professional training as deemed necessary. Management conducts staff evaluations annually. In addition, the Board performs an annual evaluation of the Director of Computer Services.

Risk Assessment

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

- new technology
- realignment of the SEOVEC organization to provide better service
- personnel issues, including hiring, termination, and evaluations
- additional services provided to member school districts and other entities
- changes in the operating environment as a result of ODE requirements, Auditor of State (AOS) and other accounting pronouncements and legislative issues

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

Monitoring

The SEOVEC organization is structured so that department managers report directly to the Director of Computer Services. Key management employees have worked here for many years and are experienced with the systems and controls at the SEOVEC. The SEOVEC Director of Computer Services and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, SEOVEC 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 are automatically run through a scheduler program and sent to management via e-mail. Exceptions to normal processing related to hardware, software or procedural problems are logged and resolved daily. In addition, the Assistant Director of Computer Services receives the same reports and monitors for interrelated and recurring problems.

INFORMATION AND COMMUNICATION

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

GENERAL EDP CONTROLS

Development and Implementation of New Applications and Systems

There are no system development activities performed by SEOVEC personnel. Instead, SEOVEC utilizes the software supplied by the State Software Development Team (SSDT) at the Northwest Ohio Computer Association (NWOCA), which is another DA Site of the OECN. The ODE determines the scope of software development for state-supported systems. Tactical means of accomplishing the priorities are determined by the Software Advisory Committee (SAC), which consists of members from the Management Council of the OECN (MCOECN), the Ohio Association of School Business Officials, the ODE and the SSDT. The SAC meets four times per year to discuss the status of proposed and ongoing projects.

Changes to Existing Applications and Systems

End-users participate in the program development/change process via the Software Performance Report/Request (SPR) tracking procedure, which is maintained by the SSDT. The SPR system utilizes SiteScape Forum, which is used for electronic conferencing, to accept and discuss proposed software enhancements in a public forum. Each major software package (USAS, USPS, SAAS, EMIS) has its own Public and DA Site forum which is monitored by the SSDT system analysts. All OECN DA Sites and a majority of member school districts have access to Forum conferences, providing end-user participation in the program development/change process.

The SEOVEC personnel do not perform program maintenance activities. Instead, they utilize the applications supplied to them by the SSDT. The OECN requires the DA Site to keep the version of each application current based on the provider's standard for continued support. Procedures are in place to ensure the SSDT developed applications are used as distributed. The SSDT, at NWOCA, copies zipped files containing the quarterly updates to the DA Sites' systems. Source code is not distributed with these files. Release notes are contained within these files and explain the changes, enhancements and problems corrected. User and System Manager manuals are also distributed with these releases. The SSDT informs the DA Sites that they will support only the latest release of the state software beginning 30 days following the software release date.

The SEOVEC uses a software utility called OECN_INSTALL to unpack these zipped files and install each individual package into its proper OECN directory. A second software utility, called INSTALL_PACKAGE, is then used to actually install the new releases on the system. Additionally, there is a third utility called INSTALL_PACKAGE_PATCH, which is used when a patch is needed for a current release. These utilities ensure that all required components are installed properly and consistently.

Only vendor supplied changes are made to the operating system or system software documentation. The Northern Buckeye Education Council (NBEC), who acts as the fiscal agent for this and other participating DA Sites, 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 to the participant for a limited series of HP software packages as approved by the Board of Trustees of the MCOECN.
- Provide telephone technical support to the participant's technical staff for a limited series of HP software packages approved by the Board of

Trustees of the MCOECN.

- Track and maintain an accurate listing of all HP hardware and software covered under the agreement.
- Provide periodic training and update sessions covering the policies and regulations governing this program as well as updating the DA Sites' 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 DA Sites 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.

Before new releases are installed, a backup of the application receiving the change or the operating systems would be performed to ensure that a copy of the old application or operating system was maintained in case of an error.

The NBEC provides documentation and support for new releases of the operating system to all the DA Sites. The releases document changes to the operating system and contain implementation procedures. The NBEC puts the OpenVMS documentation on the OECN web site, for the current version of the operating system. In addition, the SEOVEC has purchased their own copy of the operating system disks from NWOCA via the MCOECN Value-Added Reseller (VAR) program. Through the VAR program, SEOVEC is able to purchase the operating system software at a reduced amount. The current release documentation is maintained by the Assistant Director of Computer Services at SEOVEC.

IT Security

The SEOVEC has a security policy that outlines the responsibilities of member school district personnel, the SEOVEC personnel, and any individual or group not belonging to the member school district or the SEOVEC. In addition to the security policy, the SEOVEC utilizes a banner screen, which is displayed when a user logs on to the system. The screen informs the user that unauthorized access of the system is prohibited and individuals using this computer system are subject to having their activities monitored by the SEOVEC personnel.

The SEOVEC staff are granted access within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities. Access is established, granted and reviewed by the Director of Computer Services and no authorization form is used.

Users from the member school districts are granted access upon the receipt of authorization (e-mail, fax, or phone call) from the member school district's superintendent, treasurer, EMIS Coordinator or Technology Coordinator. These requests are then sent to an e-mail list and one of the SEOVEC staff

members, on the list, creates, update, or delete the account(s). A reply is sent via e-mail, acknowledging the request has been implemented; a copy of this reply is also sent to the e-mail list for SEOVEC's records.

SEOVEC sends out an annual listing, which indicates user access and privileges within the school district, to the respective superintendents, treasurers, technical coordinators or other designee, to ensure the present users on the system have the correct access and were properly authorized. Positive confirmation by the school district's authorized representative is required to ensure user access is accurate. The majority of the requests are returned via e-mail; however, they can come back in written form or verbally from the appropriate district management.

Access to the Internet has been provided to the member school districts of the SEOVEC. Access is provided through the OECN GOSIP network and routed to SEOVEC. No centralized Internet acceptable use policy is used at the SEOVEC. Each member school district is responsible for their own Internet usage policies.

Security audit messages are sent to the audit log file. Access to the 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 audits have been enabled through OpenVMS to monitor any security violations:

- ACL: Gives file owners the option to selectively alarm certain files and events. READ, WRITE, EXECUTE, DELETE, or CONTROL modes can be audited.
- AUTHORIZATION: Enables monitoring of changes made to the system UAF or network proxy authorization file in addition to changes to the rights database.
- AUDIT: Enabled by default to produce a record of when other security alarms were enabled or disabled.
- BREAK-IN: Produces a record of break-in attempts. The DIALUP, LOCAL, REMOTE, NETWORK, DETACHED, and SERVER break-in types can be monitored.
- INSTALL: Enables monitoring of modifications made to the known file list through the Install utility.
- LOGFAILURE: Provides a record of logon failures. The BATCH, DIALUP, LOCAL, REMOTE, NETWORK, SUBPROCESS, DETACHED, and SERVER logon failure types can be monitored.
- MOUNT: Enables monitoring of volume mounts and dismounts.

A batch processed command procedure executes each night to extract security violations from the audit log and compiles them into two separate reports. These reports, also called Security Monitor Reports, are e-mailed to the Assistant Director of Computer Services 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 SEOVEC utilizes Sophos Anti-Virus software on the Alpha server to scan all inbound and outbound e-mail. If a virus is found, the e-mail is quarantined and the recipient and the SEOVEC staff are sent e-mails informing them of the infected e-mail.

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

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

The User Identification Codes (UIC) are individually assigned to all data processing personnel employed at the SEOVEC. For member school districts which use the SEOVEC system, UICs are for the most part, functionally assigned and therefore, multiple district users may share an individual UIC. UICs are assigned at the member school district's request. UIC based protection controls access to objects such as files, directories, and volumes.

The system forces users to periodically change their passwords. The majority of the accounts have a password lifetime of 90 days and the remaining accounts have a password lifetime of 180 days. These accounts were setup for users of the student program and the Director of Computer Services would like their password change interval to correspond 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 (masking the account with the pre-expired parameter PWDEXPIRE) 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. The minimum password length for each user is typically the default of ten.

The operating system uses SYSGEN parameters to control and monitor logon attempts. The following is a brief description of how these parameters function:

LGI_BRK_TERM:	Determines whether the terminal name is included with the user name when counting possible break-in attempts.
LGI_BRK_DISUSER:	Determines whether the DISUSER flag will be set to disable an account after the system detects a break-in attempt.
LGI_PWD_TMO:	Determines the amount of time a user has to enter the system password correctly on a terminal on which the system password is in effect.
LGI_RETRY_LIM:	Determines the number of retry attempts allowed for users attempting to login over dialup lines before the system terminates the connection.
LGI_RETRY_TMO:	Determines the length of time allowed between login retry attempts after each login failure.
LGI_BRK_LIM:	Determines the number of failures that can occur at login time before the system takes evasive action against a possible break-in.
LGI_BRK_TMO:	Determines the length of time to attempt a login before the system assumes that a break-in attempt is occurring and evasive action is required.

LGI_HID_TIM: Determines the length of time the system will refuse any new login attempts after the detection of a possible break-in attempt, even if using a valid user name and password.

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

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

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

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

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

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

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

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 member school district users have NORMAL privileges.

The WRITE and DELETE access capabilities are not activated for WORLD access to the files in the SYS\$SYSTEM directory. The UIC associated with

each of these files is within the MAXSYSGROUP number.

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

Access to the OECN software packages is controlled at the DA Site 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.

Member school districts have been set up with sub-networks which have addresses not recognizable to the Internet. This is called a private internal network. When a request is made from within the network, a true IP address is assigned. The Cisco PIX (Private Internet Exchange) firewall equipment and additional routing devices deny all incoming traffic access to the inside servers and nodes unless the request originated from the sub-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. The Cisco PIX box and routers also prevent all outside connections (traffic) from accessing inside hosts or servers, unless the IP address originated from inside the network.

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

The following items assist in protecting the computer room and its equipment from adverse environmental conditions:

- Fire extinguishers
- Smoke detectors
- 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
- Air conditioning
- Raised floor
- UPS to provide conditioned power during brownout or power surge conditions and short-term power during power outages

IT Operations

Traditional computer operations procedures are minimal since users at the member school districts initiate all application jobs and are primarily responsible for ensuring the timeliness and completeness of processing. All SEOVEC employees have a procedures manual, which provides directions and guidelines for most of the operational functions performed. They also have access to operations procedure manuals for the Alpha system. In addition, all users, except students, have access to SiteScape Forum, which is a bulletin board that allows the SEOVEC employees to communicate with users across the state. Users can post questions and/or comments to the SEOVEC staff.

User problems that require the SEOVEC staff to change data require the authorization from the member school district. Member school districts are encouraged to review the "AUDIT" report, which shows all activity changes to their data files.

Certain routine jobs are initiated for system maintenance. SEOVEC is responsible for operational maintenance tasks, such as system backups, source code rebuilds, log reports, and other maintenance directed at the whole system. They use an automated procedure called ADMIN_OVERNIGHT, which schedules and performs these tasks. The ADMIN_OVERNIGHT procedure was created by the Director of Computer Services and it re-submits itself every night.

Common problems that arise daily, such as terminal lockups and program crashes, are usually handled by the SEOVEC service representatives over the phone and may not be documented. However, most problems are still logged through their on-line help desk application. Status reports are printed periodically and reviewed by the Director of Computer Services and the technical staff to determine when the problems that are still open will be resolved. The console log is reviewed by the Director of Computer Services on a periodic basis and is used to investigate problems that occur during operation of the system.

A hardware maintenance agreement exists with HP, and is paid annually.

The SEOVEC helps prevent file corruption through the use of a command procedure program which runs through ADMIN_OVERNIGHT. All files are scanned to verify that they are readable (e.g., no bad blocks, sectors or chains). Data integrity is maintained by the software through validity checks of all input.

Network and Internet traffic is monitored on a regular basis. A procedure runs during the day to 'ping' each router to see if they are functioning. Other tools are used to monitor traffic on the routers and firewall. These are typically used for trouble shooting purposes only. The Bess system compiles performance reports which are sent daily to the Network Technical Coordinator via e-mail. These reports are monitored to make sure the proxy servers are operating properly and can handle the volume of requests being made.

The SEOVEC has documented procedures for how to back up and restore all system data and programs. An Alpha Server 8200 is used by the SEOVEC for production. Full system backups are performed daily for the computer system. The backup tapes are documented in a backup log and system backup logs from each backup are maintained. Daily backups, from the Alpha, are maintained for at least three weeks. All system backup tapes are rotated off-site each morning by the System Operations Supervisor. The oldest tape is pulled and brought back on-site to be reused. The only tape kept overnight is the most recent daily backup tape. All other backups (daily, monthly, quarterly, annually, and demand) are stored off-site at the Athens-Meigs Educational Service Center (ESC). The off-site tapes are stored in a locked cabinet to which only the SEOVEC had access. The SEOVEC also had keys for the building and ESC office doors to ensure tapes were accessible at all times.

All data required by law to be maintained for a specific duration is maintained by the SEOVEC. Calendar year and fiscal year end information is stored indefinitely for all the SEOVEC member school districts.

The SEOVEC maintains a Disaster Recovery Plan to be followed to help minimize disruption of services to their school districts if a disaster should occur. SEOVEC has a written reciprocal agreement with the South Central Ohio Computer Association (SCOCA) and a verbal reciprocal agreement with Ohio Mid-Eastern Regional Education Service Agency (OME-RESA). There is an official agreement with SCOCA and it is included in the disaster recovery plan. There is no official agreement with OME-RESA, but the Director stated, their verbal agreement has been in place for the past several years.

The SEOVEC Disaster Recovery Plan includes the following:

- SEOVEC Responsibilities
- User Responsibilities
- Recovery Plan
- Priority Usage List
- Contact List (HP Contact Personnel, Communications Equipment Vendors, member school districts, etc.)
- SEOVEC Hardware Topology

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

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 SEOVEC'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 SEOVEC and procedures performed at member school districts that utilize the SEOVEC.

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

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS***Changes to Existing Applications and Systems***

Changes to Existing Applications and Systems - Control Objective: Change Requests - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Authorized application updates are distributed quarterly by the SSDT and installed by SEOVEC.	To help ensure the SSDT approved USAS, USPS, SAAS/EIS and EMIS application software is the version being utilized at the SEOVEC, a cyclical redundancy check (CRC) of the object program files at the SEOVEC was compared to the CRCs of the latest ODE version approved & tested by the SSDT. (March 2002).	<p>The CRCs of the object code for the USPS, SAAS/EIS and EMIS applications at the SEOVEC were the same as the CRCs of the object code from the SSDT. Two exceptions were noted for USAS, the ADJUST and the POFORM files.</p> <p>The SEOVEC changed the file name to STATE_ADJUST; however, the file length was the same. SSDT allows the DA Sites to change the name of the files, if it is necessary.</p> <p>In addition, the POFORM file has been modified to reflect customized changes specific to SEOVEC due to differences in purchase order forms. This exception was expected because this file is customizable.</p>
The SSDT distributes documentation explaining any changes, enhancements and/or problems corrected to the DA Site quarterly.	<p>Obtained and reviewed release notes and updated manuals for the most recent release from the Assistant Director of Computer Services.</p> <p>Also visited the SSDT web-site for availability of updated manuals for the most recent release to determine if all current documentation is provided to the SEOVEC.</p>	<p>Release notes are distributed to the SEOVEC and retained by the Assistant Director of Computer Services. The notes addressed revisions to the application(s) and affected processing procedures revised due to the changes.</p> <p>The SEOVEC staff accessed the SSDT web-site as necessary for user manuals. From review of the web-site, user manuals were available and based on the index, it appeared that significant volumes of support manuals were available to users and updated regularly.</p>

Changes to Existing Applications and Systems - Control Objective: Change Requests - Management should be involved in monitoring changes/upgrades to existing applications or systems to ensure they operate as intended.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The SEOVEC participates in the CSLG/ESL program for system software support	Obtained and reviewed a copy of the SEOVEC's CSLG licensing agreement with the NBEC and payment information to determine if it is current. Reviewed the online documentation and discussed this with the Assistant Director of Computer Services to determine if the SEOVEC is provided with the most current documentation for the operating systems	<p>The current agreement and payment information verified that the SEOVEC is a participating member of the OECN CSLG program for its system software for the period of July 1, 2001 through June 30, 2002.</p> <p>SEOVEC updated their operating system in April 2002.</p> <p>Online documentation does exist for the most recent version of the operating system and is put on the OECN website by the NBEC. The SEOVEC staff has access to the online documentation.</p> <p>In addition, the SEOVEC purchased their own set of installation disks through NWOCA. They also have documentation on their installation disks.</p>

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Member school districts are requested to confirm user accounts once a year.	Obtained and reviewed a copy of the confirmation memo sent to each member school district by the Assistant Director of Computer Services. Obtained and reviewed each report to determine if the member school districts responded to the memo to confirm user access rights.	The SEOVEC utilizes a "positive" confirmation process. Confirmation of user accounts is an on-going process throughout the year. Review of the reports showed all districts, except for one, returned their list to the Assistant Director of Computer Services. All of the returned reports showed some indication the district had reviewed it, whether it was signed or corrections were made.
A banner screen is displayed upon user login to help deter unauthorized access.	Obtained and reviewed a printout of the banner screens for content. Also obtained and reviewed the SYSTARTUP_VMS.COM printout to determine if it is displayed at login.	The banner screen is part of the SEOVEC logicals in the SYSTARTUP_VMS.COM, so it is displayed upon user login. It states that "unauthorized use may result in denial of future privileges, revocation of access to the system, and/or prosecution under the law." It does not imply or state that anyone is "welcome" to use their system.
Security-related events are enabled through OpenVMS to monitor potential security violations.	Obtained and reviewed the security alarms and audits enabled from the Assistant Director of Computer Services via the DCL command SHOW AUDIT/ALL.	System security alarms have been disabled; however, security audits have been enabled for ACL, MOUNT, AUTHORIZATION, INSTALL, AUDIT, BREAKIN, and LOGFAILURE. The security audits are logged in the audit journal file.

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:
Security monitor reports are generated and reviewed daily.	Discussed security monitoring procedures with the Assistant Director of Computer Services. Obtained and reviewed the following information, relating to the Security Monitor reports, to determine if these reports are produced and reviewed daily: <ul style="list-style-type: none"> • example Security Monitor reports • command procedure utilized to generate the report • ADMIN_OVERNIGHT command procedure 	A procedure called NIGHT_AUD.COM runs nightly at 10:00 PM via the ADMIN_OVERNIGHT.COM procedure. It extracts all events from the audit journal since the previous report was created. These events (security violations) are compiled into two Security Monitor Reports. One report shows only security events. The other report shows login failures. These reports are automatically e-mailed to the Assistant Director of Computer Services. These reports are reviewed daily by the Assistant Director of Computer Services. He mainly looks for login failures, breakins, and changes to the SYSUAF.
Member School District User Control Considerations: Determine if district management makes users aware of the confidential nature of passwords and that the users should take precautions to ensure passwords are not compromised. Determine if district management requests the DA Site to revoke the access privileges of district personnel when they leave or are otherwise terminated. Verify if the member school district personnel are retaining signed copies of the authorization form for new user accounts or changes to existing accounts.		

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Individual user profiles are used to grant access rights and privileges.	<p>A batch file was created using security analysis tools to extract information from the SYSUAF.DAT file to determine if:</p> <ul style="list-style-type: none"> • user accounts exist that have not been used in at least 90 days • user accounts exist that have not been used in at least 180 days • user accounts exist that are flagged 'DISUSER' • user accounts have ELEVATED privileges; defined as those accounts having more than TMPMBX and NETMBX, which are the minimum privileges to use the system 	<p>There were 1,846 of 3,679 accounts that have not been logged in to in over 90 days. Of these, 21 are flagged as 'DISUSER' and 1,119 have never been used. Most of these accounts are MOLE accounts, which do not show any type of login activity because MOLE is a web-based application.</p> <p>There were 21 accounts flagged as 'DISUSER'. Most of the accounts are template accounts used to setup new access.</p> <p>There were 173 of 3,679 accounts with ELEVATED privileges. These accounts are either system accounts, application accounts or district system manager account.</p>
Use of wild card characters in NETPROXY accounts is limited.	Obtained the PROXY listing from the Assistant Director of Computer Services via the SH/PROXY command and reviewed the listing for use of wild card characters.	There were no wildcard (*) characters used in the PROXY listing.

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Access to the operating system command line (DCL) is restricted to authorized users.	A batch file was created using security analysis tools to extract and review user accounts, which do not have the AUDIT, CAPTIVE, DISCTLY, DISUSER or RESTRICTED flags set.	<p>There were 3,478 of 3,679 accounts that did not have the AUDIT, CAPTIVE, DISCTLY, DISUSER, or RESTRICTED flags. This represents approximately 95% of the accounts, which the Director of Computer Services stated were administrative accounts.</p> <p>This has been addressed in years past through the Computer Advisory Committee. The committee members felt these restrictions were not necessary for administrative users, as access to the DCL was essential for using the Alpha effectively.</p>

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
<p>Passwords are used to authenticate users before granting them access to the system.</p>	<p>A batch file was created using security analysis tools to extract information from the SYSUAF.DAT file to determine if:</p> <ul style="list-style-type: none"> • user accounts have password minimum lengths of at least 6 characters • user accounts have a password lifetime > 90 days • user accounts exist having pre-expired passwords • user accounts exist with last password change > 90 days 	<p>No accounts had passwords less than 6 characters in length.</p> <p>There were 14 user accounts with a password lifetime of 180, and 12 of these accounts were flagged 'DISUSER'. All other accounts, including administrative accounts, have password lifetimes of 90 days.</p> <p>There were 525 of 3,679 accounts that have pre-expired passwords and 15 of these were flagged 'DISUSER'. Some of these accounts consist of system accounts. The majority of these accounts were setup for users who need access to MOLE.</p> <p>There were 1,864 of 3,679 accounts that have not had the password changed in the past 90 days. Of these, 515 accounts have had at least 1 password change, 1,349 accounts have pre-expired passwords, and 21 accounts are flagged 'DISUSER'.</p>
<p>Log-in parameters have been set to control and monitor sign-on attempts.</p>	<p>Using the OpenVMS System Generation (SYSGEN) Utility, the Assistant Director of Computer Services printed the OpenVMS Login parameters via the SHOW /LGI command. Parameters were reviewed for appropriateness.</p>	<p>Parameters have been set and controls are in place to address sign on attempts and sign on constraints for break-in detection and evasion. All of these parameters are consistent with the recommended defaults.</p>

<p>IT Security - Control Objective: System Level Access Controls - Access to the computer system, programs, and data should be appropriately restricted.</p>		<p>Control Objective Has Been Met</p>
<p><i>Control Procedures:</i></p>	<p><i>Test Descriptions:</i></p>	<p><i>Test Results:</i></p>
<p>HITMAN monitors terminal activity and logs off inactive users.</p>	<p>Reviewed the HITMAN parameters to determine if they were set to automatically logoff inactive users.</p> <p>Also, looked at the SYSTARTUP_VMS.COM file to determine the HITMAN utility is part of the startup procedures.</p>	<p>HITMAN Prime hours are 7:00 am to 5:00 pm, Monday through Friday. First and second warnings are given at 150 minutes and 165 respectively, with processes being killed at 180 minutes of idle time. There were no protected UICs and the console was the only terminal that was protected. SYSTEM is the only user that is protected.</p> <p>HITMAN Non-Prime hours are 5:01 pm to 6:59 am, Monday through Friday and weekends. First and second warnings are given at 20 minutes and 25 minutes respectively, with processes being killed at 30 minutes of idle time. There were no protected UICs or users. The console was the only terminal that was protected. All system processes are protected. In addition, there were 8 holidays designated to be treated as Non-Prime.</p> <p>HITMAN is part of the daily start up procedure.</p>

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Access to production data files and programs is properly restricted.	<p>Obtained and reviewed a directory listing of the executable files for the USAS, USPS, EMIS and SAAS/EIS application programs from the Assistant Director of Computer Services to verify WORLD Access was limited to READ and/or EXECUTE.</p> <p>Also obtained and reviewed a listing of school district data files to verify there were no files having WORLD WRITE and/or DELETE access.</p>	<p>There were no USAS, USPS or SAAS executable files that had WORLD WRITE and/or DELETE access. There were two EMIS executable files having WORLD WRITE access. According to the Assistant Director of Computer Services, these files came from ODE with that access and SEOVEC installed them. The Assistant Director of Computer Services changed the WORLD access to these two files to READ and EXECUTE.</p> <p>There was one data file (CSSSCHO) that had WORLD READ, WRITE, and EXECUTE. This same data file was present in almost every district's data file listing. This appeared to be appropriate. No other data files had WORLD access.</p>

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
A private internal network and firewall are used to control Internet traffic.	<p>Obtained and reviewed the network diagrams with the Network Technical Coordinator to confirm components of the network which control Internet access.</p> <p>Also obtained and reviewed the PIX firewall configuration to determine that inbound and outbound IP traffic is restricted through the firewall. In addition, confirmed the existence of a private internal network.</p>	<p>Access to the Internet is provided through the use of a PIX firewall and a routing system to control traffic to and from the Internet.</p> <p>The SEOVEC uses a private internal network (sub-network) that requires an IP address to be picked up through the Cisco PIX box in order to access the Internet. All sub-networks have been denied access to the Internet. As a result, all traffic is forwarded to the proxy servers and filtered.</p> <p>All inbound and outbound traffic is controlled by the PIX firewall. By default all incoming traffic is denied access to the inside servers and nodes unless the request originated from the inside. Statements have been entered into the configuration to control the outgoing IP traffic and restrict what traffic enters the network.</p>

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Users are restricted to the applications necessary to perform their job function.	Discussed the OSA utility with the Assistant Director of Computer Services, and obtained a listing of all accounts with OECN identifiers for the USAS, USPS, SAAS/EIS and EMIS applications.	Identifiers are assigned at the OpenVMS level to each individual user accounts per the request of appropriate district personnel. Unusual requests, such as USPS access for a guidance counselor, would be confirmed with the same appropriate district personnel.
The OECN_SYSMAN identifier is restricted to only authorized users.	Obtained and reviewed a listing of all users having the OECN_SYSMAN identifier to determine if only authorized users have been assigned this identifier.	The OECN_SYSMAN identifier has been restricted to only authorized personnel. It was also noted that this identifier grants special privileges only to the OECN state software. It does not grant access to data.
Member School District User Control Consideration: Verify that User Identification Codes (UICs), passwords and associated access privileges are issued only 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 adequately controlled.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Access to "key" system files is restricted.	<p>Obtained the system file directory listing for the SYS\$SYSTEM and SYS\$MANAGER directories and reviewed the file protection masks for WORLD WRITE or DELETE access.</p> <p>In addition, reviewed the file protection masks on the SYSUAF.DAT, NETPROXY.DAT and RIGHTSLIST.DAT files to ensure there was no WORLD access.</p>	<p>There were no system files having WORLD WRITE and/or DELETE access.</p> <p>The data files, SYSUAF.DAT, NETPROXY.DAT, and RIGHTSLIST.DAT did not have WORLD access.</p>
System level UICs are restricted to authorized personnel.	<p>Through the OpenVMS System Generation (SYSGEN) utility used the SHOW MAXSYSGROUP command to determine the MAXSYSGROUP number.</p> <p>Used security analysis tools to obtain a listing of all accounts with a UIC < MAXSYSGROUP #.</p>	<p>The MAXSYSGROUP number is set at eight. Only 6 accounts have UICs less than this. All of these accounts are necessary system accounts. None of the accounts belong to actual users.</p>
The use of an alternate SYSUAF file is not permitted.	<p>Through the SYSGEN utility using the SHOW UAFALTERNATE command, determined whether or not the parameter's setting allows for the use of a non-existent SYSUAF file.</p> <p>Also reviewed the SYS\$SYSTEM directory listings to determine if an alternate SYSUAF file exists.</p>	<p>The value of the UAFALTERNATE is '0', which means the operator cannot specify another SYSUAF file other than the default (SYSUAF.DAT) during system startup.</p> <p>In addition, a SYSUAFALT file does not exist under the SYS\$SYSTEM directory.</p>

IT Security - Control Objective: System Software and Utilities Access Controls - Use of master passwords, powerful utilities, and system manager facilities, should be adequately controlled.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Remote administration of the firewall and routers used to control Internet access is restricted.	Reviewed the PIX firewall configuration to determine if passwords are required to access the routing equipment used to control Internet access and if remote access is allowed.	<p>Passwords are required to access both the inquiry and configuration modes. Remote operations are only possible from the sub network used by the SEOVEC. All SEOVEC hardware technicians have the passwords necessary to access the PIX; however, only the Network Technology Coordinator makes changes to the configuration file.</p> <p>From observations of login attempts, made into the firewall, found that passwords are required. If a null password is entered access is denied. Three attempts were allowed and then the Telnet connection is disconnected.</p>

<p>IT Security - Control Objective: Physical Security - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.</p>		<p>Control Objective Has Been Met</p>
<p><i>Control Procedures:</i></p>	<p><i>Test Descriptions:</i></p>	<p><i>Test Results:</i></p>
<p>Physical access to the computer room and its contents is restricted to authorized personnel.</p>	<p>Observed the key locks and use of them throughout the period of fieldwork. Observed the existence of motion detection devices and discussed the monitoring system with the Assistant Director of Computer Services.</p>	<p>All SEOVEC computer equipment is physically secured after business hours with regular door locks and protected with a security alarm system. The security system consists of motion detectors in every room, monitoring all points off access to the building.</p> <p>Employees have their own unique code to the security alarm.</p> <p>Only the SEOVEC staff members have keys to the building.</p>
<p>Environmental controls are in place to protect/detect against damage from fire, water, humidity, or changes in temperature.</p>	<p>Toured the computer room and observed the existence of the listed environmental controls.</p>	<p>A Liebert System is used to monitor and control the temperature and humidity in the computer room.</p> <p>Elevated flooring has been installed in the computer room to protect against water damage in case of flooding.</p> <p>In addition, the building has three fire extinguishers, one inside the computer room and two at either end of the data center. They were last tested in February 2001.</p>
<p>Member School District User Control Considerations: Determine whether PCs and terminals are protected against damage or misuse by having separate areas, either independent rooms or sections of rooms that restrict access to only authorized individuals.</p> <p>Verify that communication lines, junctions and modems are secured in an area that restricts access to only authorized individuals.</p>		

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
The ADMIN_OVERNIGHT procedure runs nightly to perform routine system maintenance and to prevent file and data corruption.	Obtained the command procedure for ADMIN_OVERNIGHT.COM and discussed the various jobs with the Assistant Director of Computer Services to determine what system maintenance activities are performed and their frequency.	The ADMIN_OVERNIGHT procedure runs every day to handle routine processing. There are fourteen jobs which are run through the command procedure. These jobs perform such things as backups, directory updates, file rebuilds, data cleanup, student account creation, position vacancy reports and EMIS data submission. The Systems Operation Supervisor and Assistant Director of Computer Services regularly monitored the ADMIN_OVERNIGHT procedure and handled failed jobs as they occurred. In addition, the Director of Computer Services periodically monitors the procedure.
A service agreement with HP exists to cover maintenance on the computer hardware.	Obtained and reviewed the hardware maintenance invoice and payment to determine if hardware maintenance exists and is current.	The hardware service agreement is paid annually and is up-to-date. The current agreement runs from October 1, 2001 to September 30, 2002.
Track-It! is used to log and maintain hardware and software problem calls received by users.	Discussed the Track-It! program with the System Operations Supervisor and reviewed work order reports to determine if problems are logged and resolved in a timely manner. Also obtained and reviewed customer service surveys filled out by the users to determine if users are satisfied with the service they have received from SEOVEC.	The SEOVEC uses an online tracking system, called Track-It!, to document routine computer problem calls from the member school districts. The problems are documented with the solution that corrected the problem. The Track-It! data is periodically reviewed to assess their effectiveness at serving member school districts.

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
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Network performance is monitored by the Network Technical Coordinator.	Discussed monitoring procedures with the Network Technical Coordinator. Obtained and reviewed programming scripts and example print screens of network status to understand how the network hardware being monitored and how often.	The SEOVEC uses two scripts to monitor network status. These scripts automatically run through the Event Scheduler (cron). One script "pings" the routers every 10 minutes and generates a data file with the results. The MRTG (Multi Router Traffic Grapher) runs every 5 minutes to test the amount of traffic on the network. These are reviewed several times throughout the day. They also review statistic reports from the BESS servers. These are reviewed for performance purposes only. This helps them to determine if they are having any problems with any of their servers.

IT Operations - Control Objective: Backup - Up-to-date backups of programs and data should be available in emergencies.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Backups of programs and data are performed regularly.	<p>Met with the System Operations Supervisor to discuss the backup procedures used at the SEOVEC. Obtained the following documents for review to determine if backups are performed regularly:</p> <ul style="list-style-type: none"> • written backup procedures • backup restoration procedures • ADMIN_BACKUP command procedure • daily backup logs 	<p>SEOVEC follows the steps outlined in their written backup procedures.</p> <p>Full system backups, including the operating system, all data and program files, are completed daily, Monday thru Friday. They maintain a three week supply (15 tapes) of daily backup tapes.</p> <p>The nightly backups are submitted through a batch called ADMIN_BACKUP. This batch job is run from the ADMIN_OVERNIGHT procedure and backs up all member school district data directories.</p> <p>A backup log was completed each day and maintained for the backup tape cycle (15 days). The log is reviewed each morning to ensure the nightly backups ran successfully.</p>
Backup tapes are properly maintained and rotated regularly.	<p>Discussed with the Systems Operations Supervisor the backup tape labeling and rotation processes.</p> <p>Obtained and reviewed the month/year end backup list from the System Operations Supervisor to determine if the backup tapes listed were stored at the location indicated.</p>	<p>The backup tapes are rotated off-site each morning. The only tape stored on-site is the current day's backup tape.</p> <p>A tape listing was maintained for month and fiscal year-end backups to document the assigned tape numbers and backup file names.</p> <p>All tapes on the list, with the exception of the most current tapes (April 02 and May 02), were found to be located off-site. The exceptions were found to be stored on-site.</p>

IT Operations - Control Objective: Backup - Up-to-date backups of programs and data should be available in emergencies.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
Backup tapes are stored in secure on and off-site locations.	Toured the on and off-site storage locations to verify the existence of environmental and physical access controls.	All backups for the SEOVEC are stored off-site at the Athens-Meigs ESC in a non-fireproof, locked metal cabinet. They have 24-hour access to the backup tapes.
<p>Member School District User Control Considerations: Determine if the district retains 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.</p> <p>Verify the district establishes and enforces a formal data retention schedule with the DA Site for the various application data files.</p>		

IT Operations - Control Objective: Disaster Recovery - Adequate plans should exist for the recovery of critical computer resources following an event which disrupts data processing services for an extended period of time.		Control Objective Has Been Met
<i>Control Procedures:</i>	<i>Test Descriptions:</i>	<i>Test Results:</i>
SEOVEC maintains a current disaster recovery plan detailing the actions to be taken in the event of a disaster.	Obtained and reviewed the disaster recovery plan to determine if it contains all the information needed to react effectively and efficiently in the event of a disaster.	SEOVEC has a current disaster recovery plan in place that outlines procedures to follow in case of a continued disruption of service. It appears to cover all procedures to be followed and all key contact people.
SEOVEC has entered into reciprocal agreements with the SCOCA and the OME-RESA for use of their computer facilities in the event of a disaster..	Discussed the nature of the reciprocal agreements with the Director of Computer Services to determine if actual valid agreements are in place.	SEOVEC has a written reciprocal agreement with the South Central Ohio Computer Association (SCOCA) and a verbal reciprocal agreement with Ohio Mid-Eastern Regional Education Service Agency (OME-RESA). The agreement with SCOCA is included in the disaster recovery plan. The verbal agreement with OME-RESA has been in place for the past several years.
All data center equipment is covered by insurance.	Obtained and reviewed the insurance policy to determine if the computer equipment is covered by insurance.	SEOVEC has an insurance coverage through Westfield Insurance Company. The policy is in effect from July 11, 2001 through July 11, 2002. All of the data processing equipment for SEOVEC is insured under this blanket policy. In addition, there is a second policy, which covers the routers and network equipment owned by the SEOVEC which is located in the districts. This policy is through the same agent and covers the same period.
<p>Member School District User Control Considerations: Verify the district develops, tests, and maintains their own contingency procedures to be performed in the event of an extended loss of computer resources. Such procedures should be established based upon the maximum outage tolerances for critical applications.</p> <p>Determine if the district maintains a copy of the disaster recovery plan that points out the responsibilities of the district. Key district personnel should understand their responsibilities outlined in the plan and should have the plan readily accessible.</p>		

SECTION IV - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION**DATA ACQUISITION SITE PROFILE
OHIO EDUCATION COMPUTER NETWORK**SITE DATA

Name:	Southeastern Ohio Voluntary Education Cooperative (SEOVEC)
Number:	20
Node Name:	SEOVEC
Chairperson:	Dale Dixon Superintendent Perry Hocking ESC
Fiscal Agent District:	Logan-Hocking Local School District
Administrator:	Robert L. Lindsey (CC_RLINDSEY) Director of Computer Services SEOVEC
Address:	221 North Columbus Road, P.O. Box 1250 Athens, OH 45701
Telephone:	740-594-7663
FAX:	740-592-6251
Website:	www.seovec.org

OTHER SITE STAFF

Ronald Smith (RON)
Jimmy Battrell (JIMMY)
Bobbi Weidner (BOBBIJO)
Carol VanSickle (CAROL)
John Arkley (JOHN)
Kirk DePeel (KIRK)
Tracey Potts (TRACEY)
Amy Davis (AMY)
Tom Dubs (TOM)
Rosalie Wolfe (ROSE)
Cory Councilman (CORY)
Sara Joyce (SARA)

Chief Executive Officer
Assistant Director of Computer Services
Secretary/Treasurer
Fiscal Services/InfOhio Coordinator
InfOhio/Fiscal Services Coordinator
Student Services/EMIS Coordinator
EMIS/Student Services Coordinator
System Operations Supervisor
Network Technical Coordinator
Assistant Network Technical Coordinator
Assistant Network Technical Coordinator
Secretary/Receptionist

HARDWARE DATA

Central Processors and Peripheral Equipment

<u>Model Number</u>		<u>Installed</u>		<u>Capacity/Density/Speed</u>	
CPU:	Compaq AlphaServer GS60	Lines/Ports:	0	Memory Installed:	5.0 GB
Disk:	Storage Works	Units:	13	Total Capacity:	61 GB
Tape Unit:	TSZ07	Units:	1	Max Density:	6250 BPI
Tape Unit:	TZ88	Units:	1	Max Density:	N/A
Tape Unit:	TKZ9	Units:	1	Max Density:	N/A
Printer:	Data Products B600	Units:	1	Print Speed:	600 LPM
Printer:	HP 8000	Units:	1	Print Speed:	20 PPM
Printer:	Data Products LP29	Units:	1	Print Speed:	2000 LPM

MEMBER SCHOOL DISTRICT SITE DATA

<u>IRN</u>	<u>MEMBER SCHOOL DISTRICT</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>	<u>EMIS</u>
045906	Alexander LSD	Athens	X	X		X
043521	Athens CSD	Athens	X	X		X
135145	Athens-Meigs ESC	Athens / Meigs	X	X		X
045914	Federal Hocking LSD	Athens	X	X		X
044446	Nelsonville-York CSD	Athens	X	X		X
051607	Tri County JVSD	Athens	X	X		X
045922	Trimble LSD	Athens	X	X		X
065680	Gallia County LSD	Gallia	X	X		X
062067	Gallia-Jackson-Vinton JVSD	Gallia	X	X		X
044248	Logan-Hocking LSD	Hocking	X	X	X	X
044156	Jackson CSD	Jackson	X	X		X
045021	Wellston CSD	Jackson	X	X		X
048512	Eastern LSD	Meigs	X	X		X
048520	Meigs LSD	Meigs	X	X		X
048538	Southern LSD	Meigs	X	X		X
048777	Morgan LSD	Morgan	X	X		X
045351	Crooksville EVSD	Perry	X	X		X
044479	New Lexington CSD	Perry	X	X		X
049056	Northern LSD	Perry	X	X		X

MEMBER SCHOOL DISTRICT SITE DATA

<u>IRN</u>	<u>MEMBER SCHOOL DISTRICT</u>	<u>COUNTY</u>	<u>USAS</u>	<u>USPS</u>	<u>SAAS</u>	<u>EMIS</u>
125674	Perry-Hocking ESC	Perry / Hocking	X	X		X
049064	Southern LSD	Perry	X	X		X
125682	Gallia-Vinton ESC	Gallia / Vinton	X	X		X
043604	Belpre CSD	Washington	X	X		X
050484	Fort Frye LSD	Washington	X	X		X
050492	Frontier LSD	Washington	X	X		X
044321	Marietta CSD	Washington	X	X		X
050500	Warren LSD	Washington	X	X		X
050476	Washington County ESC	Washington	X	X		X
050518	Wolf Creek LSD	Washington	X	X		X
051698	Washington County JVSD	Washington	X	X		X
TOTALS:			30	30	1	30



STATE OF OHIO
OFFICE OF THE AUDITOR

JIM PETRO, AUDITOR OF STATE

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

SOUTHEASTERN OHIO VOLUNTARY EDUCATION COOPERATIVE

ATHENS 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
JULY 2, 2002**