STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747
Fax No.: (775) 684-6600

LORNE J. MALKIEWICH, *Director*
(775) 684-6800

LEGISLATIVE COMMISSION (775) 684-6800
RICHARD D. PERKINS, *Assemblyman, Chairman*
Lorne J. Malkiewich, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
MORSE ARBERRY, JR., *Assemblyman, Chairman*
Mark W. Stevens, *Fiscal Analyst*
Gary L. Ghiggeri, *Fiscal Analyst*

PAUL V. TOWNSEND, *Legislative Auditor* (775) 684-6815
ROBERT E. ERICKSON, *Research Director* (775) 684-6825
BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830

Legislative Commission
Legislative Building
Carson City, Nevada

We have completed an audit of the Office of Secretary of State. This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions. The results of our audit, including findings, conclusions, recommendations, and the Secretary of State's response, are presented in this report.

We wish to express our appreciation to the Secretary of State and his staff for their assistance during the audit.

Respectfully presented,

Paul V. Townsend, CPA
Legislative Auditor

May 2, 2003
Carson City, Nevada

STATE OF NEVADA
OFFICE OF SECRETARY OF STATE
SECURITY AND RELIABILITY OF
INFORMATION SYSTEMS

AUDIT REPORT

Table of Contents

Page

Appendices

EXECUTIVE SUMMARY

OFFICE OF SECRETARY OF STATE SECURITY AND RELIABILITY OF INFORMATION SYSTEMS

Background

The Secretary of State is a constitutional officer elected to a 4-year term. The mission of the Office of Secretary of State includes (1) encouraging the development and diversification of the state's business community by providing efficient, expeditious, cost-effective services to businesses wishing to organize under the laws of Nevada, (2) maintaining and making the records and information filed with the Agency easily and promptly accessible and at a reasonable price, and (3) protecting the state's citizens against investment fraud through regulation and enforcement of the securities laws and through the education of the public.

At the end of fiscal year 2002, the Agency reported total revenues of $53.4 million and expenditures of $8.5 million. In contrast, at the end of fiscal year 1998 the Agency reported revenues of $29.6 million and expenditures of $5.3 million. In 1996, a contracted re-engineering study was completed. As a result of this study, in December 2000 the Agency began a project to replace its legacy mainframe-based Uniform Commercial Code (UCC), Corporations, and integrated Accounting systems. These are being replaced with a PC-based platform with the new system referred to as the Electronic Secretary of State information system (e-SOS).

Purpose

The purpose of this audit was to determine the security and reliability of the information systems at the Office of Secretary of State. Our audit included a review of the controls over the development of information systems and controls over the Uniform Commercial Code and Accounting systems.

EXECUTIVE SUMMARY

OFFICE OF SECRETARY OF STATE
SECURITY AND RELIABILITY OF
INFORMATION SYSTEMS

Results in Brief

Adequate and consistent project management over contract execution and system development helps ensure computer systems meet user needs and contract provisions. However, we found project control weaknesses that place at risk the accomplishment of these objectives. During the course of our review the Agency recognized its initial weaknesses and has begun to make changes in their process to deliver more consistent, daily management oversight. Additional improvements in project management will further strengthen the Agency's oversight.

Weaknesses in planning and controls over security and disaster recovery place at risk the systems and information maintained by the Office of Secretary of State. There is also a greater risk that data will be inaccurate or lost. The Agency should give greater attention to creating a formal security plan, including stronger controls over system access. In addition, controls over storage and retention of credit card information need to be strengthened. Furthermore, there is no disaster recovery plan, and some backup tapes were not stored in an off-site location.

Principal Findings

- The Office of Secretary of State contracted with a vendor to develop a new computer system called the Electronic Secretary of State information system. Initially, project managers from the Agency and the contractor did not adequately or consistently monitor the development of this new system. For example, there was limited on-site project management, and the quality assurance function was not utilized. Agency management has taken steps to correct these concerns. (page 9)

- Some documentation that was required by the Request For Proposal (RFP) was not provided by the contractor. This included documentation describing the data and software code. Without this information, future maintenance of the programs will be difficult. This resulted from a lack of enforcing the contract requirements. (page 11)

- Design work presents a complete description of software to be built. However, design work for the new information systems was not consistently applied. For example, design work for the Uniform Commercial Code (UCC) application was very detailed. In contrast, there was no design document for integrating the Accounting application. Following our inquiries, an Accounting design document was provided by the contractor. While the UCC and Accounting programs have been substantially completed, more work remains. The Corporations component of the new system will be larger and more complex and will require increased attention to contract provisions. (page 11)

- The Agency should develop a formal security plan. Information technology standards, including those adopted by the State of Nevada, require agencies to adopt a security plan commensurate with the sensitivity and value of the information processed and maintained. One reason the plan has not been created is that a security officer had not been designated and given this responsibility. During our audit, a security officer was officially designated. (page 13)

- Security settings for gaining access to the Agency's information need strengthening. In one instance, a "Super User's" password function was disabled, thus allowing anyone in the Agency to have the same level of access to the system. A "Super User" is one that has enhanced access rights to a system or data, including add, update, or delete capabilities. Also, user ID's that were set up for test purposes still remained active even though no testing was being conducted. In addition, computers were not locked out after a period of inactivity, and one ex-employee still had network access. Furthermore, there was no formal process for granting system access. (page 14)

- Passwords are a key control in preventing unauthorized access to computer data. However, appropriate password controls have not been consistently applied to all users. As a result, the Agency risks allowing access to unauthorized individuals. Our review found that passwords are not always required, or forced to periodically change. In addition, a minimum password length is not required and users are not always restricted to three invalid login attempts. Agency personnel had recognized these weaknesses and have taken steps to strengthen controls. (page 16)

- Controls over credit card numbers need to be strengthened. In four of five locations we observed, papers with credit card numbers were stored in unlocked drawers and on employees' desks. In one instance, we observed an open file cabinet where transactions were up to 18 months old. Staff indicated there is a need to have frequent access to old transaction documents. However, credit card information should not be allowed to remain in inadequately secured locations. (page 18)

- Disaster recovery has not been adequately addressed. The Agency has not created a written disaster recovery plan. In addition, some backup tapes were stored in the same location as the computers instead of in an off-site location. Finally, the list to access the off-site storage contained the name of an ex-employee. The Agency has begun strengthening these controls. (page 19)

Recommendations

This report contains 10 recommendations to improve the security and reliability of the information systems at the Office of Secretary of State. The Agency should ensure contract provisions are monitored and consistently applied, and maintain on-site project management. In addition, the Agency should create a security plan and designate a security officer. To improve controls over system access, the Agency should establish appropriate security settings. In addition, it should strengthen password controls, and provide better protection for credit card information. Furthermore, the Agency should create a disaster recovery plan, and store all backup tapes off-site. Finally, the Agency should keep updated the list of employees who are authorized to access the off-site storage facility. (page 29)

Agency Response

The agency, in its response to our report, accepted all 10 recommendations. (page 25)

Introduction

Background

The Secretary of State is a constitutional officer elected to a 4-year term. The Agency's main office is in Carson City. There is a Las Vegas office for the Securities Division and for filing expedited corporations/business entities documents as well as trademarks. A small office is also established in Reno for securities investigation and enforcement.

The mission of the Office of Secretary of State is to promote its activities throughout the State. The goals of the Agency are achieved by (1) encouraging the development and diversification of the state's business community by providing efficient, expeditious, cost-effective services to businesses wishing to organize under the laws of Nevada, (2) maintaining and making the records and information filed with the Agency easily and promptly accessible and at a reasonable price, and (3) protecting the state's citizens against investment fraud through regulation and enforcement of the securities laws and through the education of the public.

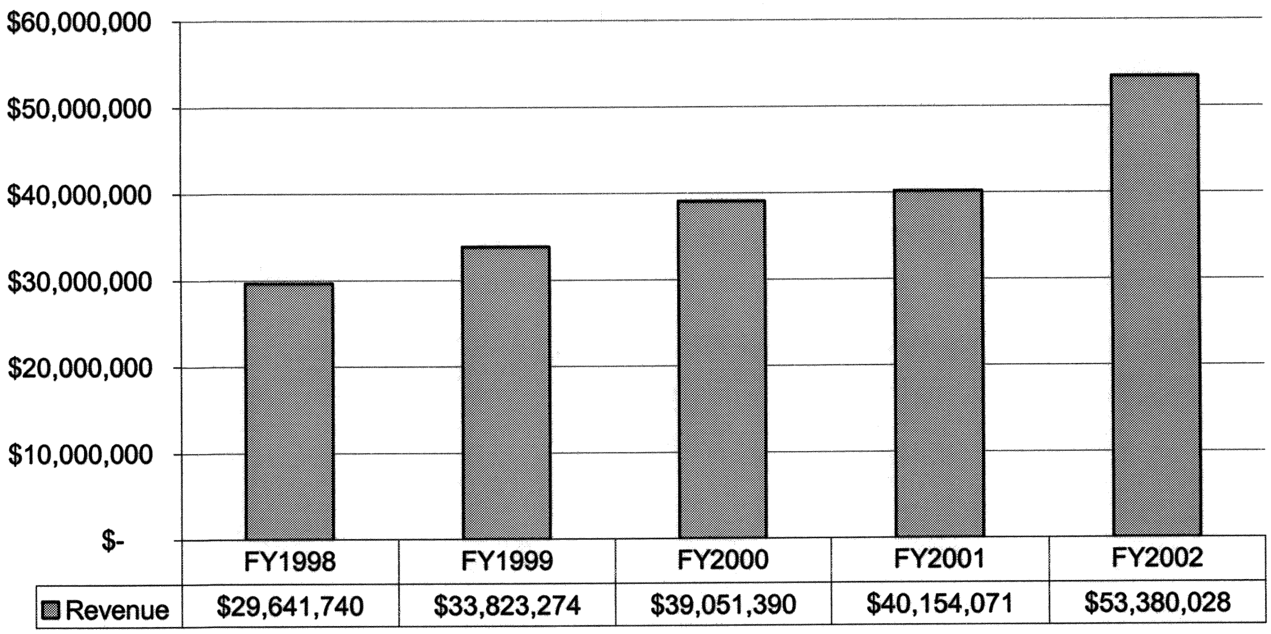
The Agency has several constitutional and statutorily mandated duties, including:

- Filing and retrieving documents related to corporations, limited liability companies, limited partnerships, trademarks, and liens against personal property pursuant to the Uniform Commercial Code (UCC).
- Regulating the securities industry in Nevada through the registration of securities, licensing of persons selling securities, and investigation of complaints.
- Executing, enforcing, and interpreting all federal and state election laws; also filing and retrieving documents related to state elections.
- Maintaining records of the official acts of the executive and legislative branches of Nevada Government.
- Licensing and administration of Notary Publics.

At the end of fiscal year 2002, the Agency reported 125 authorized positions with total revenues of $53.4 million and expenditures of $8.5 million. In contrast, at the end of fiscal year 1998 the Agency reported revenues of $29.6 million and expenditures of

$5.3 million. Most of these revenues are deposited directly to the general fund. For example, in fiscal year 2002, the Office deposited $50,121,076 into the general fund. Revenues are generated through a variety of fees. This includes fees for UCC, Corporate, and Securities filings. Chapter 601, Statutes of Nevada 2001 (Senate Bill 577) increased Corporate filing fees, resulting in a $13 million increase in Agency revenues. Exhibit 1 provides a historical view of revenues at the Office of Secretary of State.

Exhibit 1



SECRETARY OF STATE
Reported Revenues -- Fiscal Years 1998 to 2002

Source: State Accounting System Records

In 1996, a contracted re-engineering study was completed resulting in a number of recommendations for both organizational and automated systems enhancements. The Agency has been steadily implementing most of the recommendations, including a project that began in December 2000 to replace the legacy mainframe-based UCC, Corporations, and integrated Accounting systems. These are being replaced with a PC-based platform readily adaptable to Internet use. This new system is referred to as the Electronic Secretary of State information system (e-SOS).

E-SOS helps the Agency accomplish its mission by capturing, storing, and retrieving information. Examples of the information processed include:

- Corporate filings for new businesses and annual renewals
- Amendments to corporate filings
- UCC financial statements and liens
- Receiving and accounting for payments made to the Agency

An outside contractor is developing all three components of the new system (Corporations, UCC, and Accounting). The value of this contract was $2.3 million as of April 2001.

Scope and Objective

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission, and was made pursuant to the provisions of NRS 218.737 to 218.893. The Legislative Auditor conducts audits as part of the Legislature's oversight responsibility for public programs. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This audit included a review of the controls over the development of information systems, and controls over the Uniform Commercial Code and Accounting systems. The objective of this audit was to determine the security and reliability of the information systems at the Office of Secretary of State.

Findings and Recommendations

Original Project Management Did Not Consistently Monitor and Administer the e-SOS Contract

Adequate and consistent project management over contract execution and the system development process helps ensure that computer systems will meet user needs and contract provisions. However, we found project control weaknesses that place at risk the accomplishment of these objectives. During the course of our review the Agency recognized its initial weaknesses and has begun to make changes in their process to deliver more consistent, daily management oversight. Additional improvements in project management will further strengthen the Agency's oversight.

Project Management and Contract Monitoring Needed Improvement

In initial execution of the new Electronic Secretary of State (e-SOS) project, the original agency and vendor project managers did not adequately and consistently monitor the contract, losing sight of some key provisions and deliverable details. Certain documentation was not delivered, requirements and design work was inconsistently applied, some deliverables were not accepted in accordance with written procedure, and project schedules were not met. Office of Secretary of State management has taken steps to correct these concerns.

Initial Project Managers Did Not Effectively Monitor the Contract

Both original project managers from the Agency and the vendor initially did not effectively monitor and execute key contract components and deliverable documents. For example, the Accounting software was not fully integrated with the UCC application as required by contract. In addition, "up-front" imaging and receipting was not designed or implemented as required by contract. "Up-front" imaging and receipting electronically captures documents that customers send in to the Agency along with payment information. This process supports a paperless flow of transactions and electronic images throughout the Agency and allows money to be deposited by the next business day.

Through project management changes made by both the Agency and the vendor, there has been improvement in monitoring and execution of the contract. We observed a greater attention to details of the contract by Agency management. However, sustained attention is needed until completion of the contract.

Full Vendor Proposal and Contract Document Not Actively Utilized

We found no documentation that key project personnel monitored contract requirements against work results. When a copy was requested, key project personnel did not have a copy of the full contract including the vendor's response. A full contract includes the Request For Proposal (RFP), the vendor's response to the RFP, and a signed document. The complexity of system development projects requires continued monitoring by project leaders to ensure the system meets user needs. This monitoring should include comparing contract provisions to work delivered by the vendor to ensure all requirements are met.

Limited On-Site Project Management

The original Agency project manager was not on-site full time. He was present at the Carson City office 2 days each week. The remainder of the week he worked from his base location in Las Vegas. Agency management has indicated this reduced the effectiveness of communication throughout the project. According to Agency personnel, the vendor project manager was in Carson City less than 5 weeks out of the 8 months of November through June. Available and focused project management is essential to control complex projects in environments with limited technical staff. Agency management corrected this weakness by ensuring it had full-time, on-site project management.

The Quality Assurance Function Was Not Used Effectively

The Office of Secretary of State and the vendor each had a Quality Assurance (QA) manager. Our audit found that both QA managers were not crosschecking design documents to ensure they adhered to contract terms. Additionally, the Agency QA manager was only assigned after nearly 5 months into the project. In addition, he was involved initially for only 20 hours per month for the first 3 months. This was later increased to nearly full time after project management changes. The absence of effective and consistent vendor and Agency QA intensified original project management problems.

Use of effective, independent QA should provide a means to check deliverable details to contract requirements. It should also form an additional control over contract execution by independently reporting unplanned for, or unexecuted, requirements to senior management. Management can then assign corrective action to project and user managers.

No Formal Acceptance Sign-Off Was Made for Accounting Requirements

No formal sign-off or acceptance was made for the Accounting system requirements. The accounting manager and supervisor were not invited to comment on the document. This did not comply with written project procedures. In addition, the lack of a formal acceptance may have prevented early attention being paid to ensure the Accounting system worked properly with the UCC system. A key responsibility of project management is to ensure compliance with procedures requiring key stakeholders to be involved with sign-off acceptance of contract deliverables affecting their areas.

Contractor Did Not Provide Required Documentation

Part of the development of a new information system includes providing documentation to help programmers and users understand the new programs and the data they process. However, we found that the contractor had not provided documentation as required by the contract terms. For example, documentation used to describe Accounting data and diagrams as required by the RFP was not provided. In addition, technical documentation used to describe the program and software code was not provided.

Without this documentation, future maintenance of the programs will be difficult, especially for staff without in-depth knowledge of the systems. Although the contract vendor is responsible for providing this documentation, the Agency should have enforced the contract requirements.

Requirements and Design Work Were Not Consistently Applied

Design work was not consistently applied to new programs being developed in the e-SOS System. For some programs, documents that illustrate the design of the systems were very thorough. In other cases, these documents were missing or not detailed. For example, the UCC design document was detailed. However, there was no design document for custom integration of the Accounting application with the UCC application prior to start of the first acceptance test. The design document was provided following our inquiries.

Further inconsistencies involved the Request For Proposal (RFP). The RFP for UCC was detailed. However, for the Accounting system there were few RFP details. In addition, the RFP contained few details on making the new systems Internet ready. The Agency's expectation is that forms will be filled out and submitted online via the Internet.

These weaknesses will become more evident in the future, if not addressed. While the UCC and Accounting programs have been substantially completed, more work remains. At the conclusion of our audit, the Agency was in the initial stages of the Corporations program. This program will store information on businesses within the State of Nevada. It will be a larger and more complex program than either UCC or Accounting.

Without consistent and thorough attention to requirements and specifications for all system parts, there is the danger that key components will not work together in the overall system. During our review, the Agency began UCC acceptance testing without integrated Accounting functions being designed or executed. Because UCC transactions are subsequently processed by the Accounting system, there is less assurance of a properly integrated system.

Project Schedules Were Not Met

Scheduled implementation dates were missed for all three components of the e-SOS system. This was a result, in part, of not initially managing contract requirements.

UCC with integrated Accounting was scheduled to be completed by November 2001. This was not implemented until October 2002. In addition, this is not the final version—components originally intended in the contract are not yet included. This includes "up-front" imaging and receipting now rescheduled for a later version. Furthermore, the Corporations system was scheduled for completion by April 2002. However, this system was still in the design phase as of October 2002.

Recommendations

1. Ensure contract provisions are monitored and consistently applied, including documentation, design, and testing.
2. Maintain an on-site project manager and appropriate quality assurance function.

Security Controls Need Strengthening

The Office of Secretary of State has not adopted a formal, written security plan. In addition, computer security weaknesses place at risk the information maintained by the Agency. Furthermore, controls over credit card numbers need to be strengthened. Finally, disaster recovery has not been adequately addressed. Agency personnel indicated a lack of time to address these weaknesses.

The Agency Should Develop a Security Plan

Information technology standards, including those adopted by the State of Nevada, require agencies to adopt a security plan commensurate with the sensitivity and value of the information processed and maintained. One reason the plan has not been created is that a security officer had not been designated and given this responsibility. During our audit a security officer was officially designated.

The purpose of the security plan is to provide an overview of the security requirements of the organization's systems and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the systems. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.

Examples of items that can be included in a plan include controls over physical and logical security, environmental controls, contingency planning, and training. The lack of a written security plan reduces the likelihood that sound controls will be implemented. Exhibit 2 provides a list of components that should be included in a plan.

Exhibit 2

Components of a Security Plan

Document an entity-wide security plan

A security plan is documented and approved.
Plan is kept current.

Periodically assess risk

Define a process that allows an entity-wide understanding of risk assessment.
Require that risk assessments be performed.
Designate a central security group to schedule risk assessments and facilitate their conduct.
Involve mix of individuals with knowledge of business operations and technical aspects of systems.
Require final sign-off by the business managers indicating agreement with risk reduction decisions.

Establish a security management structure and clearly assign security responsibility

A security management structure has been established.
Information security responsibilities are clearly assigned.
Owners and users are aware of security policies.
An incident response capability has been implemented.

Implement effective security-related personnel policies

Hiring, transfer, termination, and performance policies address security.
Employees have adequate training and expertise.

Monitor the security program's effectiveness and make changes as needed

Management periodically assesses the appropriateness of security policies and compliance with them.
Management ensures that corrective actions are effectively implemented.

Source: Federal Information System Controls Audit Manual, General Accounting Office

Controls to Access Computer Systems Need to Be Stronger

The security settings for gaining access to the Agency's information need strengthening. In one instance, a "Super User's" password function was disabled thus allowing anyone in the agency to have the same high level of access to the system. Also, user ID's that were set up for test purposes still remained active even though no testing was being conducted. In addition, computers were not locked out after a period of inactivity and one ex-employee still had network access. Furthermore, there was no formal process for granting system access.

"Super User" Password Was Disabled

The password function for a "Super User" was disabled. A "Super User" is one that has enhanced access rights to a system or data, including add, update, or delete capabilities. In this instance, the "Super User" function can also execute restricted functions such as refunds and add new system users. While every user should have an ID and password, control weaknesses for the "Super User" designation are more severe due to the level of access granted. With the password function disabled for this employee, full access to the system data can be granted with only the employee's user ID, which can be easily guessed.

Accounting Test ID's Still Active

At the time of our review, the new Accounting software program listed 14 users that were authorized to access the data. Of these 14, four were test ID's that had unrestricted access to the information. A test ID is one set up for the purpose of testing the system. Once testing is complete, the ID should be deleted and each valid user assigned a unique ID.

Furthermore, a test ID should be restricted to a test environment so that production data is not affected. Test data can, and should, be accessed by a variety of people within the organization to test programs. This helps ensure the programs function as intended. In contrast, production data is the actual information the Agency uses to conduct business. If production data is changed or deleted by unauthorized individuals, the Agency's operations are impacted. However, our review found the test ID's had access to production data. Staff was unsure if these ID's were still valid. By not monitoring test ID's, there is increased risk that unauthorized individuals will gain access to Accounting data.

No Lockout After Period of Inactivity

To gain access to UCC or Accounting data, a user must login through a Microsoft Windows network. The Windows network was not set to automatically lock out a user after a period of inactivity. Without this control, there is greater risk of unauthorized access to Agency data. For example, an authorized user who has logged onto the UCC or Accounting system can leave without logging out. This allows other, unauthorized users unrestricted access to the information.

We found that the Agency had no policy to require the locking of computers. To implement this control, the Agency should create a policy to require each computer to have a screen saver set to lock the user out after a period of inactivity. Management indicated that some users are set up in this manner, but not all.

Ex-employee Had System Access

Of five ex-employees that recently left the Agency, one still had system access 2 months after leaving. By allowing access to ex-employees, there is increased risk of these employees or others gaining unauthorized access to Agency information.

We also reviewed password controls in the system that allows Agency users to dial-in. This system enables employees to gain access to data and check e-mail from remote locations. We found that of 15 users that had dial-in access, 1 ex-employee was on the access list. In addition, another user was unknown to the Agency's network technician. Based on the technician's judgment, this user was deleted. To strengthen controls over the dial-in system, the Agency should periodically monitor the list of users to ensure they are valid and still authorized to have access.

Informal Process for Granting System Access

The process for granting employees access has been informal. This is due, in part, to a lack of formal policies to govern security controls. State standards require that access authorization be documented and approved by those the agency head designates. However, the Agency has not created a formal procedure for granting employee access to the computer systems. Staff indicated e-mail is sent to the Agency's technology section from an employee's supervisor requesting access. In addition, there have been occasions when an employee requested and was granted access without supervisor approval. Furthermore, the e-mail is not retained for any specific length of time.

Staff agreed that a more formal process for granting access should be implemented. A written procedure should be created that requires forms to be filled out and approved by the appropriate level of management. In addition, these forms should be retained and reviewed periodically to ensure only authorized users have access to the appropriate systems and data. This will ensure only authorized employees have access to computer resources.

Password Controls Need Strengthening

Passwords are a key control in preventing unauthorized access to computer data. However, appropriate password controls have not been consistently applied to all users. As a result, the Agency risks allowing access to unauthorized individuals. Our review found that passwords are not always required, or forced to change. In addition, a minimum password length is not required and users are not always restricted to three invalid login attempts. Agency personnel had recognized these weaknesses and have taken steps to strengthen controls.

Passwords Not Always Required

Employees wishing to use an Agency program, such as the Accounting system, are first required to login through a network and then onto the individual program. We found password weaknesses both at the network level and the application level. For the first eight users we reviewed that are required to login to the network, three did not have to supply a password for network access. For these three users, the system security settings did not require a password to be used. However, these users had elected to use a password.

In addition, users of the Accounting System and UCC system were not required to provide a password to gain entrance to the programs. Only a valid user ID was required.

State standards require that both an ID and password be required to gain access to information systems. Requiring only an ID would allow anyone within the organization that had knowledge of an employee's name to gain access to data. Once unauthorized access is gained, a malicious user could destroy or alter Accounting data or UCC filings.

Forced Change of Passwords Not Consistently Applied

To prevent their discovery by others, passwords should be changed periodically. Industry standards, including those newly adopted by the Department of Information Technology (DoIT), require that passwords be changed every 90 days. However, we found that these standards are not always applied.

In a sample of eight users we selected, one was required to change the password every 40 days. In contrast, four users were never required to change their passwords, and three were required to change their passwords every 365 days. In addition, dial-in users were not forced to change their passwords.

No Minimum Password Length

Standards require that passwords be a minimum of eight characters in length. However, settings for all eight users we reviewed did not meet the standards. In five instances, the settings required a password of five characters. In the other three instances, there was no password length defined. In addition, no minimum password length was required in the system that controls dial-in access.

Users Not Restricted to Three Invalid Login Attempts

Security settings do not limit the number of invalid login attempts by users. A login attempt occurs when a user types his ID and password to gain authorized access to programs and files. However, a commonly used technique for gaining unauthorized access is to login by guessing an ID/password combination. The more attempts a hacker is allowed, the more likely he will gain access.

To prevent this from happening, computer software should limit the number of invalid ID/password login attempts. A strong control limits individuals to three invalid attempts, after which the software prevents the person from having additional attempts. However, the Agency's systems do not contain this control. For example, we tested this by attempting to login using two separate employee ID's. We attempted to login 10 times for each ID. After 10 attempts, the system had not locked us out.

Credit Card Information Needs Stronger Security

As a service to its customers, the Agency allows payment by credit card for activities such as UCC and Corporate filings. During fiscal year 2001, the Agency processed approximately $3.3 million in credit card payments. In contrast, during fiscal year 2002, this figure had increased to approximately $6.5 million—almost double that of the prior year.

When credit card transactions are processed, the Agency maintains documentation which contains credit card numbers. This is done so employees can process the credit card information with the customer's request. Through our review we found the paper copies containing credit card numbers were often left in inadequately secured locations. In four of the five locations within the Agency that we observed, papers with credit card numbers were stored in unlocked drawers or on employees' desks. In one instance, we observed an open file cabinet where transactions were up to 18 months old. Staff indicated the need to have frequent access to old transaction documents. However, credit card information should not be allowed to remain in inadequately secured locations.

Disaster Recovery Has Not Been Adequately Addressed

Disaster recovery has not been adequately addressed. The Agency has not created a written disaster recovery plan. In addition, some backup tapes were stored in the same location as the computers instead of in an off-site location. Finally, the list to access the off-site storage contained the name of an ex-employee.

No Disaster Recovery Plan Exists

Service continuity deals with an organization's ability to continue operations in the case of disruption in the information system support activities and to survive, even if a disastrous event occurs. Rigorous planning and commitment of resources is necessary to adequately plan for such an event. In addition, the new DoIT standards require agencies to develop, maintain, and test a plan.

Events that could disrupt operations include power outages, hardware or software failures, vandalism, flooding, fires, and earthquakes. To avoid disruption from such events or to recover from them, a disaster recovery plan must address those components that maximize an organization's ability to protect assets. However, the Agency has not created a disaster recovery plan. Appendix C lists the components that should be included in a plan. Examples include:

- Clearly assigns responsibilities for recovery.
- Identifies critical data files.
- Plan is periodically tested.
- Arrangements have been made for alternate processing facilities.

Without an adequate and fully tested disaster recovery plan, the Agency increases the risk of losing its capability to process information that it maintains. Staff has indicated a lack of time to be able to create one. However, during calendar year 2002 they have hired new employees with qualifications in this area.

Some Backup Tapes Were Not Stored Off-Site

The location used to store some backup tapes was not adequate to protect the data in the event of a disaster affecting the computer room. The central computers are located in one room within the Capitol Building. While some backup tapes are stored at an off-site location, the tapes for the UCC and the Accounting system data were stored within the computer room. Staff indicated they simply had not transferred the tapes to the off-site location. To ensure adequate protection of data, all backup tapes should be stored at the off-site location. Based on our inquiries, staff moved the tapes off-site.

List to Access Off-Site Storage Should Be Kept Updated

To access the off-site location used to store backup information, an employee must be on an approved list. This list is used to ensure only authorized Agency employees have access to the backup information. However, during our review, we found one ex-employee that was listed as an approved employee. Staff immediately removed the employee's name.

Recommendations

3. Plan, write, and execute a comprehensive agency security plan that complies with applicable State of Nevada IT Security Standards, as well as other prudent industry guidelines.
4. Designate an Information Security Officer with assigned responsibility to coordinate and help execute the security plan.
5. Establish security settings for each system and application so that only authorized individuals have access.
6. Strengthen password controls to prevent unauthorized access to information, including dial-in access.
7. Provide better protection of credit card information.
8. Create a disaster recovery plan.
9. Store all backup tapes at the designated off-site location.
10. Periodically update the list of employees who are authorized to access the off-site storage tapes.

Appendices

Appendix A

Audit Methodology

To gain an understanding of the Office of Secretary of State, we reviewed activities located in the Carson City and Las Vegas offices. We also reviewed budgets, laws, regulations, hearings, and policies and procedures related to the agency's operations. This was followed by interviews with Agency management and key staff in each division. We reviewed selected documents related to the new Nevada Electronic Secretary of State project (e-SOS), and attended selected status meetings, document discussions, and test activities.

To determine if controls over project management were adequate, we reviewed the Universal Commercial Code (UCC) and Accounting systems that were under development. We reviewed documents such as project plans, requirements, designs, user instructions, and other technical and user documents. We attended interviews, discussions, and status report meetings with state and vendor project management. We also reviewed project management and quality assurance techniques and activities to ensure contract and specification requirements and design were tested and delivered.

To evaluate controls over security, we documented the lack of a comprehensive security plan and designation of an information security officer. We also reviewed the Agency's procedure for signing non-disclosure agreements and conducting security training. We documented controls over remote access to the Agency's network. We also reviewed controls over the use and storage of customer credit card numbers.

To determine if security over physical access is adequate, we observed technical division practices for keeping the area and the server room locked and restricted. We also reviewed the access list to off-site backup files. To evaluate the Agency's disaster recovery procedures, we documented its progress toward creating comprehensive written, and periodically tested, Business Contingency and Disaster Recovery plans for personnel, hardware, software, networks, and facilities. We documented the existence of off-site backup files and reviewed the technical area and server room fire protection, emergency power, and air conditioning.

Our audit work was conducted from November 2001, to October 2002, in accordance with generally accepted government auditing standards.

In accordance with NRS 218.821, we furnished a copy of our preliminary report to the Secretary of State. On April 16, 2003, we met with Agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix D that begins on page 25.

Contributors to this report include:

S. Douglas Peterson, CISA
Information Systems Audit Supervisor

Roy B. Cage, CIA, CISA
Deputy Legislative Auditor

Stephen M. Wood, CPA
Chief Deputy Legislative Auditor

Appendix B
Prior Audit Recommendations

As part of our audit, we requested the Office of Secretary of State determine the status of the recommendations made in our 1995 audit. That audit contained four recommendations relating to controls over cash receipts. The Agency indicated that all four recommendations have been fully implemented. The scope of our current audit did not include the prior recommendations. Therefore, we did not verify the Agency's implementation of the prior recommendations.

Appendix C

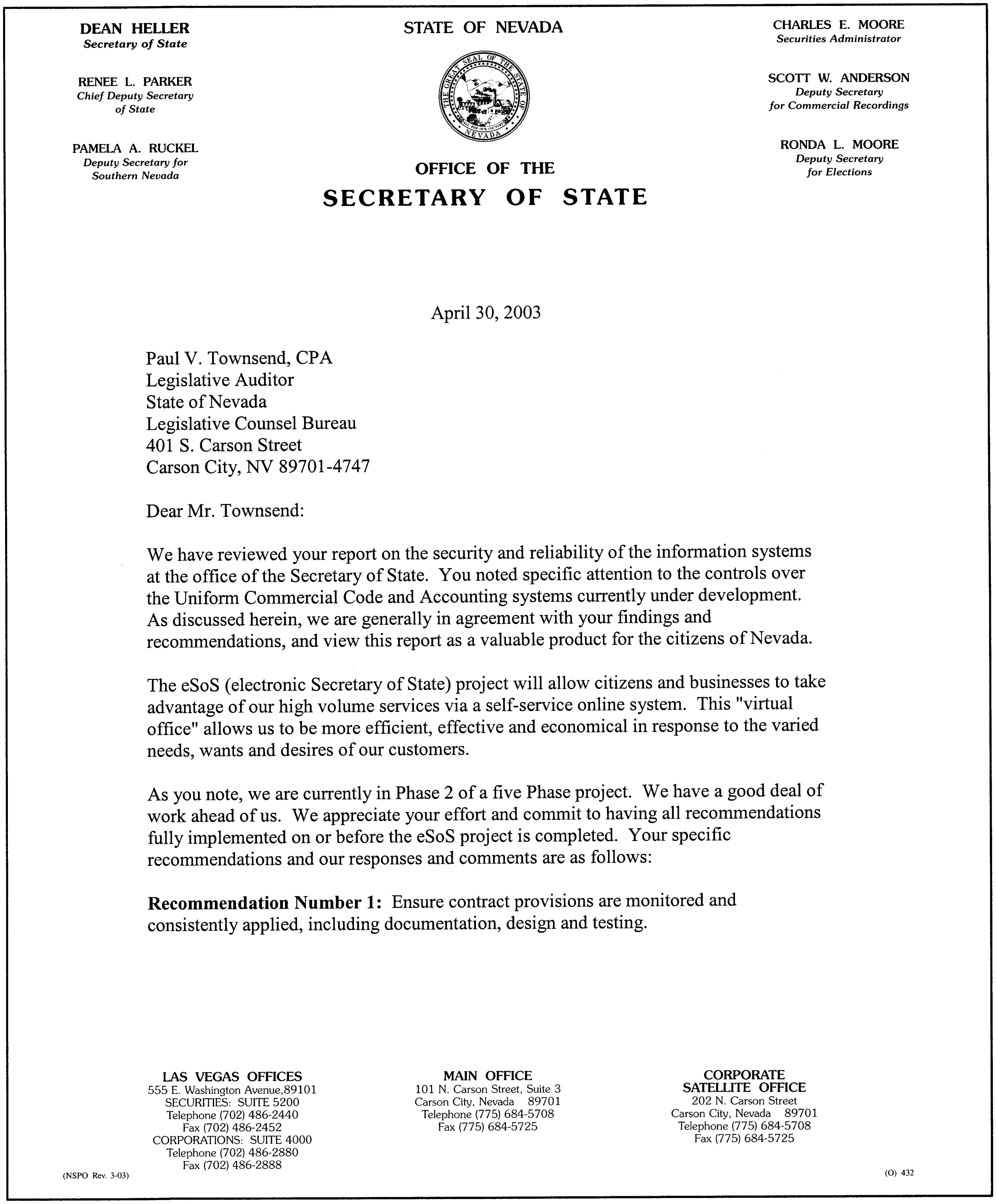
Components of Disaster Recovery Planning

Activity Number	Control Activity
1	Contingency plan clearly assigns responsibilities for recovery.
2	Contingency plan identifies alternate processing and backup storage facility.
3	Contingency plan has been distributed to all appropriate personnel.
4	Contingency plan identifies critical data files.
5	Contingency plan includes procedures to follow when the data/service center is unable to receive or transmit data.
6	Contingency plan requires user departments to develop adequate manual processing procedures for use until operations are restored.
7	A list of critical operations and data has been documented that prioritizes data and operations.
8	A list of critical operations and data has been documented that is approved by senior program managers.
9	A list of critical operations and data has been documented that reflects current conditions.
10	Computer hardware resources supporting critical operations are identified.
11	Computer software resources supporting critical operations are identified.
12	Computer supplies supporting critical operations are identified.
13	System documentation supporting critical operations are identified.
14	Telecommunication resources supporting critical operations are identified.
15	Office facilities and supplies supporting critical operations are identified.
16	Human resources supporting critical operations are identified.
17	Emergency processing priorities are established.
18	Arrangements have been made for alternate data processing and telecommunications facilities.
19	The disaster recovery plan is periodically tested under conditions that simulate a disaster.
20	Time frames in which each resource to be used has been identified.
21	A likely range of problems and scenarios has been identified.
22	Strategies for emergency response include documentation of initial actions to protect lives and limit damage.
23	Strategies for recovery include steps to continue support for critical functions.
24	Strategies for resumption determine what is required to return to normal operations.
25	Strategies have been developed to train staff.

Sources: National Institute of Standards & Technology, U.S. Dept. of Commerce, and Federal Information System Controls Audit Manual, U.S. General Accounting Office

Appendix D

Response From the Office of Secretary of State



DEAN HELLER
Secretary of State

RENEE L. PARKER
Chief Deputy Secretary of State

PAMELA A. RUCKEL
Deputy Secretary for Southern Nevada

STATE OF NEVADA

OFFICE OF THE

SECRETARY OF STATE

CHARLES E. MOORE
Securities Administrator

SCOTT W. ANDERSON
Deputy Secretary for Commercial Recordings

RONDA L. MOORE
Deputy Secretary for Elections

April 30, 2003

Paul V. Townsend, CPA
Legislative Auditor
State of Nevada
Legislative Counsel Bureau
401 S. Carson Street
Carson City, NV 89701-4747

Dear Mr. Townsend:

We have reviewed your report on the security and reliability of the information systems at the office of the Secretary of State. You noted specific attention to the controls over the Uniform Commercial Code and Accounting systems currently under development. As discussed herein, we are generally in agreement with your findings and recommendations, and view this report as a valuable product for the citizens of Nevada.

The eSoS (electronic Secretary of State) project will allow citizens and businesses to take advantage of our high volume services via a self-service online system. This "virtual office" allows us to be more efficient, effective and economical in response to the varied needs, wants and desires of our customers.

As you note, we are currently in Phase 2 of a five Phase project. We have a good deal of work ahead of us. We appreciate your effort and commit to having all recommendations fully implemented on or before the eSoS project is completed. Your specific recommendations and our responses and comments are as follows:

Recommendation Number 1: Ensure contract provisions are monitored and consistently applied, including documentation, design and testing.

LAS VEGAS OFFICES
555 E. Washington Avenue,89101
SECURITIES: SUITE 5200
Telephone (702) 486-2440
Fax (702) 486-2452
CORPORATIONS: SUITE 4000
Telephone (702) 486-2880
Fax (702) 486-2888

MAIN OFFICE
101 N. Carson Street, Suite 3
Carson City, Nevada 89701
Telephone (775) 684-5708
Fax (775) 684-5725

CORPORATE
SATELLITE OFFICE
202 N. Carson Street
Carson City, Nevada 89701
Telephone (775) 684-5708
Fax (775) 684-5725

(NSPO Rev. 3-03)

(O) 432

Response: Our initial project manager did not perform the necessary project management functions essential for success. We recognized this early in the project and immediately made the appropriate personnel changes. As a result, we now employ a seasoned project manager with the requisite skills to re-establish the project on course and on budget. We have included in our project monitoring and reporting the essential documentation, design, and testing criteria required for a successful project conclusion.

Recommendation Number 2: Maintain an onsite project manager and appropriate quality assurance function.

Response: The contract initially provided for independent Quality Assurance (QA) oversight by the vendor. Our office was not budgeted for separate QA, but a DoIT QA representative assisted in the contract procurement process and attended some project meetings on his own time. As the project progressed it became apparent that the vendor's QA person was not objectively reviewing project documentation or the contract. Therefore, we worked with the Department of Information Technology (DoIT) to formally contract for QA services within our budgeting constraints. We now have a full time, on-site project and quality assurance manager, with appropriate levels of staff support, to oversee the contract requirements. In addition, we have secured legal representation from the Attorney Generals' office to facilitate and enhance contract communication, clarification and compliance.

Recommendation Number 3: Plan, write and execute a comprehensive agency security plan that complies with applicable state of Nevada IT Security Standards, as well as other prudent industry guidelines.

Response: We are currently developing an extensive security plan with the knowledge that e-government can only flourish in a secure environment. As we take our customer base from "in line" to "online" we are cognizant of the security issues. Therefore, we have consulted with DoIT and are working closely, as a member, with the State Information Technology (IT) Security Committee to create a compliant security plan. At the time of this response, we are developing policies, standards and procedures based on the minimum requirements set forth by the State IT Security Committee.

Recommendation Number 4: Designate an Information Security Officer with assigned responsibility to coordinate and help execute the security plan.

Response: The Secretary of State's office designated an Information Security Officer (ISO) at the time of this finding by the auditors. The ISO is responsible for developing all components of the security plan to ensure all policies, standards and procedures are deployed and enforced.

Recommendation Number 5: Establish security settings for each system and application so that only authorized individuals have access.

Response: The Secretary of State's office has taken corrective action to meet the recommendations of this finding by establishing new security policies using the recently adopted State IT Security standards as a basis. Specifically, among other things, we have ensured that test ID's and employee access lists are updated immediately upon a change, that all office computers now require a lockout period of inactivity, and that password controls are strengthened as further discussed herein. These policies are reviewed on an annual basis or when significant changes have occurred.

Recommendation Number 6: Strengthen password controls to prevent unauthorized access to information, including dial-in access.

Response: To meet the requirements of this finding, the Secretary of State's office has adopted the minimum standards set forth by the State IT Security Committee and has exceeded those minimums where required by our IT Department. These policies are reviewed on an annual basis or when significant changes have occurred.

Recommendation Number 7: Provide better protection of credit card information.

Response: No one would argue with the recommendation to "provide better protection of credit card information." In 1995, the Secretary of State pioneered the acceptance of credit cards in Nevada. This Agency has always treated credit card security and usage with the same level of security as any negotiable instrument. However, we take exception to the comment . . . "credit card information should not be allowed to remain in inadequately secured locations" (p. 19).

The locations being referred to are not "inadequately secured." We have not had a single instance of credit card impropriety since credit cards were authorized in 1995. The credit card authorization slips are maintained in lockable file cabinets, behind closed doors, and access is limited to "authorized employees only." The public is isolated in a completely separate room. However, we also recognize that in a paper-based world, where a working file can be 18 months old, a lockable file cabinet in a secure location is not the best system. Therefore, built into our eSoS system are significant security authorization rules and regulations. The eSoS system is paperless. High level authorization codes and passwords are the only access vehicles to credit card information.

Recommendation Number 8: Create a disaster recovery plan.

Response: The Secretary of State's office recognizes we are vulnerable to some type of disaster occurring. Our IT Department has attempted to mitigate this vulnerability by initiating the development of a comprehensive Disaster Recovery Plan that will clearly define the steps required, personnel responsibilities, critical data to recover, and identify a remote hot site. It also includes a rigorous test plan. We will coordinate with other agencies where required, as well as internally. Once this plan has been developed, implemented and tested, the results will be made available for your review. This Disaster Recovery Plan will be tested on an annual basis or when significant changes have occurred.

Recommendation Number 9: Store all backup tapes at the designated offsite location.

Response: This recommendation is a snapshot of an isolated event. The audit report reads:

While some backup tapes are stored at an off-site location, the tapes for the UCC and the Accounting system data were stored within the computer room. Staff indicated they simply had not transferred the tapes to the off-site location . . .Based on our inquiries, staff moved the tapes offsite (p. 20).

Our backup tapes are a high priority for the Technology Division within our office. The event being described occurred during the migration from one operating system to an upgraded operating platform suitable for the new eSoS UCC and Accounting systems. Phase 2 of eSoS required significant software and hardware computer system enhancements. The upgraded system proved incompatible with our older nightly tape backup system. Due to the nature of our mission critical computer systems, backup runs occur only at night. Any problems with a backup must be corrected at night. The auditors arrived during a three-day tape backup crisis. It should be noted that as soon as a successful backup tape run was performed the auditors noted: "staff moved the tapes off-site."

The IT Department has created a Tape Backup Log to identify the rotation of backups. This log also identifies those backup tapes that are off-site. In addition, each month end tape will be stored off-site.

Recommendation Number 10: Periodically, update the list of employees who are authorized to access the off-site storage tapes.

Response: We have instituted new procedures to maintain the list of employees authorized to access the off-site storage tapes.

We appreciate the mid-project audit report and the level of professionalism your staff brought to our office. We will soon deploy Phases 2.5 through 5 of our eSoS project and believe that the contributions of your staff during the audit process can only serve to assist us in developing an enhancing our eSoS product.

Respectfully submitted,

DEAN HELLER
Secretary of State

Renee L Parker
Renee L. Parker
Chief Deputy Secretary of State

Office of Secretary of State Response to Audit Recommendations

Recommendation Number		Accepted	Rejected
1	Ensure contract provisions are monitored and consistently applied, including documentation, design, and testing	X	
2	Maintain an on-site project manager and appropriate quality assurance function.	X	
3	Plan, write, and execute a comprehensive agency security plan that complies with applicable State of Nevada IT Security Standards, as well as other prudent industry guidelines.	X	
4	Designate an Information Security Officer with assigned responsibility to coordinate and help execute the security plan	X	
5	Establish security settings for each system and application so that only authorized individuals have access	X	
6	Strengthen password controls to prevent unauthorized access to information, including dial-in access	X	
7	Provide better protection of credit card information	X	
8	Create a disaster recovery plan	X	
9	Store all backup tapes at the designated off-site location.	X	
10	Periodically update the list of employees who are authorized to access the off-site storage tapes	X	
	TOTALS	10	0