Audit Highlights

Highlights of Legislative Auditor report on the Office of Secretary of State, issued on May 7, 2003. Report #LA04-03.

Background

The Secretary of State is a constitutional officer elected to a 4-year term. The Office of Secretary of State (Agency) encourages the development and diversification of the state's business community by providing services to businesses wishing to organize under the laws of Nevada. In addition, the Agency maintains and makes records and information filed with it easily and promptly accessible. Furthermore, the Agency protects the state's citizens against investment fraud.

At the end of fiscal year 2002, the Agency reported total revenues of $53.4 million and expenditures of $8.5 million. 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 of Audit

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.

Audit Recommendations

This report contains 10 recommendations to improve the security and reliability of the information systems at the Office of Secretary of State. These recommendations include ensuring contract provisions are monitored and consistently applied, creating a security plan, and designating a security officer. In addition, we recommend improving controls over system access and providing better protection for credit card information. Furthermore, we recommend providing better controls over disaster recovery and backup.

The Office of Secretary of State accepted all 10 audit recommendations.

Status of Recommendations

The Agency's 60-day plan for corrective action is due on August 1, 2003. In addition, the six-month report on the status of audit recommendations is due on February 2, 2004.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Office of Secretary of State

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. Agency management has taken steps to correct these concerns.

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.

The Agency should develop a formal security plan. Information technology standards 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.

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. In addition, computers were not locked out after a period of inactivity, and one ex-employee still had network access. Also, there was no formal process for granting system access.

Appropriate password controls have not been consistently applied to all users. Our review found that passwords are not always required, or forced to periodically change. In addition, a minimum password length is not required. Agency personnel had recognized these weaknesses and have taken steps to strengthen controls.

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.

The Agency has not created a written disaster recovery plan. In addition, some backup tapes were not stored off-site. Finally, the list to access the off-site storage contained the name of an ex-employee. The Agency has begun strengthening these controls.

Audit Division
Legislative Counsel Bureau