Audit Highlights

Highlights of Legislative Auditor report on the Department of Conservation and Natural Resources, Information Technology Security issued on April 13, 2010. Report # LA10-12.

Background

The Department of Conservation and Natural Resources has an overall mission to conserve, protect, manage, and enhance the state's natural resources in order to provide the highest quality of life for Nevada's citizens and visitors.

The Department consists of a Director's Office and eight divisions and agencies including:

- Division of Conservation Districts
- Division of Environmental Protection
- Division of Forestry
- Natural Heritage Program
- Division of State Lands
- Division of State Parks
- Division of Water Resources
- Commission for the Preservation of Wild Horses

The Department employed 739 full-time equivalent positions and had expenditures of about $87 million during fiscal year 2009.

Purpose of Audit

The purpose of this audit was to determine if the confidentiality, integrity, and availability of the Department's sensitive information and information systems were properly protected. This audit included a review of information technology controls at the Department during calendar year 2009.

Audit Recommendations

This audit report contains 10 recommendations to improve the information security at the Department of Conservation and Natural Resources. These recommendations address controls over confidential information and network availability. In addition, these recommendations address controls over managing network users, network maintenance, and other administrative controls.

The Department accepted the 10 audit recommendations.

Status of Recommendations

The Department's 60-day plan for corrective action is due on July 8, 2010. In addition, the six-month report on the status of audit recommendations is due on January 10, 2011.

Information Technology Security

Department of Conservation and Natural Resources

Results in Brief

The Department of Conservation and Natural Resources substantially complied with state information security standards. However, we identified several areas where controls could be improved. For example, sensitive personal identifying information was stored on agency computers and critical network equipment was not always available. In addition, some former employees retained current network access and information technology staff did not always have background investigations.

Other routine network maintenance and security controls could also be improved. For example, some virus definitions were not current and some software security updates were not installed. In addition, ongoing information security training was not conducted in some divisions and account lockout settings did not limit unsuccessful login attempts. Finally, backup data was not always stored offsite. We noted that the Department corrected most deficiencies prior to completion of the audit.

Principal Findings

Confidential personal information was stored unencrypted on several Department computers. Two human resources computers and four Forestry conservation camp computers contained hundreds of social security numbers that, if inadvertently released, would require the Department to contact the affected persons.

The Department's computer network was sometimes unavailable for employee use due to ongoing problems with the Heating, Ventilating, and Air Conditioning (HVAC) system which resulted in the Bryan Building's server rooms overheating. An automated system that alerted on-call Department of Administration, Buildings and Grounds employees to respond to the problem was not configured to send text messages to the correct cell phone addresses. Therefore, the on-call HVAC staff did not receive the alerts.

Five former employees retained access to the Department's computer network after they had left the service of the Department. These accounts remained enabled from 36 to 423 days after these employees left the Department. State information technology (IT) security standards require the prompt removal of users who are no longer in the Department's service in order to reduce the risk of someone gaining unauthorized access to the state's network and data.

The Department did not conduct routine background investigations on six information technology staff with access to sensitive IT systems. Background investigations are required by state information technology standards to ensure that unsuitable individuals do not gain access to confidential information or sensitive systems.

The Department has adequate procedures for managing virus protection. However, improvements could still be made. Eleven of 760 (1%) computers we sampled did not have current virus protection. The virus definition files on these computers ranged in age from 25 to 619 days old. State IT security standards require that all computers have antivirus software installed and current virus definition files. Without current virus protection, there is increased risk that computers will become infected.

Five of 83 (6%) computers we sampled, did not have critical software security patches installed. If critical software security updates are not installed, there is increased risk that computers will be vulnerable to various hacker attacks and exploits.

Three of the Department's eight divisions did not conduct annual security awareness training as required by state information security standards. Without annual information security refresher training, there is greater risk that employees will not adequately protect state information systems and data.

The Natural Heritage Program's backup data was not stored in an offsite location but rather on a portable flash memory drive carried by an employee. Without offsite storage there is a greater risk of disruption of public services if an accident or natural disaster destroys the primary data storage devices.

An Environmental Protection Division network setting allowed unlimited unsuccessful log-in attempts rather than locking the account after three unsuccessful attempts as required by state security standards. By not enabling the account lockout setting, there is increased risk that unauthorized persons could gain access to the state's information systems.

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

Audit Division
Legislative Counsel Bureau