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
Legislative Building
Carson City, Nevada

We have completed an audit of the Department of Conservation and Natural Resources, Information Technology Security. 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 Department's response, are presented in this report.

We wish to express our appreciation to the management and staff of the Department of Conservation and Natural Resources for their assistance during the audit.

Respectfully presented,

Paul V. Townsend, CPA
Legislative Auditor

March 17, 2010
Carson City, Nevada

STATE OF NEVADA
DEPARTMENT OF CONSERVATION AND NATURAL RESOURCES
INFORMATION TECHNOLOGY SECURITY

AUDIT REPORT

Table of Contents

EXECUTIVE SUMMARY

DEPARTMENT OF CONSERVATION AND NATURAL RESOURCES
INFORMATION TECHNOLOGY SECURITY

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

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.

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. (page 7)

- 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. (page 8)

- 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. (page 10)

- 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. (page 10)

- 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. (page 11)

- 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. (page 11)

- 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. (page 12)

- 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. (page 12)

- 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. (page 12)

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. (page 17)

Agency Response

The Department, in the response to the audit report, accepted the 10 recommendations. (page 16)

Introduction

Background

The Department of Conservation and Natural Resources consists of the Director's Office and eight divisions and agencies with a 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 eight divisions and agencies include:

- **Division of Conservation Districts**: The Division provides administrative support to the State Conservation Commission which develops policy and regulations for the state's 28 locally elected conservation districts. Conservation districts provide services to individual land owners and coordinate with other public and private agencies for the protection and orderly development of the state's renewable resources.
- **Division of Environmental Protection**: The Division is responsible for implementation of environmental regulatory programs designed to protect public health and the environment.
- **Division of Forestry**: The Division provides professional natural resource and fire services to Nevada citizens to enhance and protect forest, rangeland and watershed values; conserve endangered plants and other native flora; and provide effective statewide fire protection and emergency management.
- **Natural Heritage Program**: The Program maintains comprehensive information on the location, biology, and conservation status of all endangered, threatened, sensitive, and at-risk species in the state, as well as vegetation and wetland community databases.
- **Division of State Lands**: The Division serves as the land office for the state's lands, with the exception of land owned by the Legislature, University System, and the Department of Transportation.
- **Division of State Parks**: The Division acquires, protects, develops, and interprets a well-balanced system of areas with outstanding scenic, recreational, scientific, and historical importance for the inspiration, use, and enjoyment of Nevada's citizens and visitors in order that such areas shall be held in trust as irreplaceable portions of Nevada's natural and historical heritage.
- **Division of Water Resources**: The Division works to protect the health and safety of Nevada's citizens and visitors through appropriation and adjudication of public water.
- **Commission for the Preservation of Wild Horses**: The primary duty of the Commission is to preserve viable herds of wild horses on public lands in Nevada. The Commission also serves as an advocate for wild horses

through participation with federal agencies to ensure that sufficient habitat is available for wild horse populations.

In fiscal year 2009, Department expenditures were about $87 million. In all, the Department had 739 full-time equivalent positions as well as numerous seasonal staff. The Department has locations such as state parks and forestry conservation camps located statewide with its primary locations in Carson City and Las Vegas.

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 information technology controls at the Department of Conservation and Natural Resources during calendar year 2009. The objective of our audit was to determine if the Department's information security controls were adequate to protect the confidentiality, integrity, and availability of its sensitive information and information systems.

Findings and Recommendations

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 (IT) 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.

Personal Identifying Information Was Vulnerable

The Department stored personal identifying information on some of its computers without a valid business necessity for the information. In addition, the information was not encrypted. Personal Identifying Information is often collected and stored on state computers in the course of doing business. Such information can include names, social security numbers, driver license numbers, and other confidential personal information that, if not protected, could lead to identity theft. However, collection of this confidential information should be restricted to valid business necessities and the information should be encrypted when stored.

Employee Social Security Numbers Were Stored on Local Computers

Department employee social security numbers (SSN) were stored unencrypted on both the Forestry Division and the Environmental Protection Division human resources computers. We found that Forestry was storing 213 employee SSNs while Environmental Protection was storing 251 employee SSNs. This same information can be accessed from the state's Human Resources Data Warehouse (HRDW) which is the

proper repository of that data. Management indicated that they have since eliminated one database containing the SSNs and plan to address the other by March 16, 2010.

Inmate Workers' Social Security Numbers Were Included in Conservation Camp Payroll Systems

Four of the nine Forestry conservation camps stored hundreds of inmate social security numbers on their local computers as part of their inmate payroll system. Forestry Division conservation camps pay inmates to help fight fires and inmate SSNs were used as part of the inmate payroll system. However, Division employees stated that inmate SSNs were no longer needed. According to staff, the SSNs remained from the time the payroll application was developed internally by one of the conservation camp supervisors. Department management stated that the inmate payroll system has since been revised to exclude inmate SSNs.

Local storage of employee and inmate SSNs increases the risk of unauthorized disclosure of the information. State law requires agencies that inadvertently release such information to contact the affected persons, a potentially time consuming and costly process.

Recommendation

1. Remove social security numbers stored on local computers.

Critical Information Systems Equipment Was Periodically Unavailable

The Department's computer network was not always available. The four network server rooms for the Department's divisions located in the Carson City Richard Bryan Building have been subjected to ongoing overheating problems. This has resulted in the network being unavailable for building employees. A basic requirement of any information security program is maintaining the availability of information systems so employees can perform their work.

Since December 2006, the Bryan Building's network server rooms have overheated five times. This resulted from the malfunctioning of the Heating, Ventilating, and Air Conditioning (HVAC) system that cools the network equipment located in these server rooms. These server rooms generate much heat and require constant cooling. As a result, these overheating episodes have caused the shutdown of key network equipment. Because of this, Bryan Building employees were sometimes not able to

access computing resources that are necessary to perform their work. For example, according to agency personnel, some mission critical network resources, such as the Geographic Information System (GIS), were unavailable for seven days. During another overheating event, some hard drives overheated and were destroyed. The root cause of the overheating problem has not yet been identified by employees at the Department of Administration, Buildings and Grounds Division (B&G) who are responsible for maintaining the cooling system. However, the impact of these shutdowns could be minimized.

The Bryan Building's HVAC system is setup to notify responsible parties when malfunctions are detected. This notification system sends a text message to the cell phones of on-call Buildings and Grounds HVAC employees. This allows them to respond to the alerts and reset the HVAC system. The text messages are sent to specific cell numbers, much like e-mails are sent to specific addresses. In September 2008, B&G changed their cellular service provider. This change required text messages be sent to new addresses. However, the HVAC notification system was not updated with the new addresses. Therefore, no messages were received by B&G employees. Based on our inquiries, Buildings and Grounds staff have updated and tested the Bryan Building's HVAC on-call notification system during January 2010. Updating the text message addresses will allow the notifications to reach the appropriate individuals.

Recommendations

2. Coordinate with Buildings and Grounds management to further examine the server rooms' overheating problem.
3. Coordinate with Buildings and Grounds management to periodically test the Bryan Building's on-call notification system to ensure that text messages are sent to the correct on-call support employees.

Weaknesses Exist in Managing Network Users

The Department did not always remove former employees' network access. In addition, the Department did not conduct background investigations on some

employees. These weaknesses increase the risk of unauthorized individuals gaining access to sensitive information.

Former Staff Had Current Network Access

We identified five enabled network accounts of former employees. These accounts remained enabled from 36 to 423 days after these employees left the Department. State standards require agencies to maintain a list of users that should be kept secure and up-to-date. State security policy also requires agencies to conduct quarterly reviews of user lists to ensure they are up-to-date. Four of these accounts remained enabled because IT staff indicated they did not get the termination notifications to disable the accounts.

If former employees' access to an agency's network is not revoked in a timely manner, there is a risk those former employees could gain unauthorized access to the agency's data.

Background Investigations Were Not Conducted on Some Information Technology Staff

We identified six information technology staff members who did not have background checks. Granting people access to sensitive data without background investigations increases the risk that unsuitable individuals could gain access to sensitive information, use it inappropriately, or destroy it. State standards require agencies to conduct background investigations on employees with access to sensitive information. Department management indicated background investigations were not completed for a variety of reasons, depending on the division, including a lack of awareness of the policy and associated procedures for completing a background check, a belief existing staff was "grandfathered", and even budgetary restrictions.

Department management stated they have since initiated background investigations on the staff we identified. In addition, management plans to adopt a policy to include background investigations on all newly hired IT staff.

Recommendations

4. Conduct quarterly reviews of network user accounts as required by state information security standards to ensure all former employee accounts are disabled.

5. Ensure individuals with access to sensitive information have background investigations in accordance with state security standards.

Routine Network Maintenance Needs Improvement

Routine maintenance needs greater attention to ensure adequate security is maintained. This includes ensuring virus protection is current and that operating system security updates are installed.

Virus Definitions Were Not Up-To-Date

The Department has adequate procedures for managing virus protection. However, improvements could still be made. Eleven of 760 (1%) computers we sampled lacked adequate virus protection. These virus definition files ranged from 25 to 619 days old. State security standards require that all computers have antivirus software installed and that virus protection software and definition files be updated as new releases and updates become available.

IT staff indicated some computers' virus problems were caused by an incompatibility with Windows updates that were installed the same day the last virus definitions were installed on the affected computers. Without current virus protection, there is increased risk that computers will become infected and unavailable for employees to use in performing their jobs.

Security Updates Were Not Always Installed

Five of 83 (6%) computers we sampled, did not have critical software security patches installed. Three of the five computers missing updates were located at Forestry conservation camps that are less likely to receive onsite IT support due to their remote locations. The State Lands Division did not closely monitor the update process and therefore was unaware of several failed updates. If critical software security updates are not installed, there is increased risk that computers will be vulnerable to various hacker attacks and exploits.

Recommendations

6. Develop a procedure to detect and correct computers without current virus protection.

7. Develop a procedure to detect and correct failed security update installations.

Other Security-related Controls

We found several other areas where security could be improved. For example, ongoing security training for computer users was not always conducted. In addition, backups of mission critical data were not always stored offsite. Finally, password controls needed strengthening.

Ongoing Information Security Training Was Not Always Conducted

Three of the Department's eight divisions did not conduct annual security awareness training as required by state information security standards. Staff indicated that although they were aware of the need for initial information security training of new employees, they were not aware of the need for ongoing annual refresher training. Without annual information security refresher training, there is greater risk that employees will not adequately protect state information systems and data.

Backup Data Was Not Always Stored Offsite

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. State security standards require mission critical information be backed up and stored offsite. 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. The Department has since informed us that the Natural Heritage Program's backup data is being stored offsite at the Nevada State Library and Archives along with other Department backup data.

Some Password Controls Need Strengthening

An Environmental Protection Division's network setting allowed unlimited incorrect log-in attempts rather than locking the account after three unsuccessful login 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. The Division enabled the lockout setting immediately after we identified the deficiency.

Recommendations

8. Ensure all employees receive annual security awareness training.
9. Store backup data in an approved offsite location.
10. Enforce state information security standards for password controls.

Appendices

Appendix A
Audit Methodology

To gain an understanding of the Department of Conservation and Natural Resources, we interviewed Department management and staff. We reviewed state laws, state information security standards, and the Department's own policies and procedures. We interviewed the Department's information technology staff to gain a broad understanding of the Department's network resources. We discussed how each division's information system is secured.

To ensure our audit tests were representative of the Department's statewide operations, we conducted tests using a judgmental sample of computers selected from the Department's locations throughout the state including several state parks and Forestry Division conservation camps. During our audit, we examined adherence to the state's IT security standards. For example, we tested to determine if ongoing information security training was being provided to employees and if backup data was being stored offsite. We also examined confidential information stored by the Department to determine if it was adequately secured.

To determine if controls over desktop computer security were adequate, we tested desktop computers to ensure they had the latest operating system updates as well as having current virus protection. We also examined the Department's network user accounts to determine if only current employees had access to the Department's networks. We then determined if the Department's IT support staff had background investigations.

To assess the security of the Department's network servers, we tested their security settings. Specifically, we tested to ensure they were configured to enforce state password standards. We also determined if each server had adequate operating system updates and current virus protection installed. In addition, we examined a situation periodically limiting the availability of the Department's computer network.

That situation involved the periodic overheating of network server rooms that caused the shutdown of key network servers.

Finally, we tested controls over the Department's webserver that is used to collect permit and license fees to determine if that system was adequately secured.

Our audit work was conducted from August 2009 through January 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with NRS 218.821, we furnished a copy of our preliminary report to the Director of the Department of Conservation and Natural Resources. On March 15, 2010, 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 B which begins on page 16.

Contributors to this report included:

Jeff Rauh, CIA, CISA	S. Douglas Peterson, CISA
Deputy Legislative Auditor	Information Systems Audit Supervisor

Appendix B

Response from the Department of Conservation and Natural Resources

ALLEN BIAGGI
Director

State of Nevada
Department of Conservation and Natural Resources
Office of the Director
Richard H. Bryan Building
901 S. Stewart Street, Suite 5001
Carson City, Nevada 89701
Telephone (775) 684-2700
Facsimile (775) 684-2715
www.dcnr.nv.gov

JIM GIBBONS
Governor

KAY SCHERER
Deputy Director

Division of Conservation Districts
Division of Environmental Protection
Division of Forestry
Division of State Lands
Division of State Parks
Division of Water Resources
Natural Heritage Program
Wild Horse Program

STATE OF NEVADA
Department of Conservation and Natural Resources
OFFICE OF THE DIRECTOR

March 15, 2010

Mr. Paul Townsend, CPA
Legislative Auditor
401 S. Carson Street
Carson City, Nevada 89701-4747

RE: IT Audit, Department of Conservation and Natural Resources

Dear Mr. Townsend:

As you are aware, an audit was recently conducted on the Department of Conservation and Natural Resources focusing on information technology security.

I have carefully reviewed the audit report and associated recommendations and accept them all as written (see attached checklist). As noted in the report, the majority of these recommendations have already been addressed with changes to systems or policies within the Department.

I would like thank you and your staff for your professionalism and communication in conducting the audit and presenting its recommendations.

Sincerely,

Allen Biaggi, Director
Nevada Department of Conservation and Natural Resources

(NSPO Rev. 1-07)

(O) 1451

Department of Conservation and Natural Resources
Response to Audit Recommendations

Recommendation Number		Accepted	Rejected
1	Remove social security numbers stored on local computers	X	
2	Coordinate with Buildings and Grounds management to further examine the server rooms' overheating problem	X	
3	Coordinate with Buildings and Grounds management to periodically test the Bryan Building's on-call notification system to ensure that text messages are sent to the correct on-call support employees	X	
4	Conduct quarterly reviews of network user accounts as required by state information security standards to ensure all former employee accounts are disabled	X	
5	Ensure individuals with access to sensitive information have background investigations in accordance with state security standards	X	
6	Develop a procedure to detect and correct computers without current virus protection	X	
7	Develop a procedure to detect and correct failed security update installations	X	
8	Ensure all employees receive annual security awareness training	X	
9	Store backup data in an approved offsite location	X	
10	Enforce state information security standards for password controls	X	
	TOTALS	10	0