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
RANDOLPH J. TOWNSEND, *Senator, 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*

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830
PAUL V. TOWNSEND, *Legislative Auditor* (775) 684-6815
DONALD O. WILLIAMS, *Research Director* (775) 684-6825

Legislative Commission
Legislative Building
Carson City, Nevada

We have completed an audit of the Department of Health and Human Services, 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 Health and Human Services for their assistance during the audit.

Respectfully presented,

Paul V. Townsend, CPA
Legislative Auditor

April 22, 2008
Carson City, Nevada

STATE OF NEVADA
DEPARTMENT OF HEALTH AND HUMAN SERVICES
INFORMATION TECHNOLOGY SECURITY

AUDIT REPORT

Table of Contents

EXECUTIVE SUMMARY

DEPARTMENT OF HEALTH AND HUMAN SERVICES INFORMATION TECHNOLOGY SECURITY

Background

The mission of the Department of Health and Human Services is to promote the health and well being of Nevadans through the delivery or facilitation of essential services. Also, the mission is to ensure families are strengthened, public health is protected, and individuals achieve their highest level of self–sufficiency.

The Department of Health and Human Services employs approximately 5,200 employees in numerous locations throughout the state. To accomplish its mission, the Department is organized into various boards, offices, and divisions. Our audit focused on the Department's six major divisions, each of which is responsible for an array of programs. The divisions included were Division for Aging Services (Aging), Division of Child and Family Services (DCFS), Health Division (Health), Division of Health Care Financing and Policy (DHCFP), Division of Mental Health and Developmental Services (MHDS), and Division of Welfare and Supportive Services (Welfare).

Due to the nature of the Department, the divisions deal with Protected Health Information (PHI) and other Personally Identifiable Information (PII). Examples of this type of data include: names, addresses, social security numbers, medical diagnoses, and patient developmental plans. Each of the divisions we reviewed manages its own computer network and each utilizes a combination of network, data, and web servers managed by its own IT professionals with assistance from the Department of Information Technology.

Purpose

The purpose of this audit was to determine if the selected divisions' network resources and data are secure from unauthorized access. The audit included the information technology controls at the Department of Health and Human Services during fiscal year 2007. Divisions included: Aging, DCFS, Health, DHCFP, MHDS, and Welfare.

Results in Brief

The Department of Health and Human Services was largely in compliance with state standards for securing information systems. However, weaknesses existed in controls designed to protect the confidentiality, integrity, and availability of its sensitive data and systems. This included needing greater security over desktop, laptop, and server computers as well as wireless networks. For example, 24 of the 74 laptop computers tested contained unencrypted sensitive information.

Controls over divisions' networks and the sensitive data stored needed strengthening. For example, former employees still had network access, and a report containing sensitive health information was posted on the Internet. In addition, stronger controls are needed over background investigations. These weaknesses increase the risk of unauthorized intrusion into the Department's networks and data.

Principal Findings

- Computers from four divisions within the Department were missing critical software security updates. We found 62 of the 424 (15%) computers sampled were missing critical updates. State standards require agencies to demonstrate a process in progress for installing these updates within three working days of

their release. As vulnerabilities in a system are discovered, attackers may attempt to exploit them, thereby gaining unauthorized access to data and other network resources. (page 10)

- Computers from five divisions lacked adequate antivirus protection. Sixty of 424 (14%) computers sampled did not have current antivirus protection. State standards require antivirus software be updated as new virus definitions become available. Unprotected computers are at risk of viruses and other threats that could result in harm to data. (page 12)

- In four divisions we found 24 of 74 (32%) laptop computers sampled contained unencrypted PHI or PII of clients. State standards require that this information be encrypted. Theft or loss of one of these laptops would risk the exposure of this data and necessitate notifying the individuals whose data was compromised. (page 14)

- To ensure that data cannot be recovered from computers that are surplused, special software should be used that sanitizes or securely erases a drive's data. DCFS and Aging Services only format or partition their computer hard drives before donating them to third parties. Donated computers could contain sensitive or confidential data that could be recovered and used for identity theft. (page 15)

- MHDS had posted on its website a report entitled, "2006 MHDS PASRR Program Compliance Review Report." This report contained personal information and diagnoses of many clients. Most of the information had been redacted. However, information for seven clients was still visible. MHDS subsequently removed the report and notified the affected parties. (page 15)

- MHDS uses wireless connections at various locations. Standards require wireless communications to have strong encryption to prevent unauthorized eavesdropping of the sensitive data being broadcast over the wireless network. We found 19 wireless access points using weak encryption when connected with the division's computers. Confidential data is at risk when broadcast over an improperly configured wireless network. (page 16)

- Laptop computers frequently have wireless network hardware pre-installed. This hardware can allow laptop users to connect to networks without using cable connections. However, if a laptop's wireless network card is not securely configured, the laptop can inadvertently and automatically connect to an unknown network, thereby allowing unauthorized individuals access to data on the laptop and division networks. We found five Health Division laptops and one MHDS laptop had wireless network cards activated without any security features enabled. These laptops were attempting to connect with any wireless device within range including non-state networks. (page 17)

- Sixty-four former employees in five of the six divisions had network access for as long as 29 weeks after leaving the Department. State standards require agencies to maintain a current list of employees with access and keep it up-to-date. If former employee access to a division's network is not revoked in a timely manner, there is a risk those employees could gain unauthorized access to division data. (page 18)

- DCFS had not appointed an Information Security Officer as required by state standards. It is the ISO's responsibility to ensure state IT security standards are enforced in the divisions. Without an ISO, it is less likely that IT security standards will be implemented or that other IT security issues will be addressed in an effective manner. (page 19)

- Welfare and DCFS allowed programmers to update production databases in order to fix data issues. However, there were no controls in place to ensure that changes to the databases were authorized. Accidental or intentional manipulation of the database could go unnoticed. (page 20)

- Some division network servers were not secured in a locked room as required by state standards. Unrestricted physical access to these critical network components increases the risk of accidental damage and theft or vandalism of these computers. Loss of one of these critical network infrastructure computers could result in release of confidential data. (page 20)

- Passwords ensure only authorized individuals have access to an agency's network and data. State standards require agencies to implement strong password controls. However, we found weak controls at DCFS and MHDS. This included allowing users too many login attempts, weakly constructed passwords, password expiration greater than 90 days, and allowing passwords to be re-used within too few generations. (page 21)

- Both Aging and MHDS had not completed background investigations on IT staff members as required by state standards. Background investigations ensure that persons with a criminal history do not gain access to sensitive state data and equipment. (page 21)

Recommendations

This audit report contains 13 recommendations to improve information security at the Department of Health and Human Services. These recommendations will help ensure greater security over desktop, laptop, and server computers as well as wireless networks. In addition, they provide better protection over the various divisions' networks and sensitive data. Furthermore, the recommendations will help Department staff in overseeing programmer access to data, and in promptly removing former employees' network access. (page 36)

Agency Response

The Department, in response to out audit report, accepted the 13 recommendations. (Page 27)

Introduction

Background

The mission of the Department of Health and Human Services is to:

> **Promote the health and well being of Nevadans through the delivery or facilitation of essential services. To ensure families are strengthened, public health is protected and individuals achieve their highest level of self–sufficiency.**

To accomplish its mission, the Department is organized into various boards, offices, and divisions. Our audit focused on the Department's six major divisions, each of which is responsible for an array of programs. Responsibilities of these divisions include:

- **Division for Aging Services (Aging)**: Tasked with developing, coordinating, and delivering a comprehensive support service system which will allow Nevada's senior citizens to lead independent, meaningful, and dignified lives.
- **Division of Child and Family Services (DCFS)**: Provides support and services to assist Nevada's children and families in reaching their full human potential. The division pursues this mission in partnership with the families, communities, and other governmental agencies.
- **Health Division (Health)**: Promotes and protects the health of Nevadans and visitors to the state through its leadership in public health and enforcement of laws and regulations pertaining to public health. To take such measures necessary to prevent the spread of sickness and disease.
- **Division of Health Care Financing and Policy (DHCFP)**: Works in partnership with the Centers for Medicare and Medicaid Services to assist in providing quality medical care for eligible individuals and families with low incomes and limited resources. Services are provided through a combination of traditional fee-for-service provider networks and managed care.
- **Division of Mental Health and Developmental Services (MHDS)**: Works in partnership with consumers, families, advocacy groups, agencies, and communities to provide responsive services and informed leadership to ensure quality outcomes.
- **Division of Welfare and Supportive Services (Welfare)**: Provides quality, timely, and temporary services enabling Nevada families, the disabled, and elderly to achieve their highest levels of self-sufficiency.

Due to the nature of the Department, the divisions deal with Protected Health Information (PHI) and other Personally Identifiable Information (PII). Examples of this type of data include: names, addresses, social security numbers, medical diagnoses, and patient developmental plans. This type of information is considered sensitive data

under the Health Insurance Portability and Accountability Act (HIPAA) and as such is subject to privacy and security controls as outlined in the Act. Each of the divisions we reviewed manages its own computer network and each utilizes a combination of network, data, and web servers managed by its own information technology (IT) professionals with assistance from the Department of Information Technology (DoIT). In this audit, we did not review specific applications. Rather, we evaluated controls over computers, network hardware, and data at each division.

The Department of Health and Human Services employs approximately 5,200 employees in numerous locations throughout the State. The six divisions of the Department of Health and Human Services that we audited had combined expenditures of more than $2.4 billion. Exhibit 1 shows the divisions' expenditures for fiscal year 2007.

Exhibit 1

Expenditures by Division
Fiscal Year 2007

Division	Expenditures
Aging	$ 37,168,374
DCFS	178,910,529
DHCFP	1,390,079,875
Health	155,380,237
MHDS	271,190,378
Welfare	403,971,577
Total Expenditures	**$2,436,700,970**

Source: State's Accounting System.

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 the 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 the information technology controls at the Department of Health and Human Services during fiscal year 2007. Divisions included: Aging

Services, Child and Family Services, Health, Health Care Financing and Policy, Mental Health and Developmental Services, and Welfare and Supportive Services. The objective was to determine if the selected divisions' network resources and data are secure from unauthorized access.

Findings and Recommendations

Computers Need Critical Updates

Managing critical software updates is a vital process that can help alleviate many of the challenges of securing computer systems. As vulnerabilities in a system are discovered, attackers may attempt to exploit them, possibly causing significant damage. Malicious acts can range from defacing websites to taking control of entire systems with the ability to read, modify, or delete sensitive information. State standards require agencies to demonstrate a process in progress for installing critical security updates within three working days of their release.

Computers from most divisions within the Department were missing critical software security updates. These included desktop and laptop computers, and servers. We identified computers missing critical updates that were released over one month prior to our test.

Desktop Computers

Of 313 desktop computers tested, 49 (16%) were missing at least one critical update. Exhibit 2 shows the number of desktop computers, by division, that were missing these updates.

Exhibit 2

Desktop Computers Missing Critical Updates

Division	Number of Desktops
Aging	0
DCFS	14
DHCFP	0
Health	1
MHDS	3
Welfare	31
Total	**49**

Source: Results of audit testing.

Laptop Computers

Of 74 laptop computers tested, 8 (11%) were missing at least one critical update. Exhibit 3 shows the number of laptop computers, by division, that were missing these updates.

Exhibit 3

Laptop Computers Missing Critical Updates

Division	Number of Laptops
Aging	0
DCFS	5
DHCFP	0
Health	2
MHDS	0
Welfare	1
Total	**8**

Source: Results of audit testing.

Servers

Of 37 servers tested, 5 (14%) were missing at least one critical update. Exhibit 4 shows the number of servers, by division, that were missing these updates.

Exhibit 4

Servers Missing Critical Updates

Division	Number of Servers
Aging	0
DCFS	0
DHCFP	0
Health	2
MHDS	0
Welfare	3
Total	**5**

Source: Results of audit testing.

Throughout our testing, multiple causes surfaced for each area we reviewed. For example, some divisions did not closely monitor the security update process. They were therefore unaware that some computers did not get updated. In addition, the geographic dispersion of division networks around the state made monitoring of the update process more difficult.

Recommendation

1. Develop a procedure to monitor software update installation and detect failed or missing update installations.

Antivirus Protection Was Lacking on Some Computers

State standards require antivirus software be installed on each computer to protect against computer viruses. State standards also require that all agencies update virus definition files as updates become available. These definition files allow the software to more easily identify viruses and maintain protection from current threats.

Desktops, laptops, and servers within the divisions were lacking adequate virus protection. This included 54 computers that had antivirus software installed but did not have current virus definitions. Twenty-nine of these computers had virus definitions over three months old. In addition, six computers had no antivirus software installed.

Desktop Computers

Of 313 desktop computers tested, 38 (12%) were lacking adequate virus protection. Exhibit 5 shows the number of desktop computers, by division, that were lacking adequate virus protection.

Exhibit 5

Desktop Computers Without Current Antivirus Protection

Division	Number of Desktops
Aging	0
DCFS	10
DHCFP	0
Health	1
MHDS	21
Welfare	6
Total	**38**

Source: Results of audit testing.

Laptop Computers

Of 74 laptop computers tested, 19 (26%) were lacking adequate virus protection. Exhibit 6 shows the number of laptop computers, by division, that were lacking adequate virus protection.

Exhibit 6

Laptop Computers Without Current Antivirus Protection

Division	Number of Laptops
Aging	0
DCFS	4
DHCFP	0
Health	4
MHDS	5
Welfare	6
Total	**19**

Source: Results of audit testing.

Servers

Of 37 servers tested, 3 (8%) were lacking adequate virus protection. Exhibit 7 shows the number of servers, by division, that were lacking adequate virus protection.

Exhibit 7

Servers Without Current Antivirus Protection

Division	Number of Servers
Aging	1
DCFS	0
DHCFP	0
Health	1
MHDS	1
Welfare	0
Total	**3**

Source: Results of audit testing.

The reasons for inadequate antivirus protection varied by division. In one case, MHDS' Rural Clinics, IT staff indicated they had lost the password to their antivirus server application and were unable to perform actions needed for proper operation of the antivirus system. When we alerted management of this problem, other IT staff were able to fix the problem.

Other antivirus definition problems were caused by changing the name of the server hosting the antivirus system software without redirecting the individual computers to the newly renamed server to receive periodic virus definition updates. IT staff were unaware of these configuration problems until we brought them to their attention.

Recommendation

2. Create an adequate review process to ensure computers have antivirus programs installed and that virus definitions are updated frequently.

Sensitive Information Was Not Always Protected

The Department of Health and Human Services is responsible for recording, processing, and storing large quantities of data. Much of this data is sensitive information that includes client names, addresses, social security numbers, treatment plans, and medical information. Information of this type is often referred to as PHI or PII. State laws and standards require the Department and its various divisions to protect this information.

Staff at Aging, DCFS, MHDS, and Welfare divisions use laptop computers to store PHI or PII of patients and clients. Our testing found that sensitive data was not encrypted, surplus computers were not securely erased, and a report with protected health information was posted on the Internet that contained PHI of several patients.

During December 2005, MHDS' Desert Regional Center had a break-in where 20 laptops were stolen that had unencrypted PHI of over 500 patients. This incident highlights the need for security over laptop computers. The Center followed proper protocol in notifying all affected patients. However, this example points out the risks to individuals and the cost and time to properly notify affected parties. State standards require that access to data considered sensitive or private be controlled by the use of digital identity devices, encryption software, or evolving identity methods.

Laptop Computers Contained Unencrypted Sensitive Information

Encrypting data on computers ensures that information is protected, even if lost or stolen. Of 74 laptops tested, 24 (32%) contained unencrypted PHI or PII data. Exhibit 8 shows the laptops, by division, without proper encryption.

Exhibit 8

Laptop Computers with Unencrypted Sensitive Information

Division	Number of Laptops
Aging	1
DCFS	4
DHCFP	0
Health	0
MHDS	18
Welfare	1
Total	**24**

Source: Results of audit testing.

Some individuals were unaware that encryption software is built into the Windows XP operating system and can be implemented without any additional cost.

Some Computer Drives Not Properly Sanitized

Various Department's divisions often donate older surplus computers to state approved non-profit organizations. It is the divisions' responsibility to remove any sensitive information contained on these computers before donating them. To ensure that data cannot be recovered, special software should be used that sanitizes or securely erases a drive's data.

Four divisions properly use sanitation software that renders the data unrecoverable. However, DCFS and Aging Services do not adequately sanitize the hard drives on donated computers. Files from these drives can still be recovered using data recovery software.

Report With Protected Health Information Was Posted on Internet

While reviewing the Department's website, we found a report containing PHI of several clients. This report entitled, "2006 MHDS PASRR Program Compliance Review Report," was posted onto the website by MHDS. Although most of the sensitive information in the report had been redacted, we found seven patients' names, four of which included patients' diagnoses. This report was accessible by anyone on the Internet. State standards require agencies to provide adequate protection of data. MHDS subsequently removed the report and notified the affected parties.

Recommendations

3. Encrypt all sensitive data stored on laptop computers in accordance with the state standard.
4. For each division, require the use of data sanitation software to overwrite computer drives before disposal.
5. Establish a review process in each division before information is posted on websites.

Wireless Controls Need Improvement

Wireless communication allows users the freedom to move around an office with their computers while staying connected to a network. This is made possible through the computer's wireless hardware communicating with a device known as an "access point" which is connected to a network. This communication takes place by broadcasting the data via radio waves. However, there are risks associated with this technology that could allow unauthorized access to an agency's network and data when wireless devices are not securely configured.

We found one access point that had no security controls. In addition, many access points used weak encryption to protect broadcast data. Furthermore, some laptop computers had the built-in wireless hardware unnecessarily turned on, thus creating the potential for inadvertent connections with non-state networks.

Wireless Devices Not Configured Securely

The access point of a wireless network is where security configuration settings are enabled. These settings can include encryption of data being broadcast between the access point and the remote computer, disabling the broadcast of an access point's identification, and limiting connection with the access point to specified computers.

One MHDS access point in Carson City had no security features enabled. Staff indicated this access point was operating approximately two years in this condition. Once alerted of this condition, the IT staff made configuration changes to the access point to make it more secure.

Another MHDS access point in Carson City had adequate security except for the type of encryption used. It used older Wired Equivalent Privacy (WEP) encryption that

has known vulnerabilities instead of newer encryption technology known as Wi-Fi Protected Access (WPA or WPA2) which is considered much more secure.

The MHDS' Southern Nevada Adult Mental Health Services (SNAMHS) and the Rawson-Neal Hospital complex in Las Vegas use a wireless network to cover the campus. This wireless network uses 17 wireless access points to allow staff with laptop computers to access the network. This network also uses older WEP encryption rather than the newer and more secure WPA or WPA2 encryption.

MHDS IT management indicated they had mitigated the risk of the SNAMHS wireless network by careful placement of the access points so that the wireless signals could not broadcast more than a few feet from the buildings in which they were housed. However, during our testing we picked up the wireless signals of 15 of the 17 access points from the public parking lot of the Rawson-Neal Hospital and the roads leading around the SNAMHS campus. This indicated that the physical placement of the access points was not an effective measure to prevent the wireless signals from being broadcast beyond the campus buildings.

We found another wireless network on this same Las Vegas campus that was securely configured and used the stronger WPA encryption. This network belonged to the MHDS' Desert Regional Center.

Wireless Was Enabled on Some Laptop Computers

Laptop computers frequently have wireless network hardware pre-installed. This hardware can allow laptop users to connect to networks without using cable connections. However, this wireless hardware also presents risks. If a laptop's wireless network card is not securely configured, the laptop can inadvertently and automatically connect to an unknown network, thereby allowing unauthorized individuals access to both data on the laptop and the data on the network the laptop is connected to.

One means of reducing this risk is for IT staff to disable unneeded laptop wireless cards before the computers are issued to employees. IT staff have the ability to disable a laptop's wireless networking function such that the wireless network card cannot be re-enabled by the laptop user. However, if there is a business need to use wireless networking, then proper training and oversight are needed.

We found five Health Division laptops and one MHDS laptop had wireless network cards activated without any security features enabled. These laptops were attempting to connect with any wireless device within range including non-state networks.

Recommendations

6. Configure all wireless access points with adequate security, including moving to stronger encryption.
7. Configure laptops with wireless disabled and train staff to not use this feature without proper approval and secure configuration.

Former Employees Had Network Access

User accounts are created for each employee authorized to use an agency's computer network. These user accounts establish the employee's login identification, initial password, and their network access privileges. State standards require the divisions to maintain a list of users and keep it up-to-date. If former employee access to a division's network is not revoked in a timely manner, there is a risk those employees could gain unauthorized access to division data.

We examined user accounts in each division to determine if former employee network accounts had been removed or disabled. Additionally, we reviewed the length of time the accounts remained active. We found 64 former employees with active user accounts in five divisions. These employees were either terminated, left state service, transferred to another agency, or retired. Exhibit 9 shows the number of former employees with access by division.

Exhibit 9

Former Employees With Network Access

Division	Number of Former Employees With Access	Access Period
Aging	1	19 weeks
DCFS	44	From 2 to 29 weeks
DHCFP	3	From 7 to 25 weeks
Health	1	5 weeks
MHDS	15	From 2 to 27 weeks
Welfare	0	N/A
Total	**64**	**Up to 29 weeks**

Source: Results of audit testing.

All agencies should have a process in place to ensure that employee user accounts are disabled immediately upon their separation from employment and remain disabled. Staff in each division indicated that they took immediate action to remove the former employee accounts we identified.

Recommendation

8. Periodically review user accounts to identify former employees who have not had their access disabled.

Other Security-related Controls

We found several other areas where security could be improved. For example, one division did not have an Information Security Officer, while two divisions allowed programmers direct update access to production data. Furthermore, two divisions did not sufficiently limit physical access to servers, and passwords needed strengthening in two divisions. Finally, two divisions had not conducted background investigations on some IT employees.

DCFS Lacks an Information Security Officer

According to state standards, each agency is required to have an Information Security Officer (ISO). This person is responsible for ensuring that state security standards are implemented within the division and that computer users are aware of security policies and procedures.

While five divisions had an ISO, DCFS had no one currently acting in that capacity. DCFS IT management indicated the employee acting as the division's ISO had left employment and a replacement had not yet been selected.

Programmers Had Excessive Access to Production Data

Welfare maintains data on welfare eligibility and recipients using the NOMADS information system. DCFS maintains data on child welfare including items such as adoption and child protective services using the UNITY information system. With the sensitive nature of this data, ensuring appropriate access is critical. Without controlled access, there is increased risk of accidental or unauthorized changes to data.

We found Welfare had 18 programmers and supervisors with the capability to modify production data while DCFS had 7 programmers with the capability to modify production data. The data in the NOMADS and UNITY systems reside on the State's mainframe. Best practices are to restrict the ability to update production data to those groups and individuals who are accountable for maintaining the data. For these two Divisions, this would typically be the case workers who deal with the public and maintain the case files, not the programmers.

Programming staff have been granted update access to the data in order to facilitate making data fixes. This can occur when problems are encountered while running nightly updates or when non-programming staff cannot fix the data. However, there were no controls in place to ensure that changes are only made when authorized. The result is that changes to production data could be made that are unauthorized and difficult to trace.

Controls to Limit Physical Access to Servers Need Improvement

Servers "serve up" information and data to networks, people, and other computers. Common examples include web servers, network servers, and file servers that store files. Because these servers are critical to an agency's network and data, state standards require that these servers be installed in a physically secure locked room and access be limited to only authorized personnel.

We found one DCFS office in Fallon that had a network server that was not secured in a separate locked room, but was accessible to anyone visiting the office. Another DCFS network server in Elko was in an open room with an unbarred window.

In addition, one DHCFP server in Sparks was in a closet with a sliding door located behind the receptionist desk. The sliding door could not be locked and was routinely left open.

In some cases IT staff were unaware of the servers not being in locked rooms since these rural computers were managed remotely. In another case the doors were left unlocked to allow non-IT staff to change backup tapes.

Password Controls Need Strengthening

Password controls ensure only authorized people have access to an agency's computers, network, and data. Network servers at two divisions had weaknesses in password controls. Examples include allowing users too many login attempts and weakly constructed passwords (i.e., passwords that do not use special characters or numbers).

We found one DCFS network server that did not require complex passwords composed of numbers, letters, and special characters as required by the state standard. In addition, that network server set passwords to expire after 365 days instead of the state standard of 90 days. The server settings also allowed passwords to be re-used within too few generations. DCFS IT staff indicated they had inherited this server from another agency and had been unaware of its password settings. In addition, one MHDS network server was set to allow users five unsuccessful login attempts before locking out the account rather than the state standard of three attempts. The MHDS staff were unaware of the state standard and corrected the setting immediately when the issue was identified.

Some Employee Background Investigations Had Not Been Conducted

The Department stores and processes a large amount of sensitive information. This information includes social security numbers, health information, as well as other confidential personal information. State standards require background investigations on those employees with access to this sensitive data so as to reduce the risk of access by individuals with criminal backgrounds.

We found two divisions had not fully complied with the state standard. Aging had not conducted background investigations on all four IT staff, which included one consultant. The IT staff indicated they understood the requirement but had not yet had

the time to submit the required paperwork or fingerprint cards. Also, MHDS had not yet completed background investigations on 4 of its 24 IT staff members. The MHDS indicated that the four remaining background checks were in process but the results had not yet been received.

Recommendations

9. Require each division to appoint, in writing, an Information Security Officer.
10. Create controls over production data such that any programmer changes will be properly reviewed and approved.
11. Review physical controls over servers and ensure access is limited to only those individuals who maintain them.
12. Enforce state standards for password policies.
13. Ensure individuals with access to sensitive information have a background investigation.

Appendices

Appendix A
Audit Methodology

To gain an understanding of the Department of Health and Human Services, we interviewed Department and division management and staff. We reviewed legislation, committee minutes, and state and Department policies. We interviewed the various divisions' information technology employees to gain a broad understanding of the network resources and how they are managed and utilized. We discussed how the divisions interconnect and interact with the Department of Information Technology, other state agencies, and third-party service providers.

We obtained an inventory of computers from each of the divisions. These were used to create a judgmental sample of computers throughout the Department. Factors used to determine the sample included geographic location of offices, type of computers, and technology with greater risk such as wireless networking. Our sample included the Department's statewide operations at 12 locations. The following lists the locations where computers were selected for testing.

1. Carson City
2. Elko
3. Ely
4. Fallon
5. Henderson
6. Las Vegas
7. Pahrump
8. Reno/Sparks
9. Silver Springs
10. Wendover
11. Winnemucca
12. Yerington

During our audit, we examined adherence to the state's IT security standards as well as the Department's and divisions' own IT security policies and procedures.

To determine if controls over computer security were adequate, we tested a sample of 424 of the divisions' computers. The sample included desktops, laptops, and three types of servers including file, network, and web servers. For each computer we tested for current critical operating system updates, current antivirus software and definitions, and erasing of computer drives prior to disposal.

Additional tests were conducted to address the unique risks for each type of computer. For example, tests for laptop computers included checking for unencrypted PHI or PII and evaluating laptop wireless networking capabilities and configurations.

For data servers we examined how access to PHI or PII was restricted. We also reviewed password policies enforced by network servers and how many administrator accounts were present. We examined web servers to determine if default software had been removed. For all servers, we tested how physical access was restricted.

We determined if the divisions had conducted background investigations on IT employees. Furthermore, we tested the process for ensuring network access for former employees is disabled. We also conducted tests to identify 'backdoors' into the network through unauthorized or improperly configured wireless devices. Where wireless networking was implemented, we determined if it was in compliance with state standards. We examined access rights to sensitive data on division data servers and the mainframe and if that access was appropriately restricted.

We determined if the divisions had IT security plans and contingency/disaster recovery plans as outlined in the Governor's Executive Order of 2005. Finally, we determined if each division had appointed an information security officer (ISO), in writing.

Our audit work was conducted between August 2006 and August 2007 in accordance with generally accepted government auditing standards.

In accordance with NRS 218.821, we furnished a copy of our preliminary report to the Director of the Department of Health and Human Services. On April 11, 2008, we met with a Department official to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix C that begins on page 27.

Contributors to this report included:

S. Douglas Peterson, CISA
Information Systems Audit Supervisor

Kimberly Arnett, CPA
Deputy Legislative Auditor

Jeff Rauh, CIA, CISA
Deputy Legislative Auditor

Stephen M. Wood, CPA
Chief Deputy Legislative Auditor

Grant Dintiman, CPA
Deputy Legislative Auditor

Appendix B

Glossary of Terms

Backdoor	Undocumented way of gaining access to a program, online service, or an entire computer system. Examples include unauthorized modems and wireless connections, unauthorized user accounts, as well as network connections generated by the Trojan category of viruses.
File Server	A computer configured to efficiently store and retrieve large amounts of data or files.
Domain Controller	A server that authenticates users on a network and determines permissions to use network resources.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain (clear) text; encrypted data is referred to as cipher text.
Patch	An update to a software program or operating system.
PHI	Protected Health Information as defined in the Health Insurance Portability and Accountability Act (HIPAA).
PII	Personally Identifiable Information such as name, phone number, address, social security number, etc.
Web Server	A computer that delivers (*serves up*) web pages.
Website	A site (location) on the World Wide Web. Each website contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files. Each site is owned and managed by an individual, company, or organization.
WEP	Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. Due to severe weaknesses identified in the protocol, it was superseded in 2003 by WPA.
WPA & WPA2	Wi-Fi Protected Access. The currently accepted standard for securing wireless networks. WPA2 implements the full IEEE 802.11i standard.

Appendix C

Response From the Department of Health and Human Services

JIM GIBBONS
Governor

MICHAEL J. WILLDEN
Director

DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIRECTOR'S OFFICE
4126 Technology Way, Room 100
Carson City, Nevada 89706
Telephone (775) 684-4000 • Fax (775) 684-4010
hr.state.nv.us

April 16, 2008

Mr. Paul Townsend, CPA
Legislative Auditor
Legislative Counsel Bureau
401 South Carson Street
Carson City, NV 89701-4747

Dear Mr. Townsend:

The Department of Health and Human Services accepts all 13 recommendations in your report on our Information Technology Security. The Department has some very competent and capable IT professionals, as I am sure your staff can attest, and this audit will help reinforce the need to stay vigilant in all of the areas revealed in your audit work.

Each Division provided a response to each recommendation that involved them. The combined response is fairly lengthy so I have prepared a separate document that outlines the response from each applicable Division for each recommendation. That document is attached to this response.

Please extend my thanks to your staff for the professional manner with which they conducted themselves and the productive discussions held during the audit process.

Please do not hesitate to let me know if you have any questions or concerns regarding our response.

Sincerely,

Mike Torvinen, CPA
Deputy Director, Fiscal Services

Attachment

Helping People -- it's who we are and what we do

Department of Health and Human Services
Division Responses to LCB Audit on Information Technology Security
May 2008

Recommendation #1: Develop a procedure to monitor software update installation and detect failed or missing update installations.

DCFS will conduct research to determine which procedures have been used by other agencies to successfully monitor software update installation and detect missing update installations. DCFS will implement these procedures and tailor them to meet its needs.

Health Division software is auto updated on desktop and laptop computers that attach to the network. For those users that do not connect to the network we periodically have them bring in their units and update them with the necessary software. For Health Division servers we still run, as required by the Centers for Disease Control and Prevention (CDC), "legacy software". Several of our applications are DOS core based and reside on separate servers. Certain updates have caused this software to stop functioning. As CDC continues updating these legacy applications they are moved to the more current shared environment allowing for critical updates to be applied.

MHDS - A verification process has been developed at the Division level to ensure that updates are current for each server within the Division. This will include date update released, date installed, date verified, and staff who verified. This verification process is to be monthly. PC's will be audited periodically to ensure they are current.

DWSS has implemented an asset tracking and patch management software application to track, inventory and patch all desktop systems on the DWSS network. This solution allows for real-time reporting on Operating Systems (OS) and anti-virus patch levels. The monitoring of these reports is part of the daily procedures for technicians when performing daily and weekly network checks. When deficiencies are found, the technician will run a manual update to bring the machine into compliance. Formal department policy regarding the procedures for ensuring OS critical patch compliance is currently being drafted. It is important to note that even though we have the tools to report discrepancies in patch levels, DWSS may not be able to fully comply with the state standard as we do not currently have the automated tools or the personnel resources to assure all 1,800 PCs and 150 file servers are patched in 72 hours. We use the reporting and management tools to prioritize the releases based on potential risk and try to patch the most critical systems first.

In addition to the above procedures, the division is looking at purchasing an upgrade to the Asset Management product that combines Asset Management, Patch Link and ZEN Works PC Management all into one management tool. This

will combine three current products and allow for more consistent reporting and identification of systems out of compliance. By consolidating the tools, DWSS will be able to increase the percentage of machines that are in compliance.

DWSS uses Novell's Patch Link to keep all our PC's and servers up to date with the current patches offered by all major software manufacturers. For clients to receive patches from the server, they need the Patch Link client installed. The client is installed onto the DWSS corporate image or manually installed onto servers. The devices will then register to the server and be inventoried. At this point an IT technician logs into the Patch Link server and checks the vulnerabilities page to see what systems need patches.

Recommendation # 2: Create an adequate review process to ensure computers have antivirus programs installed and that virus definitions are updated frequently.

DCFS has acquired and will implement Symantec's Endpoint Protection software. This software will give the network technical staff greater ability to manage the security settings of the remote PCs.

Health Division uses SOPHOS as the enterprise antivirus program. It has an auto update feature that allows all units that connect onto the network to be updated within minutes of connection. We also have a couple of systems that do not connect to the network. We periodically have those units checked and updated with the necessary software. For some servers we still run, as required by the Centers for Disease Control and Prevention (CDC), "legacy software". Several of our applications are DOS core based and reside on separate servers. Certain updates have caused this software to stop functioning. As CDC continues updating these legacy applications they are moved to the more current shared environment allowing for critical updates to be applied.

MHDS has set up their servers to download the most recent updates from Symantec every night. All computers that are on and connected to the network are then updated. Computers that are not on or connected are updated the next time they connect to the server. Monthly random checks of at least five computers are performed remotely or when maintenance is performed.

DWSS has implemented Patch Link, a product to manage equipment and the OS, software and anti-virus running on that equipment. The software monitors systems through the network and pushes patches to the machines as necessary. The system allows for patches to be bundled or tested in a "safe" environment before being deployed to thousands of machines, or installed immediately if a situation warrants. This software was deployed in 2007 and we are still tuning

the discovery engine to work with all DWSS approved software. We use the Patch Link reports to verify all machines are up to date and to identify those that need to be updated manually or had problems with the automated installation. These reports are also reviewed by technicians during daily and weekly network health checks. This product is also being replaced by the update mentioned above. The consolidation of these products will allow technicians to look at one report and use one management tool to report, verify, patch and manage all desktops. This update will be a 2010-2011 DWSS budget request.

Aging Service's one server in the Carson City office was identified as lacking virus protection. This was a new server, and it required a different version of Symantec Antivirus software. While antivirus software was installed, the live update function was not running correctly. This has been corrected, and live updates check for updated files on a daily basis. Information on installing antivirus software and ensuring live update is functioning will be added to the Division's Information Technology Policies and Procedures.

Recommendation #3: Encrypt all sensitive data stored on laptop computers in accordance with the state standard.

Aging Services' laptop computers have been checked for Protected Health Information (PHI) and Personally Identifiable Information (PII). By policy, this data is to be retained on network drives not computer hard drives. Microsoft encryption software has been installed, and if data of a sensitive nature is placed on the hard drive of the laptop, it is to be in an encrypted folder. Information on encryption and how to use the software is being added to the Division's Information Technology Policies and Procedures.

DCFS policy has been that no sensitive information be stored on the agency laptops. DCFS will modify this policy to require that all sensitive data stored on laptops is encrypted. Additionally DCFS will provide training to laptop users on how to encrypt data.

MHDS: All laptops have been inventoried and data files have been encrypted with training given the users. That was done at the time of the findings. All staff that use laptops are instructed to leave sensitive information on the agency server and access it with their laptops. Information is not to be downloaded. If there are staff that cannot access the server, the encryption on every laptop will protect the data.

DWSS: During the course of the IT security audit, one DWSS laptop user indicated there was a business need to temporarily store Personal Identifiable Information (PII) on a laptop while in the field. DWSS does not collect PHI and

no PII was found on a DWSS laptop during the LCB audit. However, DWSS recognizes there may be occasions when program staff has a business need to gather sensitive information while in the field, saving the data to the laptop until returned to the office where the data is then deleted from the laptop after saving it to a secure network drive.

DWSS has agreed to utilize the Encrypted File System (EFT) built into Windows XP for temporary storage of files containing sensitive data, such as PII that may be stored on a laptop. Although it is an uncommon practice to store PII on any local device at DWSS, there are some instances where it may be required. Users that have been assigned mobile devices have been instructed how to use EFS if necessary. DWSS prefers all mobile users connect to the DWSS network via secure VPN and only access and store information on the secured network whenever possible. The greatest barrier to compliance is training. The proper storage and network usage policies are not reinforced with training. DWSS has no formal computer or network education. Most users with laptops and other removable devices are not aware of the risks associated with mobile devices and the department does not have the resources to provide technical training to all mobile users.

DWSS is in the process of finalizing the draft mobile device policy, which defines removable media and what content requires encryption. It defines the user's responsibilities and the requirements to assure the device is protected with current antivirus software as well as restrictions to unsecured networks.

In addition to the above procedures, DWSS is evaluating end point security software. This software will monitor all devices as they connect to the network and give detailed audit reports on what locations the PC has been connected from, what content has been viewed or downloaded and allow restrictions to be placed on mobile devices to mitigate unsecured connections.

Recommendation #4: For each division, require the use of data sanitation software to overwrite computer drives before disposal.

Aging Services donates computers to Computer Corps in Carson City as well as to various Senior Centers throughout the state. The data on these computers is wiped clean, and once this cleansing is complete, the Operating System software is reinstalled. Based on the audit results, the IT Unit has downloaded Darik's Boot and Nuke software for overwriting hard drives. This software is advertised to completely delete the contents of any hard drive. Procedures for sanitizing hard drives will be added to the Division's Information Technology Policies and Procedures.

DCFS has obtained "Eraser," free degaussing software. DCFS will develop a policy and procedure for using the software to overwrite computer drives when disposing of or donating surplus PCs.

Recommendation #5: Establish a review process in each division before information is posted on websites.

MHDS - Any information updated to the website is now a two step process. The first level is an author who will prepare the information to be uploaded and will ensure no sensitive information is contained in the update. The information will then be reviewed and approved by another person, called the publisher, who will also audit to ensure no sensitive information is contained in the update. The publisher role is the only one that can place the information onto the website.

Recommendation #6: Configure all wireless access points with adequate security, including moving to stronger encryption.

MHDS - Both Rural Clinics and SNAMHS wireless networks are using the more secure WPA encryption. That was done at the time of the findings. We will secure any other wireless access points established using the most current encryption method available within our budgeted resources.

Recommendation #7: Configure Laptops with wireless disabled and train staff to not use this procedure without proper approval and secure configuration.

Health Division's laptops were purchased by and to perform functions as required by the program's funding agency. The active WiFi is necessary for performing assigned tasks by them. These units do not connect to the network. No sensitive or confidential information is maintained or kept on these units. However, the Health Division will ensure all staff with wireless laptops only use them with proper approval and that the laptops are configured to maximize IT security.

MHDS - One laptop in central office was found with the wireless feature not disabled. All Laptops in central office have been audited and the wireless feature has been disabled. All users have been notified not to use the feature. The laptops will be audited on a random basis to ensure the configuration is secure.

Recommendation #8: Periodically review user accounts to identify former employees who have not had their access disabled.

Aging Services did have one employee whose network access had not been disabled after leaving the agency. The IT staff now performs periodic checks of the Active Directory to ensure that former employee rights are disabled. When it is verified that the employee no longer works for the Division, his/her account is

deleted. Information on building and deleting user accounts and periodic checks will be added to the Division's Information Technology Policies and Procedures.

DCFS-IMS has requested that DCFS-Personnel notify us of terminations when they occur. Additionally, DCFS will periodically review user accounts to ensure that former employees no longer have access to the network.

DHCFP policy requires Supervisors to submit a Security Request form to IT when an employee gives notice. When this is done timely, IT will discontinue access on the employees last day. When Personnel is notified an employee is leaving / transferring they send the Supervisor an information package with includes among other things the Security Request form.

DHCFP will enhance our procedures in two ways to address possible delays in being notified of employee termination / transfer:

1. DHCFP Personnel will notify IT when they send out the termination / transfer package to the Supervisor.
2. On a quarterly bases DHCFP IT send the Agency Chief's a list of employees with active logins. The Chief will respond with any changes / discrepancies to that list.

Health uses Personnel Roster Change forms. These forms are sent through out the agency to inform of personnel staff movement, terminations and changes. Upon receiving the form IT makes the necessary changes in the network. The 1 employee found was immediately corrected.

MHDS – A review of all users' accounts will be done periodically by the Division and information will be provided to each agency for review and action. Each agency has addressed this issue with their Personnel and IT staff.

Recommendation #9: Require each division to appoint, in writing, an Information Security Officer.

DCFS will appoint a Security Officer by May 1, 2008. We are currently trying to make sure we fully understand the skills and responsibilities needed so we can appoint an appropriate staff member.

Recommendation #10: Create controls over production data such that any programmer changes will be properly reviewed and approved.

DWSS has implemented a procedure with the Department of Information Technology (DoIT) to track all after hour's issues requiring DWSS staff to access the production environment. All after hour's events are documented by DoIT, and then reconciled by DWSS Operations including the nature of the event, actions

taken to resolve the issue, and the future mitigation. DWSS has identified the personnel that routinely support after hour's production activities and will begin to restrict access to all accounts based on the level of activity. This analysis, combined with the list of personnel required to access and maintain the production environment during normal business hours, will allow DWSS to significantly reduce the number of staff with production access. Currently all access to production environments are governed by the DWSS Work Item (WI) and Work Order (WO) process. Both processes include documentation of the changes and Deputy/Chief approval prior to scheduled implementation. DWSS will continue to use the after hours report, WI, and WO to evaluate access to production data and develop policies, standards, and procedures to govern access to our production environments.

DCFS currently has a procedure in place that controls the process by which updates are made directly to the database. Anytime a change is needed to the database, a "SPUFI request form" is completed by the requestor and signed by the requestor's supervisor. The request form is forwarded to the IMS Helpdesk where a helpdesk technician validates the appropriateness of the request. If the request is determined to be valid, the helpdesk forwards the request to a programmer who then completes the change. The programmer returns the request form to the helpdesk technician who then verifies the correctness of the programmer's change.

Recommendation #11: Review physical controls over servers and ensure access is limited to only those who maintain them.

DCFS has reviewed the physical controls over our servers. The audit identified a network server in Fallon that was not secured in a separate locked room. The Fallon office does not have a room in which the server could be secured. Consequently, DCFS demoted this server to a file and print server. A server in the DCFS central office facility was promoted to replace the server in Fallon.

The audit also identified a DCFS server in Elko that was in an open room with an unbarred window. The Elko office has relocated and all servers were moved into a secured location.

DHCFP has servers located in a closet in the Reno District Office, which does not have a locking door. Plans are already in progress to move the IT equipment into a room which will meet / exceed all the suggested security requirements. The move will be complete by May '08.

Recommendation #12: Enforce state standards for password policies.

DCFS had one network server that did not enforce state standards for password policies. This server supports the DHHS Director's Office. In December, DCFS network staff notified DHHS Director's Office staff that the standards would be enforced and on January 1, 2008, the standards were enacted.

MHDS - The one DRC server that had allowed users five unsuccessful attempts was changed, at the time of the finding, to the state standard of 3 attempts before lock out.

Recommendation #13: Ensure individuals with access to sensitive information have a background investigation.

Aging Services is in the process of completing Background Check on all IT Staff, which includes three staff and one contractor. This requirement has been added to the Division's Information Technology Policies and Procedures.

MHDS - Three of the four backgrounds checks are successfully completed. The fourth person's background fingerprinting failed due to a medical condition that indirectly affects the fingers and the ability to process the fingerprints successfully. We soon expect improvements in the person's medical condition that will allow them to be re-fingerprinted.

Department of Health and Human Services
Response to Audit Recommendations

Recommendation Number		Accepted	Rejected
1	Develop a procedure to monitor software update installation and detect failed or missing update installations	X	
2	Create an adequate review process to ensure computers have antivirus programs installed and that virus definitions are updated frequently	X	
3	Encrypt all sensitive data stored on laptop computers in accordance with the state standard	X	
4	For each division, require the use of data sanitation software to overwrite computer drives before disposal	X	
5	Establish a review process in each division before information is posted on websites	X	
6	Configure all wireless access points with adequate security, including moving to stronger encryption	X	
7	Configure laptops with wireless disabled and train staff to not use this feature without proper approval and secure configuration	X	
8	Periodically review user accounts to identify former employees who have not had their access disabled	X	
9	Require each division to appoint, in writing, an Information Security Officer	X	
10	Create controls over production data such that any programmer changes will be properly reviewed and approved	X	
11	Review physical controls over servers and ensure access is limited to only those individuals who maintain them	X	
12	Enforce state standards for password policies	X	
13	Ensure individuals with access to sensitive information have a background investigation	X	
	TOTALS	13	0