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*

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

Legislative Commission
Legislative Building
Carson City, Nevada

We have completed an audit of Utilization and Security Over State Internet Sites. 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 of Information Technology's response, are presented in this report.

We wish to express our appreciation to the management and staff of the Department of Information Technology and those state agencies that assisted us during the audit.

Respectfully presented

Paul V. Townsend, CPA
Legislative Auditor

June 7, 2004
Carson City, Nevada

STATE OF NEVADA
UTILIZATION AND SECURITY OVER STATE INTERNET SITES

AUDIT REPORT

Table of Contents

STATE OF NEVADA
UTILIZATION AND SECURITY OVER STATE INTERNET SITES

AUDIT REPORT

Table of Contents
(continued)

EXECUTIVE SUMMARY

UTILIZATION AND SECURITY OVER STATE INTERNET SITES

Background

The Department of Information Technology (DoIT) was created in 1965 and derives its authority from NRS 242. The Department is the state's lead agency for the delivery of effective and efficient information services. All state agencies and elected officers must use DoIT for the design of their information systems, unless exempt by statute.

The Department provides Internet access for the majority of state agencies. Those agencies connect to the Internet through the state's networking infrastructure known as the Silvernet. The Silvernet links approximately 274 distinct agency networks statewide. Each of these networks corresponds to an agency's physical office somewhere in Nevada. Primary locations include Carson City, Las Vegas, and Reno/Sparks, with the remainder located throughout rural Nevada. The State has approximately 198 websites. DoIT hosts approximately 140 of these websites, with the remainder hosted by individual agencies.

Purpose

The purpose of this audit was to determine if controls are sufficient to ensure the security and integrity of the state's computer network, and information stored by agencies. Our audit included a review of controls over the State's Internet security and utilization during calendar year 2003.

Results in Brief

Basic Internet security needs improvement to ensure greater protection over information stored by the State. Improvements are needed over devices that manage the flow of information as it moves throughout the state's network to prevent intrusion. These devices require regular monitoring to ensure adequate security. Another improvement needed is to prevent sensitive information from being placed on various state websites which could lead to unauthorized intrusion into the network. In addition, backup and recovery controls need to be strengthened so data is not lost after a disaster. Furthermore, the State has not prioritized its approach to implementing security procedures.

These weaknesses, if left uncorrected, provide opportunities for malicious users to gain access to the state's computers, or reduce the chances of effectively recovering from a disaster. The Department can overcome these weaknesses by implementing established policies and focusing greater attention on security.

Principal Findings

- A router is a device that contains many rules to manage the flow of network traffic and it is designed to provide security to the state's network. The Department's Internet router is called a border router. We found 12 rules in the router that did not conform with established standards. The overall effect of not conforming to standards is to render the state's network less secure. (page 10)

- A firewall is a device designed to prevent unauthorized access to or from a network. We found that administration of the Department's firewall needs

to be strengthened. First, the firewall was administered by one person who had sole authority to configure the device. This practice renders the system vulnerable to a single point of failure should this person depart the position. Second, procedures for maintaining the firewall have not been formally documented. Third, any firewall settings that do not conform to standards should be documented in a letter of exception. However, we found three special firewall permissions which allowed inbound connections from the Internet that were not documented. (page 11)

- Some state websites contained sensitive information including network diagrams, system administrator names, and floor plans for a building containing critical computer equipment. This information should not be available to the public because it could provide a malicious user (hacker) with useful information in their attempts to penetrate the state's network. (page 12)

- DoIT maintains several computers that contain the websites of approximately 140 state agencies. These computers, called web servers, contained security weaknesses that rendered them vulnerable to attacks. First, the web servers were not located behind the protection of a firewall. Second, staff had not applied software updates or properly set some security settings. By not doing so, there is an increased risk that attackers will use the computers for unauthorized activities. For example, in November 2002 an attack resulted in the creation of computer accounts that would allow unauthorized individuals access to the servers. In addition, the attack resulted in approximately 60 Gigabytes of pornographic and regular movies and images being copied on a state web server. During this period, the server was being used to distribute the movies and images. (page 13)

EXECUTIVE SUMMARY

UTILIZATION AND SECURITY OVER STATE INTERNET SITES

- Network servers are the computers used to run an agency's network. We found security settings on these servers that were not in accordance with state standards. These settings resulted in a less secure network. They included passwords of insufficient length, lack of password complexity, and passwords not changed frequently. In addition, passwords could be reused too frequently, and users were not locked out after three unsuccessful login attempts. We found these weaknesses at the Department of Information Technology and other agencies selected for testing. These agencies included the Department of Personnel, Department of Business and Industry's Insurance Division, and the Department of Human Resources Director's Office. (page 14)

- Users with computers running Microsoft Windows need to periodically use the "Windows Update" feature to install the latest security updates. Of 46 computers we tested at DoIT and selected agencies, 32 needed updating. Twenty-two of these computers needed 5 or more critical updates. Some of these updates dated back to the year 2000. During August 2003, 72 state agency networks were infected with a malicious code. The Department indicated it was a result of not having updates installed. (page 15)

- The Department uses devices that allow individuals to dial into the state's network from remote locations. While this provides a convenient service to users, there is increased risk of unauthorized access through dial-up communications. This risk occurs when users who no longer need access are not promptly removed. As of July 2003, there were 632 active dial-up user accounts, and the Department's method for removing unnecessary users was having limited success. The Department should request confirmation of access and remove all users who do not respond. (page 17)

- The Department had not implemented procedures to detect unauthorized wireless access devices. These devices can circumvent other security measures such as firewalls. In addition, the current state standard for wireless networking did not include key components that would help guide state agencies in implementing this technology. (page 18)

- The Department hosts a Virtual Private Network (VPN) system that allows remote users to connect their computers to the state's network in a secure manner through encryption. Currently, there is no mechanism that ensures VPN users install updated software to fix known security problems. The Department has no way to detect which version users have. (page 19)

- Incident handling refers to the process used when hacker attacks or virus infestations occur. National standards recommend an incident handling capability to limit or prevent damage resulting from attacks. Our review found an inadequate process in the State. For example, agencies do not report incidents that occur, and there is no report format for agencies to use. In addition, although DoIT has an internal process to report incidents, the report format does not adequately characterize the nature of the attack. (page 20)

- Implementation of Information Technology (IT) security has not been adequately prioritized and planned. Neither DoIT nor other agencies had received guidance on how to prioritize their efforts toward the most critical security areas. Without good detailed project planning and management techniques, it is unlikely that available resources will be most effectively used in IT Security. (page 21)

- Backup and recovery procedures exist to guide individuals in preserving data and restoring computer systems in the event of operational problems or a

disaster. However, the Department's backup and recovery procedures are incomplete. For example, the Department has not created a contingency and disaster recovery plan, or conducted periodic testing of recovery capabilities. (page 21)

Recommendations

This audit report contains 15 recommendations to improve Internet security and utilization in the State. These recommendations help ensure greater security over hardware designed to limit unauthorized access to the state's information. In addition, they provide for better security over desktop computers and communication devices. Finally, the recommendations help ensure stronger controls over security incidents, prioritization of IT security planning, and backup and disaster recovery procedures. (page 34)

Agency Response

The Department of Information Technology, in its response to our report, accepted our recommendations, contingent on receiving additional staff. (page 28) Therefore, we have prepared additional comments on the Department's response to clarify that we believe the recommendations can be implemented with existing resources. (page 36)

Introduction

Background

The Department of Information Technology (DoIT) was created in 1965 and derives its authority from NRS 242. The Department is the state's lead agency for the delivery of effective and efficient information services. All state agencies and elected officers must use DoIT for the design of their information systems unless exempt by statute. Exempt agencies include:

- The Court Administrator
- Department of Motor Vehicles
- Department of Public Safety
- Department of Transportation
- Employment Security Division of the Department of Employment, Training, and Rehabilitation
- Department of Wildlife
- Legislative Counsel Bureau
- State Controller
- Gaming Control Board and Nevada Gaming Commission
- The University and Community College System of Nevada

The Nevada Information Technology Operations Committee (NITOC) is responsible for developing policies that apply to Nevada state agencies. NITOC is responsible for reviewing policy proposals from eight other working committees to ensure they are consistent with each other and generally acceptable to Nevada state agencies. The eight working committees are: Strategic Planning, Security, E-government, Technical Standards and Architecture, IT Project Oversight, IT Workforce, Justice IT Integration, and Electronic Records Management. The NITOC Security sub-committee has thus far produced 17 statewide Information Technology (IT) security standards.

In fiscal year 2003, the Department had authorized expenditures of $35,240,509 and 216 authorized full-time equivalent positions. The Department is located in Carson City.

Wide Area Networking Infrastructure - The Silvernet

The Department of Information Technology provides Internet access for the majority of state agencies. Those agencies connect to the Internet through the state's networking infrastructure known as the Silvernet. The Silvernet links approximately 274 distinct agency networks statewide. Each of these networks corresponds to an agency's physical office somewhere in Nevada. Primary locations include Carson City, Las Vegas, and Reno/Sparks, with the remainder located throughout rural Nevada. Within these LANs (Local Area Networks) are approximately 15,000 employees' desktop computers, data servers, and other information technology devices that are linked together by the Silvernet's telecommunications backbone.

Pursuant to a March 8th, 2000, Executive Order, all state departments were to establish a presence on the official website of the State of Nevada. As a result of this order, many state agencies have an informational website where citizens can access useful information about the services agencies provide to the State. In addition, public forms are also accessible through the state website as prescribed by the Executive Order. There are approximately 198 state websites. DoIT hosts approximately 140 of these websites, with the remainder hosted by individual agencies.

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 controls over the State's Internet security and utilization during calendar year 2003. Agencies included in this audit were the

Department of Information Technology, Department of Personnel, Department of Business and Industry's Insurance Division, and the Department of Human Resources Director's Office. The objective of the audit was to determine if controls are sufficient to ensure the security and integrity of the state's computer network and information stored by agencies.

This audit is the first phase of our review over Internet security. We will conduct additional Internet security audits at selected state agencies.

Findings and Recommendations

First-line Security Defenses Need Greater Attention

Protecting the state's networks and information from the Internet begins with certain key devices that represent a first-line of defense. The first of these security devices is a router that controls electronic traffic to and from the Internet. We reviewed the state's Internet router that manages traffic between the Silvernet and the Internet to determine if it was configured in accordance with established standards. Another key device is a firewall that prevents all traffic from passing through unless the traffic has been specifically allowed based on rules created by the Department of Information Technology (DoIT) security staff. We reviewed the administration of the firewall to determine if it was properly managed. Our review found improvements need to be made in managing both devices.

In addition, we found information maintained on various state websites that could provide a malicious user (hacker) with too much information. This information included detailed network diagrams, schematics of computer buildings, and names of information technology (IT) system administrators or security employees.

Weaknesses in these areas can provide hackers with greater opportunity to gain unauthorized access to the state's network. We noted that during our testing, DoIT staff made improvements in these areas. However, as the state's network changes and grows, constant monitoring will be required to ensure these key functions continue to block unwanted traffic.

Router Configuration Can Be Improved

A router contains many rules to manage the flow of network traffic. DoIT's Internet router, which is called a border router, is a key device in network security. Rules are entries in the router's software that tell the device where to send network traffic it receives. Our review found that while most of the rules in the border router were properly configured, 12 entries required a change to conform with established recommendations for router security. The configuration changes involved areas such as logging of system events, the lack of designating network time servers to

synchronize log entries, and running of unnecessary services. The overall effect of these misconfigurations was to render the network less secure. When notified of these weaknesses, DoIT staff took action to adjust the configuration settings.

Firewall Procedures Need To Be Strengthened

To further strengthen security, administration of the state's border firewall needs improvement. Firewall administration was largely dependent on the actions and decisions of a single employee. In addition, the policy governing firewall management was not complete and some firewall practices were not documented.

Inadequate Separation of Duties

The state's firewall, maintained by DoIT, was administered by one person who had sole authority to configure the device as he saw appropriate. Although this 'ownership' of the firewall has thus far resulted in a well-configured firewall, the practice renders the system vulnerable to a single point of failure should this person depart the position. In addition, these sensitive functions should be divided among different individuals. DoIT staff indicated other responsibilities had kept them from assigning an additional employee to configure the firewall. A system of checks and balances should be implemented over firewall administration to ensure that no single person can implement changes in the firewall's configuration without documented managerial approval. DoIT staff indicated they have subsequently implemented a peer review procedure to ensure that a second, knowledgeable staff member reviews all firewall changes.

Policy Governing Firewall Is Incomplete

Certain policies and procedures used to help administer and manage the firewall are not documented. For example, DoIT routinely applies firewall updates and installs new features. However, procedures relating to this process have not been formally documented.

Setting firewall policy should be a high-level managerial responsibility since the firewall is the primary defensive mechanism against outside intrusions into the state's network. Sound controls dictate procedures should be properly documented to ensure management is involved in setting policy. Staff indicated other responsibilities had taken priority over developing a firewall policy. However, to ensure continuity of firewall

security, DoIT should develop written firewall administration policies and procedures that include mechanisms to document management oversight.

Some Exceptions Were Not Documented

According to DoIT's policies, any firewall settings that do not conform to standards should be documented in a letter of exception. This is so all involved parties, including user agencies, are aware of the risks involved. DoIT's firewall had over 400 lines of code for various entries and settings. We found 3 out of 11 special firewall permissions that allowed inbound connections from the Internet lacked these exception letters. By not documenting these exceptions, there is an increased risk of management not being aware of firewall security exposures. This, in turn, could result in a misconfigured firewall and unauthorized access to state computer systems. Staff indicated they were aware of the exceptions but had overlooked the required exception documentation. DoIT had resolved two of the three exceptions prior to the completion of our audit.

Information on Some Websites Presents a Security Risk

Some state websites contained sensitive information, including network diagrams, system administrator names, and floor plans for a building containing critical computer equipment. This information should not be available to the public since it could provide hackers with useful information in their attempts to penetrate the state's network. This situation has occurred, in part, because DoIT does not have a policy to guide what kind of information should be withheld from public websites. In addition, DoIT does not have a procedure to periodically scan websites to look for sensitive information.

Recommendations

1. Enhance periodic examination of the border router configuration to ensure it is configured in accordance with standards.
2. Implement procedures to improve firewall administration.
3. Periodically review state web sites to ensure only appropriate information is present.

Computers Need Improved Security

Various computers the Department maintains contained security weaknesses. The first of these, computers that run the state's websites, were not positioned behind a firewall and contained software settings that rendered them more vulnerable to attacks. In addition, computers used to run office networks were not always securely configured. We found these weaknesses with DoIT's computers and the selected agencies we tested. Finally, desktop computers at DoIT and selected agencies were not always updated with the latest security patches from Microsoft. If these conditions continue, the risk of unauthorized intrusion increases.

Computers Running State Websites Were Vulnerable to Attacks

DoIT maintains several computers that contain the websites of approximately 140 state agencies. These computers, called web servers, are a key component of the state's electronic infrastructure and, as such, need strong security to prevent malicious intrusion. However, each of these computers contained security weaknesses.

First, the web servers were not located behind the protection of a firewall. National standards recommend that web servers be placed behind a firewall to limit their exposure to unauthorized access attempts. The Department indicated the web servers were set up this way historically but agreed this change should be made. Staff has indicated they are working to make the change.

Second, each of the web servers contained vulnerabilities in the software. Some of these vulnerabilities related to software updates that had not been applied and others related to certain web server settings that made the computers less secure. DoIT staff indicated they had encountered problems when trying to apply some of these software updates. However, we were able to find published solutions to these problems. The Department should pursue ways to properly install software updates and changes in security settings without adversely affecting web server performance.

Great care should be taken to ensure web servers are configured properly. By not doing so, there is an increased risk that attackers will use the computers for unauthorized activities. For example, in November of 2002, DoIT staff discovered that hackers had attacked one of the state's web servers and modified a website. However, a month later, it became clear the extent of the intrusion had been underestimated. The

attack had resulted in the creation of computer accounts that would allow unauthorized individuals access to the servers. In addition, approximately 60 Gigabytes of pornographic and regular movies and images had been copied on the server. During this period, the server was being used to distribute the movies and images. The Department indicated they have removed the offensive files and taken steps to improve web server security.

While it is unknown exactly how the security breach occurred, the Department can take steps to reduce the risk of this kind of incident from occurring in the future. These steps include developing procedures to guide staff when it becomes necessary to apply software patches. In addition, staff should periodically review the web servers using available automated software to ensure that previously undetected vulnerabilities are not present.

Security Settings on Network Servers Could Result in Unauthorized Access

Network servers are the devices used to run an agency's network. A system administrator uses these servers to add or remove user accounts, control user access to files, and set the various policies such as user password length and composition. However, these network server settings did not comply with policy created by the Nevada Information Technology Operations Committee (NITOC). These policies are designed to guide agencies, including DoIT, in securing their computer systems.

Our testing found these weaknesses at DoIT and also at the agencies we selected for additional testing. These agencies included the Department of Personnel, Department of Human Resources Director's Office, and the Department of Business and Industry's Insurance Division. DoIT network technicians are given the responsibility to administer network settings for these agencies.

Password control settings administered by DoIT staff were deficient. For example, they did not require passwords of sufficient length. In very few instances did passwords meet the state NITOC standard's length of at least eight characters. In addition, passwords were not of sufficient complexity. This means that password composition was not required to be a combination of letters, numbers, and special characters as required by the same NITOC standard. Weak passwords allow hackers

to gain easier access to user accounts using widely available password cracking software. Exhibit 1 shows the security settings we reviewed.

Exhibit 1

Security Settings at Agencies Reviewed

	Password Length	Password Complexity	Password Change Frequency	Password History	Account Lockout Threshold
Standard Settings	8 Characters	Mix of letters, numbers, and special characters	Change at least every 90 days	Do not reuse password for six password changes	Lock computer after 3 unsuccessful attempts to login
Agency					
DoIT	6	Complexity Disabled	90 days	1	15 attempts
Department of Personnel(1)	0	Complexity Disabled	90 days	1	Not Defined
Human Resources(2)	0	Complexity Disabled	90 days	4	3 attempts
B&I Insurance Division	5	Not Applicable(3)	Never	0	Not Defined

Note: (1) Fairview Drive Local Area Network
(2) Department of Human Resources Director's Office
(3) Network Operating System does not allow password complexity to meet NITOC password policy standard

These incorrect password settings existed even where the agencies used DoIT computer technicians. Service level agreements between DoIT and these supported agencies could improve password security by specifying which network responsibilities the agency's own staff perform and which belong to DoIT. Service level agreements represent a mutual understanding between agencies regarding the level of service support one agency provides to another.

Desktop Computers Are Not Updated With Latest Security Patches

For anyone who uses a computer running Microsoft Windows, it is a standard task to click on "Windows Update" to obtain the latest software updates. Some of these updates are listed as "critical" and are usually security related. In our testing, we found various desktop computers that were not updated with Microsoft's "critical" updates.

We tested a sample of 46 desktop computers at DoIT and selected agencies. Of the 46 computers, 32 needed updating. Twenty-two of these computers needed 5 or more critical security updates. In addition, some of these updates dated back to the year 2000. Three of these computers also lacked current antivirus protection. These

missing security updates and antivirus protection render these computers vulnerable to malicious code, especially Internet viruses and worms. During August 2003, 72 state agency networks were infected with a malicious code. The Department indicated it was a result of not having these updates installed. Considerable time and effort were expended to repair these infected computers.

The State needs to implement a more proactive solution or it will be faced with spending increasing amounts of time eradicating computer viruses while agency employees will be less productive until the viruses are removed. It is unlikely that an approach relying on computer user actions will provide a reliable solution. This is because of the large number of state agency local area networks involved. There are currently over 270 agency networks with approximately 15,000 users.

To overcome these risks, DoIT should develop a procedure to ensure that these software updates are applied to all state computers in a timely manner. DoIT indicated that in November 2003 it successfully implemented, on a limited scale, a centralized software update solution known as a Software Update Server (SUS). The SUS pushes updates out to user desktop computers without requiring any type of user intervention. We believe statewide implementation of this solution has the potential to minimize this problem. However, further testing must be conducted to determine if the SUS solution can cover the state's entire network.

Recommendations

4. Ensure greater security over web servers by placing them behind the state's firewall, developing a policy for installing critical patches, and periodically testing for vulnerabilities.
5. Enforce standards relating to security settings for web servers and agency network servers. This should include service level agreements between the Department and other state agencies.
6. Develop a procedure to ensure users' computers are updated with the latest security patches and antivirus software.

Communication Devices Need Better Monitoring

Several means of gaining access to the state's computer network potentially circumvent the up-front protection of its firewall. These access methods include dial-up modems, wireless network connections, and Virtual Private Network (VPN) connections. Each means of access needs improved security to better protect the state's network.

Dial-Up Security Needs Strengthening

The Department uses devices that allow individuals to dial into the state's network from remote locations. While this provides a convenient service to users, there is increased risk of unauthorized access through dial-up communications. This risk occurs when users who no longer need access are not promptly removed. As of July 2003, there were 632 active user accounts listed with dial-up access. The Department had a method for removing old accounts of people who no longer needed them. However, this method was having limited success.

During the audit, the Department initiated a quarterly process of sending lists of dial-up users to participating agencies asking them to identify accounts needing deletion. DoIT supplemented this with a monthly comparison of the dial-up user list with a report from the Department of Personnel that shows employees who have left state service. However, the monthly check of terminating employees fails to detect departing contractors or employees terminated prior to the start of the monthly review. In addition, the process of sending quarterly lists to agencies to identify unauthorized users was receiving limited cooperation. To ensure only authorized users have dial-up access, the Department should send a request to all users asking for confirmation of access needs and remove any who do not respond. Department management has agreed with this approach.

Additional security enhancements are needed for the dial-up access function. The devices that allow the dial-up connections did not support automated enforcement of strong passwords specified by state standards. Meeting state password standards would provide greater security over dial-up. The Department has indicated plans to increase the security over these devices.

DoIT Should Provide Greater Oversight of Wireless Network Implementation

Wireless networking is a technology that allows users to connect to a network or the Internet without using cables. To set up a wireless network, one needs a wireless network card in a computer that communicates with a device called a wireless access point. The wireless access point is then connected to the traditional network by a cable.

Several state agencies have already implemented wireless networking, and many more have expressed interest to DoIT in implementing this technology. Wireless network technology continues to evolve and has become a cost effective alternative to conventional wired networks. However, these wireless networks present serious security risks.

To address these risks the Department needs to implement procedures to detect unauthorized wireless devices or ensure proper configuration of those that are authorized. If not skillfully configured, wireless network access points can provide hackers with backdoors into a network. Backdoors are undocumented ways of gaining access to a program or computer system. This can occur because an individual sitting outside a state agency building equipped with a computer and wireless network card can access that agency's wireless network without being detected. These backdoors can circumvent existing security mechanisms such as firewalls.

Given the potential serious consequences of improper implementation of these wireless network access points, the Department should more closely monitor and control them to ensure they are implemented in a secure and standardized manner. In addition, procedures should be developed to periodically detect unauthorized wireless networks and to test the security of authorized, established wireless networks using readily available hardware and software. Subsequent to our review, the Department indicated they had begun to perform these tests and was successful in detecting two previously unknown wireless access points.

In addition, NITOC's current wireless policy did not address numerous items recommended by national standards for wireless networking security. The Department should work with the NITOC committee to amend its current wireless policy guidance to address all pertinent wireless security items. Exhibit 2 lists examples of items that should be included in a wireless network policy.

Exhibit 2

Items Needed in Wireless Policy

- Describe who can install access points and other wireless equipment.
- Provide limitations on the location of and physical security for access points.
- Describe the type of information that may be sent over wireless links.
- Describe conditions under which wireless devices are allowed.
- Define standard security settings for access points.
- Describe the hardware and software configuration of all wireless devices.
- Provide guidelines on the use of encryption and key management.
- Define frequency and scope of security assessments to include access point discovery.

Source: National Institute of Standards and Technology Special Publication, "Wireless Network Security"

Guidance Needed to Ensure VPN Software Is Updated

The Department hosts a VPN system that allows remote users to connect their computers to the state's network in a secure manner. A VPN is a program that encrypts data so unauthorized individuals cannot intercept the data while it is in transit between a user's remote computer and the state's network. Currently, there is no mechanism that ensures VPN users install updated software to fix known security problems. We noted that DoIT has recently implemented a new procedure to inform state VPN users of their responsibility to load updated client software. However, there remains no way for DoIT to identify which VPN users have not followed this guidance and continue to use the vulnerable software. DoIT should develop a process to ensure that VPN users update their client software. The Department agreed that a procedure could be developed to further communicate to users the importance of updating the VPN software.

Recommendations

7. Ensure greater security over dial-up accounts by deleting unauthorized users and providing adequate security settings.

8. Proactively review the configuration of agency wireless networks prior to them being connected to the state's network.
9. Update current wireless policy to address national standards for wireless networking security.
10. Develop a procedure to ensure Virtual Private Network users have the latest software.

Other Security-Related Procedures Need Strengthening

We found several other areas where network security could be improved. For example, there is no statewide standardized procedure for handling hacker intrusions and virus infestations. In addition, implementation of IT Security has not been adequately prioritized and planned. Finally, backup and recovery procedures are incomplete.

Incident Handling Is Not Adequate

Incident handling refers to the process used when security breaches occur. The most frequent security incidents affecting the state's network are hacker attacks and virus infestations. NIST recommends all organizations have a security incident handling capability in order to limit and repair damage from incidents, and to prevent similar damage in the future.

Security incident handling could be improved throughout the State. Agencies do not always report security incidents that occur. In addition, there is no standardized incident report format for agencies to use for reporting these incidents. Furthermore, although DoIT has an internal process to report security incidents, the format could be improved. The format is a subjective, narrative description of the incident. For example, DoIT's format does not objectively characterize the incident into one of 10 recognized categories. Nor does it characterize the method of intrusion into one of the eight recognized types. In addition, it does not identify the type of systems impacted. These categories and types are recognized by the Federal Bureau of Investigation through joint projects with academic institutions and state and local law enforcement.

The result of these weaknesses is that security incidents go unreported. Furthermore, state senior IT management does not become aware of the magnitude and scope of security threats that would enable them to better focus their resources on proactive, preventative solutions. For instance, the security incident that occurred resulting in approximately 60 Gigabytes of pornographic and regular movies and images being placed on DoIT's web server would have benefited from a more thorough reporting process. The full extent of this incident was never reported to DoIT management. DoIT should develop, through NITOC, effective security incident handling policies, procedures, and reporting formats that apply to all agencies, including itself.

Implementation of IT Security Has Not Been Adequately Prioritized and Planned

Prioritization and planning are fundamental managerial responsibilities intended to focus efforts on the state's high-risk areas and important systems first. Neither DoIT staff nor agencies supported by DoIT had received guidance on how to prioritize their security efforts toward the most critical areas. We observed staff with various security projects planned but no focus on which were a higher priority. Prioritization helps ensure that tasks, staffing, and required effort are identified with realistic targets given limited resources available and competing needs. For example, DoIT had begun working on backup and recovery and service level agreement work with two state agencies. However, without a prioritized plan, it was not clear if work at these agencies was of the highest priority to the State. In addition, expected completion dates were not clear for either task.

Detailed plans had not been developed for prioritized implementation of other approved state IT security polices, standards, and procedures. As a result, it was not clear if efforts under way were coordinated and focused on the most critical areas to the State, or when they should be completed. Without good detailed project planning and management techniques, it is unlikely that available resources will be most effectively used in IT security.

Backup and Disaster Recovery Procedures Are Incomplete

The Department is responsible for maintaining computers that house data owned by other state agencies on over 40 computers as well as the central mainframe. Part of

that responsibility includes backup of data stored on computers and providing the capability to restore damaged or corrupted data. Our review concentrated on DoIT's servers. We did not review mainframe backup operations as they are separate from the web servers.

While our review found the Department did conduct backup procedures for state agencies, they were not completely in accordance with state standards. For example, the Department had not created plans addressing recovery and contingency activities in the event of a disaster. In addition, there were no written backup or recovery procedures for the Department's servers. The following lists the backup and recovery procedures that need to be completed.

- **The Department has not created contingency and recovery plans that are necessary to guide staff efforts in the event of a major disruption of service.**

- **No semi-annual testing of backup and recovery capabilities occurred. The efficacy of backed up data and software can only be verified through such testing. For example, recently it was discovered that an e-mail server backup process had not been working for two and a half years due to a software setup problem.**

- **No written backup and recovery procedures for DoIT's Web servers, data servers, or RS/6000 systems existed. Informal procedures were based on phone calls or informal discussions rather than approved written procedures.**

- **DoIT server farm administrators did not back up state agency programmer changes to software and programs since they viewed this as the agency's responsibility. However, this was not formally documented, increasing the possibility of software changes being inadequately backed up due to responsibility confusion.**

- **Configuration files for routers and firewalls backed up on CD's were not stored at an approved off-site location. Instead the files were located at a Department employee's home. Configuration files contain the unique set of communication and security parameters. Their secured storage and subsequent availability is vital.**

- **Department security personnel had begun creating an inventory of servers. However, they had only completed about two-thirds of the inventory as of August 2003. In addition, other staff and management at the Department were unaware that such an inventory existed. An accurate inventory of devices and software can significantly expedite recovery and setup of devices destroyed in a disaster.**

If left uncorrected, the listed items will make recovery of Internet-related systems difficult following operational problems or disaster situations. To overcome these weaknesses, the Department should implement service level agreements with the agencies it supports that clearly prescribe backup and recovery expectations. This will not only reduce the confusion over who is responsible for backup and recovery, but will allow agencies to obtain the level of service they need for their own unique circumstances. In addition, by having written agreements, top management at DoIT and other agencies can be better informed and provide the proper direction.

Policy Needed for Backup Generator

The DoIT computing facility relies on a large backup generator to provide power in the event of a power disruption. However, a policy does not exist that dictates how often the computer facility's backup generator should be tested. Although the generator is periodically tested, a policy will allow management to direct staff efforts. Without such a policy, management oversight is diminished and the result could be an untested generator. To ensure management is kept informed, DoIT should develop and implement a policy that prescribes the testing frequency of its computing facility's backup generator.

Recommendations

11. Develop a more comprehensive incident handling standard that is applicable to all state agencies, including a thorough report format.
12. Develop a policy to guide staff efforts when a suspected security breach has occurred at another agency.
13. Prioritize and plan the state's security work in terms of risk and importance.
14. Ensure that backup and disaster recovery procedures are complete. This should include service level agreements between the Department and other state agencies.
15. Create a testing policy for the Department's backup generator.

Appendices

Appendix A

Audit Methodology

To gain an understanding of Internet security, we conducted interviews at the Department of Information Technology and other selected state agencies. These agencies included the Department of Personnel, Department of Business and Industry's Insurance Division, and the Department of Human Resources Director's Office. These agencies were selected based on popularity of their websites and the sensitivity of the information they store.

We also reviewed legislative meeting minutes, budgets, and laws related to Internet security. We gathered statistics on website usage throughout state government. We also gathered generally accepted Information Technology standards and guidelines from the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA). In addition, we reviewed policies and procedures created by NITOC. To further understand Internet security, we obtained and reviewed network diagrams for DoIT and other selected agencies.

To determine if controls limiting access to the state's network were adequate, we reviewed the Department's border router and its rules. We also reviewed the method used to maintain the state's firewall, including separation of duties and sufficient policies to guide staff. We then examined state websites to determine if agencies allow sensitive information to be posted on the Internet. We reviewed these controls with security personnel at DoIT.

To evaluate controls over computer security, we tested DoIT's computers that are used to host the state's websites. Specifically, we tested these computers to determine if they were configured in a secure manner that would prevent unauthorized intruders. We also tested computers at DoIT and selected agencies to determine if they had access settings in place to prevent unauthorized access. Next, we tested individual desktop computers at DoIT and selected agencies to ensure they were updated with the

latest operating system patches. In addition, we tested network computers and desktop computers to determine if they contained automated anti-virus protection.

To assess security over communication devices, we reviewed the list of users who connected to the state's network using modems. We documented DoIT's methods for keeping the list current. We then reviewed the extent of DoIT's efforts to test for unauthorized wireless connections. In addition, we examined DoIT's methods for ensuring users who connect through the VPN connection are using the most recent software.

We next evaluated additional security-related controls. For example, we reviewed the state's process for reporting and managing security problems. We reviewed controls over the backup and recovery of data, including the backup generator.

Finally, we reviewed DoIT's efforts at prioritizing security-related projects. We documented projects that have been undertaken and those left to complete. We also met with staff and management to discuss how these projects will be completed.

Our audit work was conducted from March 2003 to November 2003, in accordance with generally accepted government auditing standards.

In accordance with NRS 218.821, we furnished a copy of our preliminary report to the Department of Information Technology. On May 17, 2004, 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 C that begins on page 28.

Contributors to this report include:

S. Douglas Peterson, CISA
Information Systems Audit Supervisor

Roy Cage, CIA, CISA
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

Antivirus Software: A utility that searches a hard disk, incoming e-mail, or downloaded files for viruses or other malicious programs and removes any that are found.

Backbone: The main telecommunications mediums that connect the rest of the wide area network (WAN) together.

Backdoors: Undocumented ways 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.

Client/Server: Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application on a desktop computer that sends and receives e-mail to and from an e-mail server.

Common Vulnerability Exposure (CVEs): Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures.

Data Server: A computer configured to efficiently store and retrieve large amounts of data or files.

Demilitarized Zone (DMZ): A computer or small subnetwork that sits between a trusted internal network such as a corporate private LAN, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web servers.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Hacker: Typically used to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data.

Host: To provide the infrastructure for a computer service. For example, there are many companies that host web servers. This means they provide the hardware, software, and communications lines required by the server, but the content on the server may be controlled by someone else.

Intranet: A network belonging to an organization, accessible only by the organization's members, employees, or others with authorization.

Internet: A global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions.

Internet Service Provider (ISP): An organization that provides access to the Internet.

Local Area Network (LAN): A computer network that spans a relatively small area. Most LANs are confined to a single building or small group of buildings.

Malicious Code: Computer viruses, trojans, worms, or other programs that disrupt normal computer operations in a destructive manner.

Patch: An update to a software program or operating system.

Router: A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways or where two or more networks connect.

Silvernet: The name of the state's wide area network (WAN).

System Administrator (SA): An individual responsible for maintaining a multi-user computer system, including a local area network (LAN). Typical duties include: 1) adding and configuring new workstations, 2) setting up user accounts, 3) installing system-wide software, 4) performing procedures to prevent the spread of viruses, and 5) allocating mass storage space.

Virtual Private Network (VPN): A *network* that is constructed by using public communication lines to connect computers. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Web Server: A computer that delivers (*serves up*) web pages.

Web Site: A site (location) on the World Wide Web. Each web site 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.

Wide Area Network (WAN): A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

Appendix C
Response From the Department of Information Technology

KENNY C. GUINN
Governor
Director

STATE OF NEVADA

TERRY SAVAGE
CIO,

DEPARTMENT OF INFORMATION TECHNOLOGY
505 E. King Street, Room 403
Carson City, Nevada 89701-3702
(775) 684-5800

DATE: May 27, 2004

TO: Paul V Townsend
Legislative Auditor, LCB

FROM: Terry C Savage, Director
Department of Information Technology

SUBJECT: LCB Audit Response – May 2004

Attached is the Department of Information Technology's Written Response based on the audit by the Legislative Counsel Bureau. The fifteen recommendations highlighted in the report have been addressed with comments on findings.

Please note that while we accept all of these recommendations as desirable, implementation is contingent on receiving the additional resources identified (4-5 additional FTEs). Funding for these resources will be included in our 06/07 budget request. It is likely that some incremental progress will be possible prior to receiving the additional resources, but the bulk will need to be deferred. We will provide details when we submit our corrective action plan.

If you have any questions or need any further assistance, please contact me at (775) 684-5848.

cc: Lee Pierson, Executive Branch Auditor IV, Department of Administration
Perry Comeaux, Director, Department of Administration
Michael Hillerby, Governor's Chief of Staff

Department of Information Technology
Response to LCB Audit

Please note that while we accept all of these recommendations as desirable, implementation is contingent on receiving the additional resources identified (4-5 additional FTEs). Funding for these resources will be included in our 06/07 budget request. It is likely that some incremental progress will be possible prior to receiving the additional resources, but the bulk will need to be deferred. We will provide details when we submit our corrective action plan.

1) Enhance periodic examination of the border router configuration to ensure it is configured in accordance with standards.

- Although the Router Audit Tool (RAT) recorded 43 errors, 12 independent errors as noted by the Audit Staff, we define these as falling into 4 different modifications. In the 4 findings that we agreed with, one of them was contingent upon a question posed to the CIS as we disagreed with the tool findings (we later agreed to implement the one after the availability of version 12.3 of Cisco code, which was acceptable by the auditors). The CIS response to our query is enclosed as Attachment A to this memo. Also, the CIS publishes the tool to help administrators secure their routers and does not consider that any router should receive a perfect score (see Attachment B, responses to FAQs from their website) for security is mitigation of risk and some risk is required to conduct e-Government such as Router Audit Tool finding 2: IOS (no snmp-server) – "SNMP is required for network monitoring and network health. Used for both our Multi-Router Traffic Grapher (MRTG) as well as Concord Network Health Software. Per the provided Router Audit Test (RAT) tool documentation, should be disabled only if not in use. There are access controls on its use, allowing only two stations to send SNMP queries, as well as allowing only read access."
- We experienced mixed results with the tool and opted to carefully screen the NSA Router Security Configuration Guide, highlight pertinent areas, and apply as many of the recommended measures that we could under the constraints of production needs. That was completed prior to the audit. We are concerned by the statement "render the network less secure." We would request an explanation on what level of security has been lost, or what risk this imposes. Additionally, "DoIT staff took action" to implement changes for the other faults uncovered by the tool, which were false positives. We made the changes because, as explained in writing to the audit team, it was the "path of least resistance." For instance, it is not necessary to have a "no proxy-arp" command on an interface that is administratively shutdown and not configured. Implementation of those changes had no effect on network security.

Resources in man hours	Ongoing (weekly)	Monthly	Project
		4	

2) Implement procedures to improve firewall administration.

- The firewall was administered by 2 people, not 1, for the last 3 years. Also we requested the removal of the sentence "This practice renders the system vulnerable to a single point of failure should this person depart the position." Although we agree conceptually, the DoIT backup firewall administrator was, as a point of clarification, the individual who originally configured the firewall and implemented the solution. Firewall policy has existed (initial release 3/21/02) and change control procedures, which address firewall changes, have existed since 8/27/03 (Silvernet Change Control Procedure).
- One of the three firewall permissions which allowed inbound connections has already been removed and the other two were questionable in nature. Those two would not allow an individual to create a VPN connection inbound from the Internet, but did allow an outbound initiated connection to respond appropriately. The firewall did not have a mechanism to allow the return traffic as it does for normal IP connectivity. The policy was updated and the exceptions are no longer required.
  We are implementing additional controls of Firewall administration with separation of duty between the operation staff who actually change the firewall rules and the newly created oversight group known as

the Security Unit who shall periodically review the firewall rules as well as approve exemptions. These policies will formally be documented.

Resources in man hours	Ongoing (weekly)	Monthly	Project (onetime)
	4		24

3) Periodically review state web sites to ensure only appropriate information is present.

Cultural change has begun in this area, however prior to the Homeland Security Act most information had been deemed as public record. However, a clear definition and standard will be required on what is not appropriate information by the State Security Committee as this affects many State agencies. Once those standards have been identified and an awareness program put in place will strengthen the entire state's web environment.

Resources in man hours	Ongoing (weekly)	Monthly	Project
	2		36

4) ***Ensure greater security over web servers by placing them behind the State's firewall, developing a policy for installing critical patches, and periodically testing for vulnerabilities.***

- A migration plan has been developed and implementation of the migration has already begun.
- Policy for critical patch management is being developed as well as a test plan.

Resources in man hours	Ongoing (weekly)	Monthly	Project
	4		160

5) Enforce standards relating to security settings for web servers and agency network servers. This should include service level agreements between the Department and other state agencies.

We scheduled the implementation of the State PSP on passwords for the IS environment. At the last moment Internet Services group was asked to hold off by other state agencies for further evaluation based on costs to the helpdesk around the state and what threat is really being mitigated. At the State IT Security meeting DoIT was asked to write a temporary exception for the State Email environment on behalf of the Department of Admin. We are also working on revising service level agreements to reduce this for occurring in the future. We are working on the creation and development of Standard Technical Implementation Guides (STIG's) for the web environment as well as the many other platforms and systems utilized within the State.

Resources in man hours	Ongoing (weekly)	Monthly	Project
	40		160

6) Develop a procedure to ensure user computers are updated with the latest security patches and anti-virus.

Procedures should be covered through a service level agreement between the Department and other state agencies as well; however the standard again is driven from the State Security Committee and agencies becoming compliant with those standards. However, we have implemented the Microsoft SUS solution and have experienced great success with it for our windows environment.

Department of Information Technology
Response to LCB Audit

Resources in man hours	Ongoing (weekly)	Monthly	Project
	4		56

7) Ensure greater security over dial-up accounts by deleting unauthorized users and providing adequate security settings

The recommendation "the Department should send a request to all users asking for confirmation of access needs and remove any who do not respond" if implemented, may have limited effect. Any contract or other employee who was no longer authorized connectivity could respond that they were still an active account. The solution we are strengthening is to ask the agencies approving authority if the account is required and disable or delete as necessary (which we do when we audit the accounts, quarterly – see Attachment C), however are working on rewording the language used in the quarterly mailing. Additionally, state security standard 4.60, Paragraph 6.01 (I), requires agencies to keep records and notify DoIT immediately upon any change of access or authorization. By State standard, the agency ISO's are responsible to remove access or change level(s) of authorization.

Resources in man hours	Ongoing (weekly)	Monthly	Project
		8	

8) Proactively review configuration of agency wireless networks prior to them being connected to the State's network.

When aware of new wireless initiatives, DoIT currently reviews for compliancy; however we are not always aware of new initiatives and are working on building better awareness of State policies.

Resources in man hours	Ongoing (weekly)	Monthly	Project
		16	

9) Update current wireless policy to address national standards of wireless networking security.

When asked for clarification of the recommendation it was determined that DoIT should be responsible for auditing all State agencies for unauthorized wireless. DoIT's current staffing level cannot support an auditing team for wireless networks. DoIT does continuing inspection of premises, by both the WAN groups and the TECH groups at all DoIT employee sites. We will, however continue to work with the State Security Committee on development of comprehensive standards and policies and they are currently re-writing the wireless standard, which has existed as a section of the Data Communications and Remote Connections standard, effective 11/25/02. We are also working on building a full assessment team to work with State agencies on all security standards.

Resources in man hours	Ongoing (weekly)	Monthly	Project
		54	56

10) Develop a procedure to ensure Virtual Private Network users have the latest software.

Our Cisco VPN software does not virtually support this. DoIT will be required to manually review the VPN logs to determine over 1200 clients and what their version is on their system as a log is only generated after a client has attempted to connect to the network. The best available solution is to strengthen the end-user agreement and forward out emails to the user community periodically to check for an update to our client web site. Again, this will require cooperation from end-user community.

Department of Information Technology
Response to LCB Audit

Resources in man hours	Ongoing (weekly)	Monthly	Project
	32		16

11) Develop a more comprehensive incident handling standard that is applicable to all state agencies, include a thorough report format.

This function falls within the State Security Committee, however DoIT will work to assist and lead getting this accomplished and the need for the Incident Team is even coming to light within the CyberTerrorism sub-committee for Homeland Security as outlined by their strategic plan whom we also will work with.

Resources in man hours	Ongoing (weekly)	Monthly	Project
	16		160

12) Develop a policy to guide staff efforts when suspected security breech has occurred at another agency.

A formal policy and awareness program will be developed to assist all DoIT employees to understand what is required; in addition, the awareness program should reach out to all end-users so incidents can be mitigated before they happen or at the point they occur.

Resources in man hours	Ongoing (weekly)	Monthly	Project
	2	4	64

13) Prioritize and plan the state's security work in terms of risk and importance.

- The development of the new Security Unit has facilitated great improvements in this regard already; however this task will be ongoing in nature.

Resources in man hours	Ongoing (weekly)	Monthly	Project
	8		

14) Ensure that backup and disaster recovery procedures are complete. This should include service level agreements between the Department and other state agencies.

The Security Unit has identified this and currently working to develop full Business Recovery Plan plus IT Continuity of Operations. Security unit has recently added an additional resource with primary responsibility to address this topic.

Resources in man hours	Ongoing (weekly)	Monthly	Project
	48		160

15) Create a testing policy for the department backup generator.

DoIT has created policy.

Resources in man hours	Ongoing (weekly)	Monthly	Project
		1	2

Department of Information Technology
Response to LCB Audit

Summary

Resources in man hours	Ongoing (weekly)	Monthly	Project
Total man hours	160	87	878
FTE	5		

Department of Information Technology
Response to Audit Recommendations

Recommendation Number		Accepted	Rejected
1	Enhance periodic examination of the border router configuration to ensure it is configured in accordance with standards	X	
2	Implement procedures to improve firewall administration.	X	
3	Periodically review state web sites to ensure only appropriate information is present	X	
4	Ensure greater security over web servers by placing them behind the state's firewall, developing a policy for installing critical patches, and periodically testing for vulnerabilities	X	
5	Enforce standards relating to security settings for web servers and agency network servers. This should include service level agreements between the Department and other state agencies	X	
6	Develop a procedure to ensure users' computers are updated with the latest security patches and antivirus software	X	
7	Ensure greater security over dial-up accounts by deleting unauthorized users and providing adequate security settings	X	
8	Proactively review the configuration of agency wireless networks prior to them being connected to the state's network	X	
9	Update current wireless policy to address national standards for wireless networking security	X	
10	Develop a procedure to ensure Virtual Private Network users have the latest software	X	
11	Develop a more comprehensive incident handling standard that is applicable to all state agencies, including a thorough report format	X	
12	Develop a policy to guide staff efforts when a suspected security breach has occurred at another agency	X	
13	Prioritize and plan the state's security work in terms of risk and importance	X	

Department of Information Technology
Response to Audit Recommendations
(continued)

Recommendation Number		Accepted	Rejected
14	Ensure that backup and disaster recovery procedures are complete. This should include service level agreements between the Department and other state agencies	X	
15	Create a testing policy for the Department's backup generator	X	
	TOTALS	15	0

Appendix D
Auditor's Comments on Department's Response

The Department of Information Technology accepted all recommendations but indicated implementation is contingent on receiving additional resources. The Department indicates four to five additional staff will be requested for the 2006/2007 budget (page 28). We have provided comments to clarify that we believe the recommendations can be implemented with existing resources.

Beginning in early calendar year 2002, the Nevada IT Operations Committee (NITOC) created security standards applicable to state agencies, including the Department of Information Technology. These standards address many of the same areas as our audit report. As a result, the Department has had adequate time to prioritize their resources to address the standards.

Findings discussed in the audit report are in areas where staff already has responsibility. This has allowed the Department to implement some of the recommendations with existing resources. In addition, progress has been made towards implementing other recommendations. For example, on page 11 we note improvements have already been made in strengthening firewall procedures. On page 16 we indicate the Department is implementing a procedure to help ensure software updates are applied to computers in a timely manner. Furthermore, these findings identify improvements needed in the Department's approach to security and were not intended to create new responsibilities. Although full implementation of the audit's recommendations will require ongoing efforts, existing staff have thus far proven capable.

It should also be noted that in several instances, the Department's response indicates additional duties that were not part of the audit's findings or recommendations. For example, recommendation number five states, "Enforce standards relating to security settings for web servers and agency network servers…" (page 16). The Department indicates a delay in implementing this recommendation and states the need for an additional ongoing 40 man hours per week. However, their response specifically addresses the state e-mail environment which is beyond the scope of the recommendation (page 30).

Managing staff workload given available resources is a major part of the management process for any organization. To accomplish this, the Department must prioritize the 216 full-time equivalent positions it has available. In addition, the Department must consider risk when directing staff efforts. Those systems and security requirements that are of greatest risk to the State should receive attention first. Not all computer systems can or should be addressed at the same time. For this reason, the audit recommends that the Department prioritize and plan the state's security work in terms of risk and importance (page 21).