STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747
Fax No.: (775) 684-6600

LEGISLATIVE COMMISSION (775) 684-6800
BARBARA E. BUCKLEY, *Assemblywoman, Chair*
Lorne J. Malkiewich, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
WILLIAM J. RAGGIO, *Senator, Chairman*
Gary L. Ghiggeri, *Fiscal Analyst*
Mark W. Stevens, *Fiscal Analyst*

LORNE J. MALKIEWICH, *Director*
(775) 684-6800

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 the Security Over Selected State Agency 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 State Gaming Control Board, Department of Corrections, Public Employees' Benefits Program, and the Department of Information Technology for their assistance during the audit.

Respectfully presented,

Paul V. Townsend, CPA
Legislative Auditor

January 26, 2006
Carson City, Nevada

STATE OF NEVADA
SECURITY OVER SELECTED STATE
AGENCY INTERNET SITES

AUDIT REPORT

Table of Contents

EXECUTIVE SUMMARY

SECURITY OVER SELECTED STATE AGENCY INTERNET SITES

Background

In 2004, the Legislative Auditor issued a report on Utilization and Security Over State Internet Sites. That was the first phase of our review over Internet security. That report focused on the Department of Information Technology (DoIT) and agencies whose networks were administered by DoIT employees. This audit is the second phase of our review and includes agencies which maintain their own networks. These include the State Gaming Control Board, the Department of Corrections, and the Public Employees' Benefits Program. Although these agencies maintain their own networks, standards created by the State should be followed, inasmuch as the standards apply to all but two Executive Branch state agencies.

The Nevada Information Technology Operations Committee (NITOC) is responsible for developing standards that apply to state agencies. NITOC is responsible for reviewing proposed standards 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: IT Project Oversight, Security, Integration, Communications, IT Workforce, Enterprise Architecture, Electronic Records Management, and Technical Standards. As of July 2005, the NITOC Security working committee had produced 20 statewide Information Technology (IT) security standards.

Purpose

The purpose of this audit was to determine if controls are sufficient to ensure the security and integrity of selected state agencies' computer networks and information stored by those agencies. Our audit included a review of controls over Internet security at selected state agencies for fiscal year 2005.

Results in Brief

More needs to be done to assist state agencies in securing their networks. The 2004 audit on Internet security and this audit indicate security weaknesses continue to exist in state agencies. For example, improvements are needed over devices that manage the flow of information throughout individual agencies' networks and the State. These devices require regular monitoring to ensure adequate security. Further improvements in controls are needed for users' computers including password settings, security updates, and antivirus software. In addition, state required security-related plans have not been created or are incomplete. Finally, controls to access sensitive computer equipment need more frequent monitoring.

These weaknesses, if left uncorrected, provide increased opportunities for malicious users to gain access to agency computers, or reduce the chances of effectively recovering from a disaster. The Department of Information Technology has the statutory authority and staff to provide assistance to state agencies. This assistance will be valuable to agencies in properly securing their information systems.

Principal Findings

- The Department of Information Technology has statutory authority to assist and advise nearly every Executive Branch agency. However, more can be done. This assistance would help agencies overcome the security weaknesses we have noted in the last two audits. The recently formed Office of Information Security group within the Department will greatly aid efforts to provide proper security training and guidance to state agencies. (page 10)

- A router is a device that contains many rules to manage the flow of network traffic. The Gaming Control Board is the only agency in our review that maintains its own routers. For Gaming's three primary routers, we found 33 rules that did not conform to established benchmarks. The overall effect of not conforming to these benchmarks is to render a network less secure. We noted that the agency's staff took immediate action to reconfigure their routers. (page 12)

- A firewall is a device designed to prevent unauthorized access to a network. Gaming is the only agency in our review that maintains its own firewall. We found the policy for this firewall needs improvement. The policy did not address who is authorized to create or modify firewall settings. This policy change would ensure greater awareness of how the firewall should be administered, and reduce the risk of unauthorized changes. (page 12)

- Web servers are computers that contain websites. Gaming and the Department of Corrections maintain their own web servers. For both agencies combined, 41 changes were needed to ensure secure configuration. The changes included settings designed to prevent malicious users from intentionally overloading the servers and to prevent the servers from displaying sensitive information on the agencies' websites. (page 13)

- Computers need to periodically be updated with the latest security software updates, referred to as patches. Of Gaming's five network servers tested, two were missing critical patches. In addition, critical patches had not yet been installed on the Public Employees' Benefits Program's (PEBP) server. A statewide standard on how often critical patches should be installed would be helpful to state agencies. (page 13)

- Network servers are the computers used to run an agency's network. We found password settings on network servers that were not in accordance with state standards. These settings resulted in a less secure network. They included passwords of insufficient length, 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 Gaming and Corrections. However, PEBP uses a fingerprint scanner that allows users to gain access to their network. As a result, we did not test password controls at PEBP. (page 14)

- Desktop computers are configured with accounts which grant the user permission to perform certain tasks. According to state standards, computers should be configured to grant the least privilege that a user needs to perform his or her job function. However, at Corrections, all computers were given the highest privilege level. In addition, Gaming had several duplicate administrative accounts that were unnecessary. Appropriate account settings are an important deterrent to unauthorized access. (page 15)

- Network servers contain accounts that are used to grant employees permission to use a network and its resources. We found that Gaming had three active user accounts belonging to former employees. This increases the risk of unauthorized access to the agency's network and its data. (page 16)

- Of the 50 desktop computers we tested for critical security patches at the three selected agencies, 35 needed updating. Some of these computers needed five or more critical patches. For example, during August 2003, 72 state agency networks were infected with a malicious code. Not having critical security patches installed can result in unauthorized intrusions. (page 16)

- State standards require antivirus software to be installed on computers and regularly updated. This reduces the risk of viruses infecting computers. Of 13 computers we tested at Corrections, 1 did not have updated antivirus definitions. This was caused by an error in settings that prevented the updates from occurring. (page 17)

- Disaster recovery plans exist to guide individuals in preserving data and restoring computer systems in the event of operational problems or a disaster. Corrections did not have a disaster recovery plan. Gaming and PEBP did have plans but they were missing key components or were not up-to-date. (page 17)

- Various state standards require all agencies to have a comprehensive Information Technology (IT) risk assessment, a security plan, and an ongoing IT security awareness training program. Corrections did not have any of the plans or training in place. PEBP had not completed a risk assessment and had not conducted ongoing IT security awareness training. These requirements exist to ensure each agency adequately assesses its own security risks and develops a plan tailored to minimize those risks. Ongoing security awareness training ensures that all agency users understand their IT security responsibilities. (page 18)

- Controls over physical access ensure that only appropriate users are allowed access to sensitive computer equipment. We discovered that Gaming's network room was accessible by 65 individuals. Once staff was made aware of this situation, they reduced this to eight employees who had a legitimate reason to access the network room. (page 19)

Recommendations

This audit report contains two recommendations to improve Internet security. The Department of Information Technology should create a standard for timeliness of patch installation. In addition, the Department should provide more ongoing assistance, training, and security assessments to state agencies regarding information security. (page 27)

Agency Response

The Agency, in its response to our reported, accepted the two recommendations. (page 26)

Introduction

Background

In 2004 the Legislative Auditor released a report on Utilization and Security Over State Internet Sites. This was the first phase of a review over Internet security. The 2004 report focused on the Department of Information Technology (DoIT), the Department of Personnel, the Department of Business and Industry's Insurance Division, and the Department of Human Resources Director's Office. These agencies' networks are all administered by DoIT employees.

This audit is the second phase and continues our review over Internet security. Agencies selected in this second phase are responsible for maintaining their own networks. The agencies include the State Gaming Control Board, the Department of Corrections, and the Public Employees' Benefits Program (PEBP). Even though these agencies are responsible for maintaining their own networks and ensuring their own security, they must adhere to the security standards created by the State. Within the Executive Branch of state government, only two agencies are exempt from standards adopted by the State—the Nevada System of Higher Education and the Nevada Criminal Justice Information Computer System. All other agencies are subject to the standards.

Some of these standards have been created through a committee made up of representatives from various state agencies. The Nevada Information Technology Operations Committee (NITOC) is responsible for developing standards that apply to Nevada state agencies. NITOC is responsible for reviewing proposed standards 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: IT Project Oversight, Security, Integration, Communications, IT Workforce, Enterprise Architecture, Electronic Records Management, and Technical Standards. As of July 2005, the NITOC Security working committee had produced 20 statewide Information Technology (IT) security standards.

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 hundreds of 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 Local Area Networks (LANs) are thousands of employees' desktop computers, data servers, and other information technology devices that are linked together by the Silvernet's telecommunications backbone.

Pursuant to a March 8, 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 over 200 state websites. DoIT hosts approximately 140 of these websites, with the remainder hosted by individual agencies, or Internet service providers.

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 selected state agency Internet sites during fiscal year 2005. Agencies included in this audit were the State Gaming Control Board, the Department of Corrections, and the Public Employees' Benefits Program. The objective of the audit was to determine if controls are sufficient to ensure the security and integrity of selected state agencies' computer networks and information stored by those agencies. This audit is the second phase of our review over Internet security.

Findings and Recommendations

More Can Be Done to Assist Agencies With Security

Nevada Revised Statutes (NRS) 242.111 requires the Department of Information Technology (DoIT) to adopt regulations necessary for information services. This includes developing policies for the information systems of the Executive Branch of government. The policies can include items such as criteria for selection, and location and use of information systems.

The responsibility given to DoIT through NRS 242 has been carried out, in part, through the creation of information technology standards. DoIT facilitated the development and acceptance of these standards through creation of the Nevada Information Technology Operations Committee (NITOC). This committee, composed of members of various agencies, has developed the standards. The first of these standards was created in 2002 with more created in subsequent years. Examples of topics discussed in the NITOC standards include contingency planning, passwords, backup and recovery, and physical security.

NRS 242.111 exempts the Nevada System of Higher Education and the Nevada Criminal Justice Information Computer System from the standards for information systems. However, all other Executive Branch agencies must follow the standards.

DoIT's responsibility for ensuring the security of information systems extends beyond helping to form state standards. NRS also allows the Director of DoIT to act in an advisory role. As a result, even though DoIT does not maintain day-to-day control over some state agencies' networks, it is within their scope of authority to advise all agencies.

In 2004 the Legislative Auditor released an audit on Utilization and Security Over State Internet Sites. This was the first phase of an audit on security in various state agencies. This audit is the second phase. Through both audits, we have found numerous security weaknesses within state agencies. We found weaknesses in areas such as routers, firewalls, computers running websites, desktop security, wireless, antivirus software, and disaster recovery planning. Combined, these weaknesses serve to render the state's networks and information vulnerable to attack. More needs to be done to educate state agencies, train them, and assist in whatever way possible to ensure the state standards are understood and implemented.

The Department of Information Technology has the authority and staff to provide assistance to state agencies. With the addition of five new security positions during the 2005 Legislative Session, the Department is better equipped to provide additional oversight of Internet and network security. DoIT has created a new section specifically for this purpose—the Office of Information Security. This office is set up to support agencies and would be one way the Department can provide training and other assistance in enhancing the security of the state's networks. Specifically, the office was established to provide information security guidance, oversight, and direction. This is done to ensure the protection of information systems from unauthorized access, and to develop and coordinate plans for the recovery of critical systems and applications.

According to the Department of Information Technology, the Office of Information Security has already conducted a few security assessments at agencies. Future plans include conducting security training and assessments, publishing security bulletins, and coordinating disaster recovery planning. Through this office, DoIT can provide increased oversight and assistance to ensure agencies are complying with state standards for information security.

First-line Security Defenses Need Greater Attention

Devices such as routers and firewalls represent the state's first line of defense from threats that originate on the Internet. Routers are devices that route network traffic to and from its intended destination in a logical and efficient manner. They can also be used to filter out unwanted traffic. A firewall is a device that prevents all traffic from passing through unless the traffic has been specifically allowed by a set of rules established by the agency. Our review found areas for improvement in the security of these devices.

Router Configurations Can Be Improved

Only one of the three agencies we audited, the State Gaming Control Board, maintained its own routers. DoIT maintained the routers of the other two agencies we audited, and thus were not tested in our audit. We found multiple configuration settings that did not agree with established benchmarks for routers. In all, we identified 33 configuration changes to improve security of the three Gaming routers we examined. Some of these configuration changes were related to such items as limiting remote access to the routers so that hackers could not compromise these routers and reroute traffic. Routers should be periodically tested to determine if they are configured in accordance with the current benchmark standard. We noted that the agency's staff took immediate action to reconfigure their routers to enhance security.

In addition, Gaming indicated that passwords used to access the agency's routers were only six characters long. Eight characters in length is required by state standards.

Firewall Policy Needs Strengthening

Of the agencies reviewed, only Gaming maintained its own firewall. The other agencies used DoIT's firewall. We found no weaknesses in the rules applied to Gaming's firewall to establish security. However, the written firewall policy did not address who is authorized to create or modify firewall settings. State standards require firewall policies to address who can authorize changes. Without this, there is an increased risk that changes will be made to the firewall that management is not aware of.

Firewalls use rules to govern the flow of traffic and to prevent traffic unless specifically allowed by a rule. Because firewalls can contain many rules, the set of rules can become complicated. Because of its configuration, Gaming's firewall contained rules that had no impact on security. These rules should be deleted or deactivated to avoid the need to monitor unnecessary settings.

Computers Need Improved Security

Various computers maintained by the agencies we reviewed contained security weaknesses. The first of these, computers that run agency websites, contained vulnerabilities. In addition, computers used to run agency networks were not always securely configured. Finally, desktop computers were not always up-to-date with security patches or antivirus definitions.

Computers Running Agencies' Websites Need More Secure Configurations

Web servers are the computers that operate websites that are accessed via the Internet. Websites typically provide pages of linked information and are being used increasingly to facilitate access to state services. We found weaknesses in the configuration settings of agencies' web servers.

Two of the agencies we audited, Gaming and Corrections, maintained their own web servers. The other agency, PEBP, used DoIT's services to maintain its website. We tested the configuration of the two agency hosted web servers to determine if they were configured in accordance with best practices. We identified multiple configuration settings that were not in accordance with these practices. Gaming's web server needed 23 configuration changes while Corrections' web server required 18 changes. These changes were needed to reduce vulnerabilities that might allow compromise of the web servers such as a denial of service attack. Web servers should be periodically tested to determine if they are securely configured.

Network Servers' Security Settings 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 create settings such as user password length and composition. However, agency network servers did not comply with state standards. These standards are designed to guide agencies in securing their computer systems.

Our review found improvements need to be made in the standard for installing critical software security updates. In addition, password settings were weak. Furthermore, user accounts were not properly controlled.

Software Update Standard Needed

Patches are software updates supplied by manufacturers that often fix software security-related problems. Just as desktop computers require periodic updates of software security patches, so do the computers that run a network. We found that two of the agencies we audited had network servers that were missing critical updates. One of these agencies, PEBP, indicated it had an unwritten policy of installing these patches once each quarter and that this quarterly update had not yet occurred. Two of five network servers at Gaming were missing critical patches. Staff at Gaming indicated they applied these patches only in conjunction with routine computer maintenance. This was due to the remoteness of the network server locations. Agencies should have some discretion as to when patches are installed. However, neither agency had a written policy on when patches should be installed.

Without timely installation of software security patches, network servers remain vulnerable to unauthorized access, loss of functionality, and loss of data. A state standard on software patch management would assist agencies in understanding their responsibility. As of June 2005, a NITOC interim *Operating System Patch and Upgrade Management* standard existed. That interim standard does not indicate how often patches should be installed. A final standard for patch installation timeliness would be of great benefit to state agencies.

Password Settings

Network servers are used to administer user accounts and to set criteria for passwords such as their length, composition, and frequency of change. We found password settings were not in accordance with state standards for numerous user accounts at both Gaming and Corrections. Weak password settings allow hackers to gain easier access to user accounts using widely available password cracking software. We found the following password conditions at Gaming and Corrections:

State Gaming Control Board

- **Password change settings for individual users were set to change every 180 days rather than the state standard of every 90 days. In addition, all five administrator passwords, used to get access to the network servers, were not set to ever be changed.**

- **Individual users were allowed five invalid login attempts in one Gaming network while another network did not have a setting, thus allowing unlimited attempts. The standard is three or less attempts. In addition, administrative access to two network servers was set at five login attempts.**

- **Users should not be allowed to reuse the same password. Standard practice is six passwords should be remembered by the system, thus preventing password reuse. Four networks were set to remember only five passwords for individual users**

while one was not set. In addition, settings for administration of all five network servers were set to remember five passwords.

The traditional method for testing accounts is through a review of network settings. This method was used to test Gaming's settings. Corrections, however, was able to provide password settings for all users and administrative accounts. As a result, we tested all 1,051 Corrections' user accounts for conformity to state standards.

Department of Corrections

- **223 accounts were not required to have passwords. Passwords should be required for all users.**

- **173 accounts had passwords of fewer than the standard of eight characters in length, while 162 had no minimum length set.**

- **296 account settings allowed reuse of the same password after it had expired. Passwords should not be reused for six generations.**

- **241 account settings were not set to be changed every 90 days, which is the standard.**

- **108 accounts were set to allow more than the standard of three unsuccessful login attempts before locking the user out, while 236 did not have a lockout threshold set.**

Corrections has some older desktop computers that prevents password policies from being enforced on their network. This contributed to some of these weaknesses.

The Public Employees' Benefits Program uses a biometric fingerprint scan to authenticate users instead of using passwords. As a result, password settings are not applicable at PEBP.

Administrator Access Not Restricted

Computers use administrator accounts to grant and restrict user access. Administrator accounts and administrator level access provide substantial network privileges and should be restricted to the least number of accounts. These accounts should be accessible by a few agency IT personnel who need such access to maintain the system. Many users at Corrections had been granted administrative level privileges on their own computers. This would allow employees to alter security settings. In addition, we found that Gaming had several duplicate administrative accounts that were unnecessary. These conditions increase the risk of inappropriate use of agencies' networks and data.

Active User Accounts of Former Employees

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. We examined user accounts in each agency to determine if former employee computer accounts had been removed or disabled.

We found three former employees with active user accounts at Gaming. All agencies should have a process in place to ensure that employee user accounts are disabled immediately upon their separation from employment. Failure to disable these accounts may allow the person to gain unauthorized access to the network and its data.

Desktop Computers Not Updated With Latest Security Patches or Antivirus Definitions

Desktop computers are used by almost every state employee in the day-to-day performance of their job responsibilities. We tested agencies' desktop computers to ensure patches were appropriately applied and that antivirus software was current. We found weaknesses in both areas.

Software Patches Were Missing

Security patches should be installed on each desktop computer in order to protect from well known vulnerabilities. We identified missing critical security patches on desktop computers at Gaming, Corrections, and PEBP. In these three agencies, we found 35 of the 50 desktop computers we examined were missing critical patches. Some of these computers needed five or more critical patches. Gaming and Corrections installed the software updates when a desktop PC required other maintenance. PEBP installed them quarterly. The result was that these desktop PCs remained vulnerable to well-known threats for prolonged periods.

These vulnerabilities, if exploited by a hacker, could result in a takeover of the vulnerable computer as well as subsequent unauthorized access to the entire computer network on which the compromised PC resides. Such unauthorized access could result in theft or destruction of data and inoperability of the invaded computer network. For example, during August 2003, 72 state agency networks were infected with a malicious code. A state standard on how often software patches should be installed would assist agencies in understanding their responsibility related to installing these patches.

Antivirus Definitions Were Missing

State standards require antivirus software to be installed on each computer to protect from computer viruses that typically come from the Internet. The software needs to be periodically updated with new virus definitions. These definitions allow the software to more easily identify viruses and ensure protection from current threats.

The Department of Corrections had some computers whose virus definitions were not up-to-date. We tested 13 computers and found 1 did not have current virus definitions. This was caused by an error in settings that prevented the virus definitions from updating. Without current virus definitions, computers are more vulnerable to viruses and other malicious programs. Desktop computers should be periodically tested to determine if their antivirus definitions are being kept current. We noted that the agency took immediate action to correct the problem.

Other Security-related Procedures Need Strengthening

We found several other areas where network security could be improved. For example, disaster recovery planning was not adequate. In addition, security-related plans were incomplete or missing. Furthermore, access to some computer equipment was excessive.

Disaster Recovery Planning Needs Greater Attention

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For this reason, an agency should have procedures in place to protect information resources and minimize the risk of unplanned interruptions and a plan to recover critical operations, should interruptions occur. The state's NITOC standards require each agency to establish plans to ensure the ability to continue critical business services and operations. Furthermore, as shown in Appendix B, on February 7, 2005, the Governor issued an Executive Order requiring all agencies to have disaster recovery plans ready by February 1, 2006.

Events that could disrupt operations include power outages, hardware or software failures, vandalism, flooding, fires, and earthquakes. To avoid disruption from such events or to recover from them, a disaster recovery plan must address those components that maximize an organization's ability to protect assets.

The Department of Corrections did not have a disaster recovery plan. PEBP's plan concentrated on backing up data rather than true recovery of services. Gaming's disaster recovery plan was missing a few key components. For example, it had not been updated, and there was no evidence it had been tested or that employees had been trained on the plan. Without an adequate and fully tested disaster recovery plan, agencies increase the risk of losing their capability to process information.

The Office of Information Security within the Department of Information Technology has posted on their website a disaster recovery template. This document provides guidance on the items that should be considered in a plan. It is one method DoIT can use to provide much-needed assistance to agencies in creating and maintaining disaster recovery plans.

Security-related Plans Were Incomplete or Missing

The state's NITOC Security Committee has published several standards that require each agency to take actions to create its own IT security policy infrastructure. These agency specific policies are necessary in order to ensure that each agency has analyzed its own unique computing circumstances and their associated risks. These policies include: 1) conduct an IT risk assessment, 2) based on that risk assessment, create an IT security plan to mitigate the risks, and 3) establish an ongoing IT security awareness training program for all employees.

IT Risk Assessment

IT risk assessment provides a basis for IT risk management. It is a systematic process of identifying and evaluating risks and then implementing cost-effective controls or safeguards to reduce them.

Neither Corrections nor PEBP had completed a comprehensive IT risk assessment. Without completing a comprehensive risk assessment, it is unlikely these agencies will implement cost-effective safeguards proportionate to the risks to which they are exposed. In addition, some risks may go unidentified, leaving the agency more exposed and vulnerable than necessary.

IT Security Plans

A security plan provides for the protection of state information technology assets commensurate with the sensitivity and value of the information processed and maintained, and commensurate with the risk to public safety. Corrections did not have an IT security plan as required by NITOC standards. In addition, PEBP has security policies but not formatted into one cohesive plan. Recognizing the importance of these plans, the Governor issued an Executive Order which is shown in Appendix B. This order requires each state agency to develop an IT security plan by February 1, 2006.

DoIT's Office of Information Security has posted an IT Security Plan template on their website. This will help facilitate each agency's development of a plan.

Ongoing IT Security Awareness Training Program

An effective level of awareness and training of all state computer users is fundamental to a viable IT security plan. State standards require agencies to conduct ongoing IT security awareness training through such delivery mechanisms as security bulletins, e-mails, and websites.

We found that neither Corrections nor PEBP had implemented ongoing IT security awareness training. Although PEBP has a new hire training class, there is no ongoing security awareness training yet implemented. Gaming had established such a program using e-mail reminders.

During our audit, DoIT's Office of Information Security was in the user testing phase of a web-based security awareness training program. DoIT staff indicated they intend to make this web-based training available to all state employees once completed.

Physical Access Should Be Monitored More Frequently

We found that Gaming had allowed excessive access to its computer equipment room. At the time of our audit, 65 persons had access to the computer equipment room. Many were employees of other agencies in the same building. This access resulted from the installation of a new cardkey access system throughout the building about one week before our testing. However, it is unknown how long this situation would have continued had it not been identified during our audit. We noted that the agency took immediate action to reduce access to eight of its own employees. Physical access to sensitive computing and telecommunications equipment rooms should be periodically reviewed to ensure only appropriate individuals have access.

Recommendations

1. The Department of Information Technology should create a standard for timeliness of patch installation.
2. The Department of Information Technology should provide more ongoing assistance, training, and security assessments to state agencies regarding information security.

Appendices

Appendix A
Audit Methodology

To gain an understanding of Internet security, we conducted interviews at the State Gaming Control Board, the Department of Corrections, and the Public Employees' Benefits Program (PEBP). These agencies were selected based on popularity of their websites and the sensitivity of the information they store.

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, and the National Security Agency. In addition, we identified industry benchmark practices from organizations such as the National Security Agency, United States Government Accountability Office, Department of Defense, and the SANS Institute. Furthermore, we reviewed standards and procedures created by NITOC. To further understand Internet security, we obtained and reviewed network diagrams for the selected agencies.

To determine if controls limiting access to Gaming's network were adequate, we reviewed the configurations for three of their routers. We also reviewed the method used to maintain their firewall, including separation of duties and sufficient policies to guide staff. The other agencies selected in our review did not maintain their own routers and firewalls. They relied on the Department of Information Technology to maintain these devices. As a result, no review of these devices took place at Corrections or PEBP. For all agencies, we then examined their websites to determine if they allow sensitive information to be posted on the Internet.

Of the agencies selected for this review, Gaming and Corrections maintained their own web servers. We tested these computers to determine if they were configured in a secure manner that would prevent unauthorized users. We also tested computers at all selected agencies to determine if they had access settings in place to prevent unauthorized use. Next, we tested individual desktop computers 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 antivirus protection.

To assess security over communication devices, we reviewed each agency's use of modems. We also tested for unauthorized wireless connections at each agency.

We next evaluated additional security-related controls. We reviewed agencies' efforts at disaster recovery planning. Furthermore, we determined if agencies had conducted IT risk assessments, created IT security plans, and conducted ongoing IT security awareness training. Finally, we tested controls over access to rooms containing sensitive computer equipment.

At the end of our audit work, we met with management and staff of the State Gaming Control Board, the Department of Corrections, and the Public Employees' Benefits Program. During these meetings with each agency, we provided information on our audit work, gave specific details of test results, and asked for comments. We also explained to each agency that the Department of Information Technology would be responsible for responding to the audit recommendations in the final report.

Our audit work was conducted from August 2004 to June 2005, 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 Information Technology. On January 11, 2006, we met with officials from the Department to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix D which begins on page 26.

Contributors to this report included:

S. Douglas Peterson, CISA
Information Systems Audit Supervisor

Jeff Rauh, CIA, CISA
Deputy Legislative Auditor

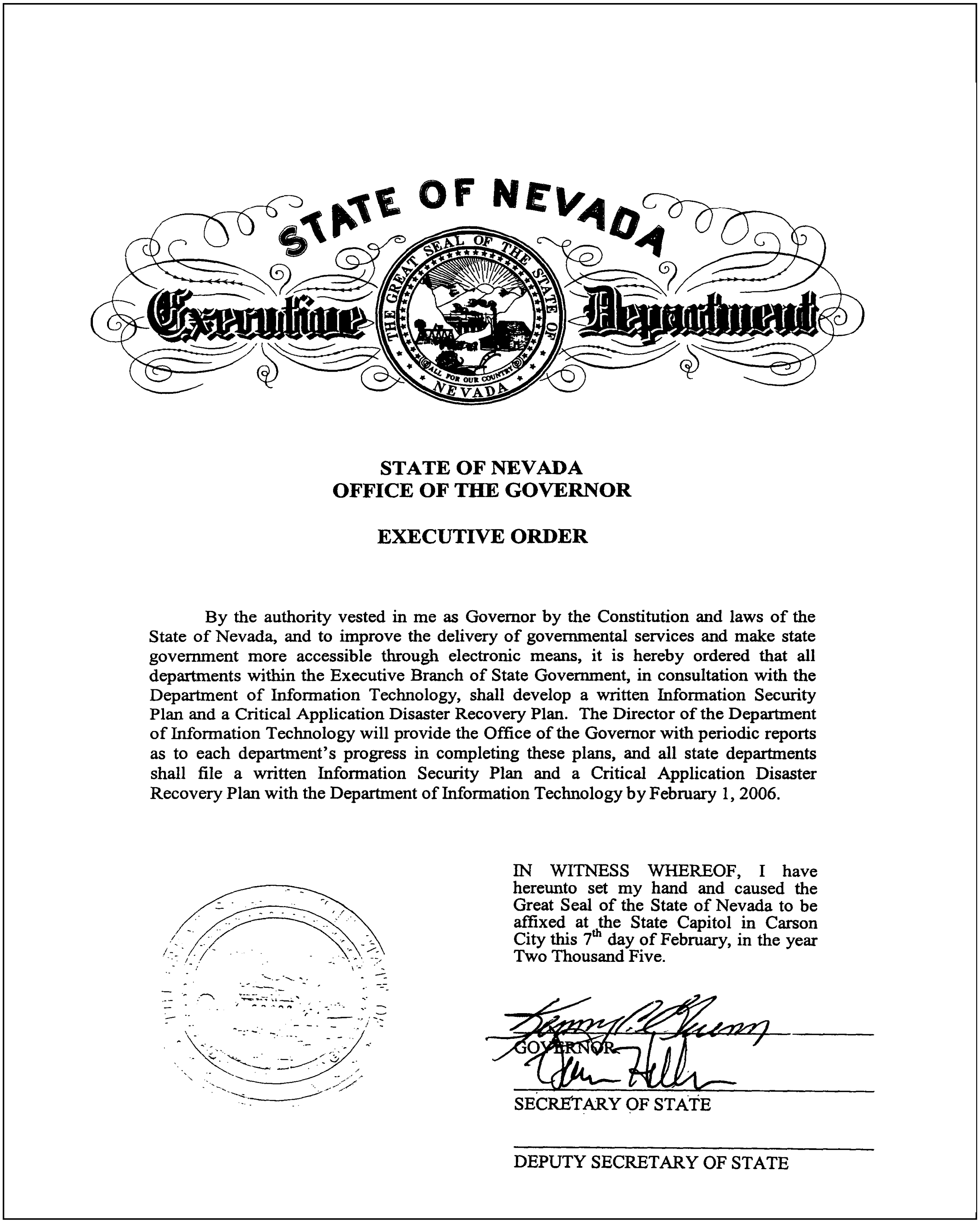
Grant Dintiman, CPA
Deputy Legislative Auditor

Kimberly Arnett, CPA
Deputy Legislative Auditor

Stephen M. Wood, CPA
Chief Deputy Legislative Auditor

Appendix B

Governor's Executive Order



STATE OF NEVADA

Executive Department

STATE OF NEVADA
OFFICE OF THE GOVERNOR

EXECUTIVE ORDER

By the authority vested in me as Governor by the Constitution and laws of the State of Nevada, and to improve the delivery of governmental services and make state government more accessible through electronic means, it is hereby ordered that all departments within the Executive Branch of State Government, in consultation with the Department of Information Technology, shall develop a written Information Security Plan and a Critical Application Disaster Recovery Plan. The Director of the Department of Information Technology will provide the Office of the Governor with periodic reports as to each department's progress in completing these plans, and all state departments shall file a written Information Security Plan and a Critical Application Disaster Recovery Plan with the Department of Information Technology by February 1, 2006.

IN WITNESS WHEREOF, I have hereunto set my hand and caused the Great Seal of the State of Nevada to be affixed at the State Capitol in Carson City this 7th day of February, in the year Two Thousand Five.

Kenny C. Guinn

GOVERNOR

Dean Heller

SECRETARY OF STATE

DEPUTY SECRETARY OF STATE

Appendix C

Glossary of Terms

Antivirus Software A utility that searches a hard disk and incoming e-mail 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.

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

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 that 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.

Local Area Network (LAN) A computer network that spans a relatively small area. Most LANs are confined to a single building or 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, the places where two or more networks connect.

Silvernet The name of the state's Wide Area Network (WAN)**.**

System Administrator 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.

Appendix C

Glossary of Terms
(continued)

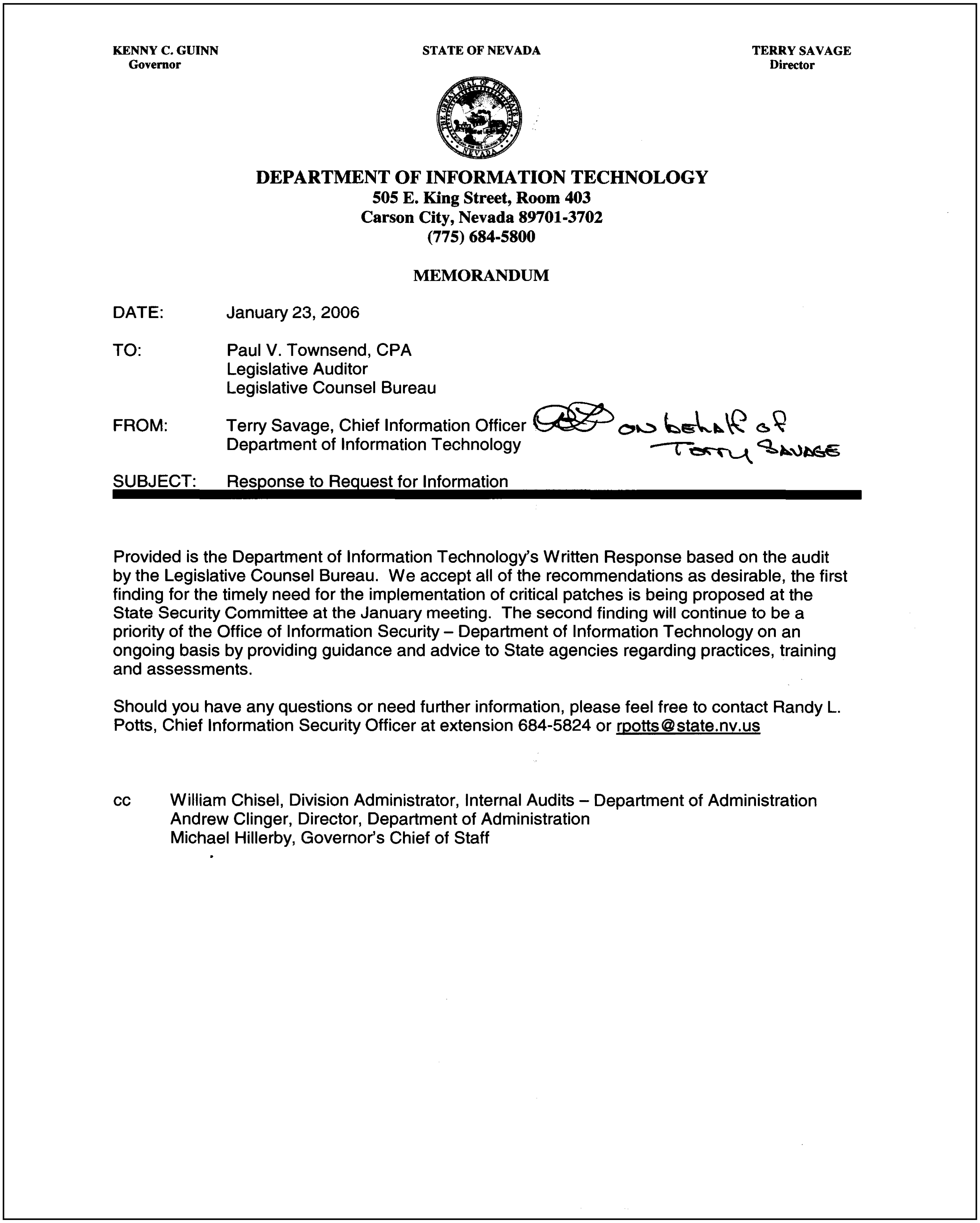
Web Server A computer that delivers (serves up) Web pages.

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.

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 D

Response From the Department of Information Technology



KENNY C. GUINN
Governor

STATE OF NEVADA

TERRY SAVAGE
Director

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

MEMORANDUM

DATE: January 23, 2006

TO: Paul V. Townsend, CPA
Legislative Auditor
Legislative Counsel Bureau

FROM: Terry Savage, Chief Information Officer on behalf of
Department of Information Technology Terry Savage

SUBJECT: Response to Request for Information

Provided is the Department of Information Technology's Written Response based on the audit by the Legislative Counsel Bureau. We accept all of the recommendations as desirable, the first finding for the timely need for the implementation of critical patches is being proposed at the State Security Committee at the January meeting. The second finding will continue to be a priority of the Office of Information Security – Department of Information Technology on an ongoing basis by providing guidance and advice to State agencies regarding practices, training and assessments.

Should you have any questions or need further information, please feel free to contact Randy L. Potts, Chief Information Security Officer at extension 684-5824 or rpotts@state.nv.us

cc William Chisel, Division Administrator, Internal Audits – Department of Administration
Andrew Clinger, Director, Department of Administration
Michael Hillerby, Governor's Chief of Staff

Department of Information Technology
Response to Audit Recommendations

Recommendation Number		Accepted	Rejected
1	The Department of Information Technology should create a standard for timeliness of patch installation ...	X	
2	The Department of Information Technology should provide more ongoing assistance, training, and security assessments to state agencies regarding information security	X	
	TOTALS	2	0