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
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*

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 Department of Motor Vehicles Information Technology Security. This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions. The results of our audit, including findings, conclusions, recommendations, and the Department's response, are presented in this report.

We wish to express our appreciation to the management and staff of the Department of Motor Vehicles for their assistance during the audit.

Respectfully presented,

Paul V. Townsend, CPA
Legislative Auditor

November 2, 2006
Carson City, Nevada

STATE OF NEVADA
DEPARTMENT OF MOTOR VEHICLES
INFORMATION TECHNOLOGY SECURITY

AUDIT REPORT

Table of Contents

Page

Executive Summary 1

Introduction 7

Background 7

Scope and Objective 8

Findings and Recommendations 10

Computers Need Critical Security Updates 10

Antivirus Protection Was Lacking on Some Computers 11

Password Controls Need Strengthening 12

Additional Web Server and Firewall Weaknesses 12

Web Server Security Needs Improvement 13

Web Server and Firewall Administration Needs Improvement 13

Access Controls to Network and Data Need Strengthening 14

Invalid Network Access 14

Excessive Time Required to Disable Network Access of Former Employees 15

Excessive Access to Production Data 15

Photo Capture Computers Contained Personal Information 17

Background Investigations Not Always Conducted 18

Appendices

A. Audit Methodology 20

B. Glossary of Terms 23

C. Response From the Department of Motor Vehicles 25

EXECUTIVE SUMMARY

DEPARTMENT OF MOTOR VEHICLES INFORMATION TECHNOLOGY SECURITY

Background

The Department of Motor Vehicles provides a variety of regulatory and licensing functions. Some of these include issuing driver licenses, vehicle registrations, and enforcing emission laws. The Department is headquartered in Carson City with a total of 21 offices located throughout the state. These include 17 full-service offices and 4 limited service offices.

The Department is increasingly using technological solutions to expedite the delivery of its services to the public. These include alternative driver license and vehicle registration renewal methods via the Internet and through electronic kiosks. The Internet and kiosk renewal transactions have grown rapidly since 2002.

The Department's increased reliance on technology to provide its services exposes it to greater risk from malicious users and the other problems that come with technology.

Purpose

The purpose of this audit was to determine if the Department of Motor Vehicles' network resources and data are secure from unauthorized access or modification. Our audit included a review of controls during fiscal year 2006.

Results in Brief

The Department has controls in place to protect its systems and data; however, some improvements are needed. For example, improvements need to be made in applying critical security updates to computers, installing and updating antivirus protection, and enforcing password standards. Some weaknesses also existed on the Department's web servers. In addition, access to some Department resources was too great. This included former employees with access to network resources, programmers' access to production data, and credit card information stored unencrypted on a computer. Furthermore, the Department had not conducted background investigations on some employees, including information technology staff and external users. These weaknesses, if left uncorrected, provide opportunities for malicious users to gain access to the Department's network and data.

Sensitive information was being stored on removable media attached to computers and on computers at various field offices throughout the State, without the Department's knowledge. This information contained names and social security numbers of some individuals who had renewed their driver licenses. A procedure to periodically test all computers designated for processing driver license photographs will ensure information is promptly deleted.

Principal Findings

- Computers running Microsoft Windows need to periodically be updated with the latest security software updates. Of the 87 desktop computers we tested for critical security updates at the Department, 17 did not have the expected software updates installed. In addition, several servers were missing these same security updates. These servers included network servers, the web server, and the computers that act as firewalls. State agency networks have been infected with malicious code in the past as a result of not having critical security updates installed. (page 10)

- Antivirus software is required by state standards to be installed on computers and regularly updated. This reduces the risk of viruses infecting computers and rendering them temporarily unusable. Of the 90 desktop and laptop computers we examined, 6 lacked adequate antivirus protection. In addition, we found four servers lacking antivirus software. (page 11)

- The Department's network servers were set to allow six unsuccessful login attempts before locking the users out of their computers, rather than the state standard of three attempts. In addition, the web server had some accounts with weak or non-expiring passwords. Further, the firewall had some accounts with no minimum password length. Weak password controls give malicious users greater opportunity to gain unauthorized access to the Department's network. (page 12)

- The Department's web server allowed the use of weak encryption keys for processing credit card transactions. These keys did not meet credit card industry encryption standards. In addition, the web server contained sample applications that can be used by hackers. Further, the Department did not have written policies and procedures for administering the web server. These factors combine to increase the risk of unauthorized access to the web server. (page 13)

- The Department did not have written policies and procedures for administering the firewall system. This documentation ensures that the firewall policies in effect are those that implement the security approved by Department management. They also help ensure continuity of security policies when the system's administrator changes or departs the agency. (page 14)

- Both the web server and firewall had too many user accounts with administrative level access privileges. Excessive accounts with administrative privileges increase the likelihood of unauthorized access or that unauthorized changes could be made to these devices. (page 14)

- Network servers contain accounts that are used to grant employees permission to use a computer network and its resources. We found that the Department had 31 active user accounts belonging to former employees. Continued network access could allow a former employee to gain unauthorized access to the network and its data. (page 15)

- When the Department disabled departing employees' computer user accounts, it often took too long. The Department's policy is to disable these accounts within eight days of an employee's departure. Thirteen of the user accounts we reviewed took longer than the Department's policy. Ten of these 13 user accounts averaged 54 days until being disabled. Untimely disabling of these accounts increases the risk of unauthorized access to the Department's network and its data. (page 15)

- The Department uses computer programmers to make modifications to the database used in the main DMV application. Programming staff have been granted update access to the database in order to quickly fix problems. However, there were no controls in place to ensure that changes to the database were only made when authorized. (page 15)

- The Department maintains a database of credit card transactions that includes sensitive personal information. This database is accessible to 44 Department employees and contains unencrypted credit card data. The Department has not encrypted this data because it intends to stop using the database by the end of 2006 and replace it with a new system. At that time the old database should be encrypted. (page 16)

- Each DMV field office is equipped with a computer to capture driver license photographs and personal information such as names, addresses, and social security numbers. Each day the prior day's information is to be deleted. However, we found various computer disks and two laptop computers with this data as far back as 2002. The Department has since implemented procedures to ensure old information is routinely deleted. (page 17)

- Although required by Department policy and state standards, the Department did not have evidence that all background investigations had been conducted on information technology staff. Thirteen of 52 Motor Vehicle Information Technology staff did not have documentation that a background investigation had been completed. Additionally, 23 non-state users such as county assessors and auto dealerships were allowed access to Department databases containing sensitive information without background investigations. (page 18)

- State standards require that those who access the Department's data sign security awareness statements indicating they understand the confidential nature of the information to which they have access. These statements also inform them of the penalties for the unauthorized disclosure of that information. We found that county assessor employees, and some other non-state employees with access to the Department's data had not signed such statements. (page 19)

Recommendations

This audit report contains 13 recommendations to improve information security at the Department of Motor Vehicles. These recommendations would help ensure greater security over desktop and server computers. In addition, they provide for better protection over the Department’s network and sensitive data. Finally, the recommendations would help ensure that employees in sensitive positions have background checks conducted. (page 29)

Agency Response

The Department, in its response to our report, accepted all 13 recommendations. (page 25)

Introduction

Background

The Department of Motor Vehicles' (DMV) mission is to:

> **Provide progressive and responsive service delivery to our citizens. We maintain the highest controls to ensure the accurate collection and timely distribution of all revenues. We improve the safety of those driving on our highways through our licensing, monitoring, and intervention practices. We assist Nevada in meeting its federally mandated air quality standards. We protect state consumers and businesses against fraud and unfair business practices. We ensure the integrity and privacy of our records.**

The Department is headquartered in Carson City with a total of 21 offices throughout the state that serve the public. There are 17 full-service offices and 4 limited service offices. The Department of Motor Vehicles had 1,188 full-time equivalent positions for fiscal year 2006. The Department is made up of seven divisions as follows:

- Administrative Services – provides various support functions to the Director's office and other divisions and agencies.
- Central Services and Records – provides support functions for driver licenses, registrations, titles, etc.
- Compliance Enforcement – enforces laws and regulations governing sales, emissions, repair, driver training, etc.
- Field Services – provides vehicle registration, driver license, and revenue collection activities.
- Management Services and Programs – provides support to the Director and other divisions with a focus on training, legislative and regulatory development, and related functions.
- Motor Vehicle Information Technology – provides support for the data processing activities of the Department including application design, coding, test and maintenance including network and operations support.
- Motor Carrier – enforces laws and regulations governing fuel taxes, motor carriers, and collections.

Alternate methods for renewing vehicle registrations and driver licenses have increased substantially with Internet and kiosk renewal transactions. Exhibit 1 shows the number of transactions for vehicle registration and driver license renewals for fiscal years 2002 to 2006.

Vehicle Registration and Driver License
Renewal Transaction Activity
Fiscal Years 2002 - 2006

Exhibit 1

	2002	2003	2004	2005	2006	2002 – 2006[1] % Change
Vehicle Registration Renewals						
Counter/Walk-in	531,004	538,637	547,988	572,989	602,162	13%
Mail-in	560,441	517,271	507,007	482,136	439,667	-22%
IVR (Telephone)	31,840	27,882	25,626	31,204	29,666	-7%
Web	134,185	216,741	287,385	356,287	420,405	213%
Kiosk	-	-	16,886	142,639	205,504	-
Totals	**1,257,470**	**1,300,531**	**1,384,892**	**1,585,255**	**1,697,404**	**35%**
Driver License Renewals						
Counter/Walk-in	223,730	224,817	223,197	203,692	219,402	-2%
Mail-in	50,722	40,200	47,850	63,570	71,891	42%
IVR (Telephone)	3,009	1,963	2,017	3,221	112	-96%
Web	11,339	13,932	18,213	27,347	38,229	237%
Kiosk	-	-	-	1,393	3,501	-
Totals	**288,800**	**280,912**	**291,277**	**299,223**	**333,135**	**15%**

[1] Kiosk service started in 2004 for vehicle registration renewals and in 2005 for driver license renewals.

The Department continues to capitalize on the capabilities of the Internet by automating additional services. The Department's increased reliance on technology to provide its services exposes it to greater risk from malicious users and the other problems that come with technology. This creates a need for increased security due to the sensitive data being transmitted back and forth over the Internet.

Scope and Objective

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission, and was made pursuant to the provisions of NRS 218.737 to 218.893. The Legislative Auditor conducts audits as part of the Legislature's oversight responsibility for public programs. The purpose of the legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This audit included a review of controls over the Department of Motor Vehicles' network, computers, and stored data during fiscal year 2006. The objective of the audit was to determine if the Department's network resources and data are secure from unauthorized access or modification.

Findings and Recommendations

Computers Need Critical Security Updates

Various computers were missing critical software security updates. These included desktop computers, computers used to run the Department of Motor Vehicles' (DMV) network, its web server, and computers that function as the Department's firewall. Department officials indicated it is their intent to install these critical software security updates within one week of their release.

Computers missing software security updates represent vulnerabilities in the Department's computer network defense system. The updates reduce the risk of a malicious entity exploiting the network's vulnerabilities to gain unauthorized access. According to the National Institute of Standards and Technology (NIST),

> **Vulnerabilities are weaknesses in software that can be exploited by a malicious entity to gain greater access and/or permission than it is authorized to have on a computer.**

Desktop Computers and Domain Controllers

Of the 87 computers we sampled at field offices statewide, we found 17 (20%) did not have the expected critical software security updates installed. In addition, the Department's five active directory network servers had not had critical security updates installed for over 16 months.

Web Server and Firewall

Web servers are the computers that host the websites that are accessed via the Internet. The Department website not only provides information about services and locations, it also allows customers the opportunity to renew their driver licenses and vehicle registrations without having to visit a DMV office. The Department accepts payment for these transactions via the website. Thus, sensitive personal information passes through this server.

Firewalls filter network traffic that pass through them based on a set of rules that define acceptable traffic on the network. If the traffic is going to, or originating from an unacceptable address – that traffic is discarded or blocked.

The web server and the computers that act as firewalls were missing critical security updates. Department officials indicated there was not an automated process to monitor the installation of critical software security updates. Such a process would greatly aid the Department's efforts at ensuring updates are installed properly.

Recommendation

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

Antivirus Protection Was Lacking on Some Computers

Some of the Department's computers were lacking antivirus protection. This included computers that had antivirus software installed but did not have current antivirus definitions and one computer that had no antivirus software installed.

Antivirus software must 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.

Of the 90 desktop and laptop computers we sampled statewide at various field offices, we found 6 computers (7%) that lacked adequate antivirus protection. Two of these computers had virus definitions that had not been updated in over 14 months. One computer had no antivirus software installed. In addition, we found four servers lacking antivirus software.

State standards require that all agencies' computers have antivirus software installed and that they should update virus protection software and definition files as new releases and updates become available. Department officials indicated they did not have a procedure in place to identify computers that were missing antivirus protection.

Recommendation

2. Develop a procedure to proactively identify any computers on the network that do not have current antivirus protection.

Password Controls Need Strengthening

Password controls ensure only authorized people have access to an agency's computers, network, and data. Weaknesses in password controls included allowing too many login attempts, weak passwords (i.e., passwords that do not use special characters or numbers), and non-expiring passwords. We found the following password control weaknesses on the various computers and servers at the Department:

- Network group policy settings that set password controls for users' computers allowed six unsuccessful login attempts instead of the state standard of three unsuccessful login attempts.
- The web server had one account with a weak password and three accounts with non-expiring passwords. The state standard requires strong passwords and changing of passwords every 90 days.
- Password settings on the two computers that acted as firewalls set no minimum password length. The state standard requires passwords be at least eight characters in length.

Weaknesses in passwords compromise security by allowing unauthorized individuals increased opportunity to gain access to the Department's network and gain access to critical data.

Recommendations

3. Set the group policy setting on the network server to lock out accounts after three unsuccessful login attempts.
4. Ensure password standards are enforced for the web server and firewall computers.

Additional Web Server and Firewall Weaknesses

We noted several areas where security over the Department's servers could be improved. These included weaknesses in the encryption used when web browsers communicate with the Department's web server. In addition, administration over the web server and the firewall servers needed strengthening. Furthermore, there appeared to be too many Information Technology (IT) staff with access to administer the servers and no written policies to guide staff's efforts.

Web Server Security Needs Improvement

We noted some additional weaknesses with the Department's web server. Because this server is used to accept payments for vehicle and driver license renewals, it must meet the standards established by the major credit card companies for the encryption of sensitive data. These standards are known as Payment Card Industry (PCI) standards. The PCI standards are designed to ensure the security of personal data such as bank card information as it moves over public networks such as the Internet.

Data encryption is handled by an encryption key used by the web server and the end user's web browser (for example: Internet Explorer). The key is used by the browser and the web server to encrypt the data being sent back and forth between the two computers. These keys can be various lengths with longer keys being more complex and thus more secure. PCI standards require encryption keys be a minimum of 128 bits in length. We found that the Department's web server allowed the use of keys with a length of 56 bits. While the Department had licensed an encryption key that met PCI standards, they were unaware of the weaker keys enabled on the system and thus had not disabled them. The Department promptly disabled the weak keys when they were notified of their existence.

We also found that the server still had sample applications installed as well as certain features enabled that increase the security exposure of the server. Microsoft and the National Institute of Standards and Technology (NIST) consider sample applications and the other security weaknesses we found to be severe security risks.

Web Server and Firewall Administration Needs Improvement

Computer administration encompasses the tasks, policies, and procedures for maintaining a computer system. The tasks include determining basic options and settings, authorizing changes to a computer system, making and testing changes, and implementing those changes in the production environment. We tested the administrative controls of the web server and the firewall. The administration of critical devices such as the web server and the firewall should be restricted to the fewest possible individuals knowledgeable about the device and its operation. We used an automated tool from Microsoft to check various features and settings on these computers. The Microsoft testing tool notes that any more than two administrator accounts are considered a non-critical failure. The web server had 30 accounts and the firewall had 18 accounts with administrative privileges. An excessive number of administrator accounts increases the security exposure of the devices and potentially lessens accountability. We also found there were no written policies or procedures with regard to the administration of these devices. Such a policy would guide the staff in determining the appropriate number of administrator accounts.

Recommendations

5. Periodically review the encryption keys to ensure they meet industry standards.
6. Develop policies and procedures necessary to administer the web server and firewall computers. These should address unnecessary settings, sample applications, and how many administrator accounts are needed.

Access Controls to Network and Data Need Strengthening

Department servers house sensitive data for Nevada consumers. System administrators use network servers to add or remove user accounts, control user access to files, and control other settings, such as encryption that further secures the data. During our testing we found that the Department needed to strengthen the control over these servers.

Our review found improvements needed to be made in the control over the maintenance of the network access lists. Additionally, programmers had update access to sensitive information with no monitoring of their activities. Furthermore, a database that stores transactions with credit card numbers was unencrypted.

Invalid Network Access

User accounts are created for each employee authorized to use an agency's computer network. These user accounts establish the employee's login identification, initial password, and their network access privileges. State standards require agencies to maintain a list of users that should be kept secure and up-to-date.

We examined user accounts to determine if former employee computer accounts had been removed or disabled. We found 31 former employees with active user accounts. These employees were either terminated, left state service, transferred or retired. Although the Department indicated these employee accounts had been previously disabled, changes to the network caused these accounts to be re-enabled. We noted the Department's staff took immediate action to disable these accounts.

All agencies should have a process in place to ensure that employee user accounts are disabled immediately upon their separation from employment and remain disabled. Failure to disable these accounts may allow a person to gain unauthorized access to the network and its data.

Excessive Time Required to Disable Network Access of Former Employees

We found 13 of 29 (45%) accounts of former employees were not disabled in a timely manner when employees left the Department. Ten of these accounts averaged 54 days before they were disabled. The Department's policy is to disable employee accounts within eight days of their leaving employment with the Department. The cause of this problem is that the Department's supervisors do not always submit the required IT security form to the Department's help desk in a timely manner. This could result in former employees gaining unauthorized access to the Department's network and its data.

Excessive Access to Production Data

With the data that the Department maintains, ensuring appropriate access is critical. Without such a system, there is increased risk of unauthorized changes to data or theft. For example, computer programmers had full update access to production data. In addition, a database with credit card transactions was unencrypted.

Programmer Access to Production Data

The Department maintains personal data on all the licensed drivers and registered vehicle owners in the state. This data resides on the state's mainframe computer within the Department of Information Technology. The Department of Motor Vehicles uses computer programmers to make modifications to the production data used to process transactions.

Our review found that the Department's programming staff have update access to the production data in the databases on the mainframe. This data includes personal information such as names, addresses, social security numbers, vehicle titles, and driver license information. Typically the ability to update production data is restricted to those groups and individuals who are accountable for maintaining the data. For the Department this would be the Field Services employees who deal with the public in registering and renewing vehicles and licenses.

Programming staff have been granted update access to this data in order to facilitate making data fixes in an expeditious manner when a customer is waiting. However, there were no controls in place to ensure that changes are only made when authorized. This means that changes to production data could be made that are unauthorized and untraceable. During the course of the audit, the Department implemented a log file to track changes made to sensitive production data tables. This should give the Department greater accountability over changes made to the data.

Credit Card Database

The Department maintains a database of sensitive personal information based upon credit card payment transactions completed since February 2000. The information is stored unencrypted and can be accessed by members of a group composed of 44 programmers and supervisors in the Department's IT area. An upgrade to the payment processing system is available that would encrypt the data. However, the Department has chosen not to purchase this upgrade since they are moving future transactions to a new system and payment data will no longer be stored in this database. While this improves the process for the future, it will still be necessary to maintain the database from the prior process. The Department indicates they will stop using the old system by the end of 2006. At that time they intend to store the database from the old process in a secure format.

Recommendations

7. Periodically review user accounts to identify former employees who have not had their access disabled.
8. Ensure that all supervisors submit timely notification of employee terminations to the Department's help desk.

9. Log and review updates to production data by the programming staff.
10. Encrypt the old credit card payment data for secure storage after the legacy system is retired.

Photo Capture Computers Contained Personal Information

In March 2005, a computer system was stolen from a DMV field office in Las Vegas. The stolen system contained personal information on approximately 8,700 Nevada residents. The Department took immediate action to protect the identities of the individuals by notifying them, reissuing driver licenses, and notifying the credit bureaus. The equipment was later recovered and a forensic analysis of the system indicated that the data had not been accessed. As a result of this incident, new procedures were implemented to ensure that no personal information was stored on the computers overnight and to encrypt the files stored on the system during the day.

Each DMV field office uses a computer with a special camera and printer to process driver licenses. This setup is through a contract with the Digimarc Corporation. As driver licenses are processed, personal data is encrypted and stored on drives attached to these computers. At the end of each day, the drives are removed from the computer and securely stored. The next day the previous day's files are deleted.

We tested the Digimarc systems in 10 field office locations around the state to ensure no old files were being stored on the computers or any drives attached to them. We found 321 files on a combination of removable disks, hard drives, and flash drives that contained personal information. The files dated from 2002 to the present. Of particular concern is the setup used by the Elko and Winnemucca offices. Each has a traditional computer system and another portable laptop system known as a traveler. The traveler is used when staff visit remote locations such as Jackpot and Lovelock. The Elko and Winnemucca traveler systems combined, accounted for 242 of the 321 old files we found. It should be noted that we could open these files and see names, addresses, and social security numbers for people who had renewed their driver licenses.

In other field offices we found files were located on removable disks referred to as Zip disks. Zip disks are similar to a floppy disk but with greatly expanded storage capacity. The Zip disk format was abandoned when Digimarc started using faster and larger capacity flash drives. However, we found some of the Zip disks were still in the Digimarc computers. We also found Zip disks stored in office safes. Once this was brought to management's attention, they removed the disks to have them erased or destroyed. The risk of allowing these files to remain on the computers and removable storage media like Zip disks is the potential future theft of personal data.

The Department took immediate action when notified of this situation. They contacted Digimarc and a series of discussions ensued. Through these discussions, it was made clear who had responsibility for removing old files from the computers. An automated process was put in place to delete any stray files at the end of the day. However, to ensure this process continues to work correctly, clear responsibility must be agreed upon and assignment made to review these computers periodically.

Recommendation

11. Periodically scan all Digimarc capture stations to ensure old files are removed.

Background Investigations Not Always Conducted

The Department processes many transactions for Nevada consumers. These transactions contain sensitive data, such as social security numbers, credit card numbers, names, and addresses. Department policy and state standards require background investigations on those positions and people with access to sensitive data maintained by the State.

Our test to determine if background investigations had been done focused on employees with routine access to sensitive data. We examined the Department's Motor Vehicle Information Technology (MVIT) staff, outside vendors, contractors, and other offices with access to this data. Of the 52 MVIT staff, 13 employees did not have evidence of background investigations in their personnel files. Department management attests that these background investigations have been previously conducted; however, there is no evidence in the personnel files to support this assertion.

Additionally, we found 23 non-state employees such as county assessor office employees, police departments, and auto dealership employees that did not have background investigations or signed security awareness documents. Security awareness documents ensure the Department that the outside entities have been informed of the sensitivity of the data they are allowed to access. In returning the document, the entity acknowledges its responsibility to keep the data safe. The Department indicated the lack of background investigations and security awareness documentation was due to the long standing relationships with some of these outside entities established prior to the requirements.

Without conducting background investigations, the risk increases that a person with previous criminal activity could be hired or granted access to sensitive data. Theft or improper disclosure of this information could result in identity theft. State agencies dealing with sensitive data should have a process in place to ensure that access is only granted to those employees or entities that have been investigated properly. The Department indicated that management would take action to complete the necessary background investigations and follow up with all outside entities regarding investigations and security awareness documentation.

Recommendations

12. Ensure that all Motor Vehicle Information Technology staff have a background investigation.
13. Work with external users to sign security awareness documents, and submit to a background investigation.

Appendices

Appendix A
Audit Methodology

To gain an understanding of the Department of Motor Vehicles, we interviewed Department management and staff. We reviewed legislation, committee minutes, as well as state and Department policies. We interviewed the Department's information technology staff to gain a broad understanding of the Department's network resources and how they are managed and utilized. We discussed how the Department interconnects and interacts with the Department of Information Technology, other state agencies, and third-party service providers.

To ensure our audit tests were representative of the Department's statewide operations, we conducted tests at 13 of the 17 full-service offices located throughout the state. The following locations were selected for testing:

- Carson City
- Reno
- Minden
- Winnemucca
- Elko
- Tonopah
- Hawthorne
- Yerington
- Las Vegas – Flamingo Office
- Las Vegas – Decatur Office
- Henderson
- Mesquite
- Pahrump

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

To determine if controls over desktop computer security were adequate, we tested a sample of the Department's desktop computers to ensure they were updated with the latest operating system updates as well as having current antivirus protection. We also examined the Department's network user accounts to determine if only current employees had access to the network. We then determined if the Department's computer network users had background investigations conducted and that they had signed security awareness statements.

To assess the security of the Department's network servers, we tested their security settings. Specifically, we tested to ensure they were configured to enforce state password standards for all accounts. We also conducted tests to identify 'backdoors' into the network through unauthorized or misconfigured wireless devices or dial-in modems. To ensure the Department's internal network was properly isolated from the public Internet, we examined the configuration and administration of the Department's computers that act as its firewall.

We tested the Department's web servers and web applications to determine if they were properly protected. We examined the Department's electronic payment process, used for online driver license renewals and vehicle registrations, and the data processed through it to determine if they were properly secured. We tested to determine that these online transactions used effective encryption methods to secure sensitive data passing over the Internet.

We examined how the Department backs up and secures its data. We reviewed the data captured by the Department's Digimarc servers as well as credit card payment data that the Department retains. We examined which users had access to sensitive data and if the data access was appropriately restricted. We examined how electronic kiosks and its transactions are secured. Finally, we examined the adequacy of the Department's plans for recovery operations in the event of a disaster.

Our audit work was conducted between November 2005 and July 2006, 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 Motor Vehicles. On October 18, 2006, we met with Department officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix C which begins on page 25.

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

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.

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.

Cipher Text Data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key.

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.

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

Encryption The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain (clear) text; encrypted data is referred to as cipher text.

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.

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 communication 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.

Kiosk A booth providing a computer related service, such as an Automated Teller Machine (ATM). Another type would offer tourist information. DMV kiosks allow users to process some individual transactions.

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

Appendix B

Glossary of Terms
(continued)

Patch An update to a software program or operating system.

Secure Sockets Layer (SSL) A protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data; a public key known to everyone and a private or secret key known only to the recipient of the message.

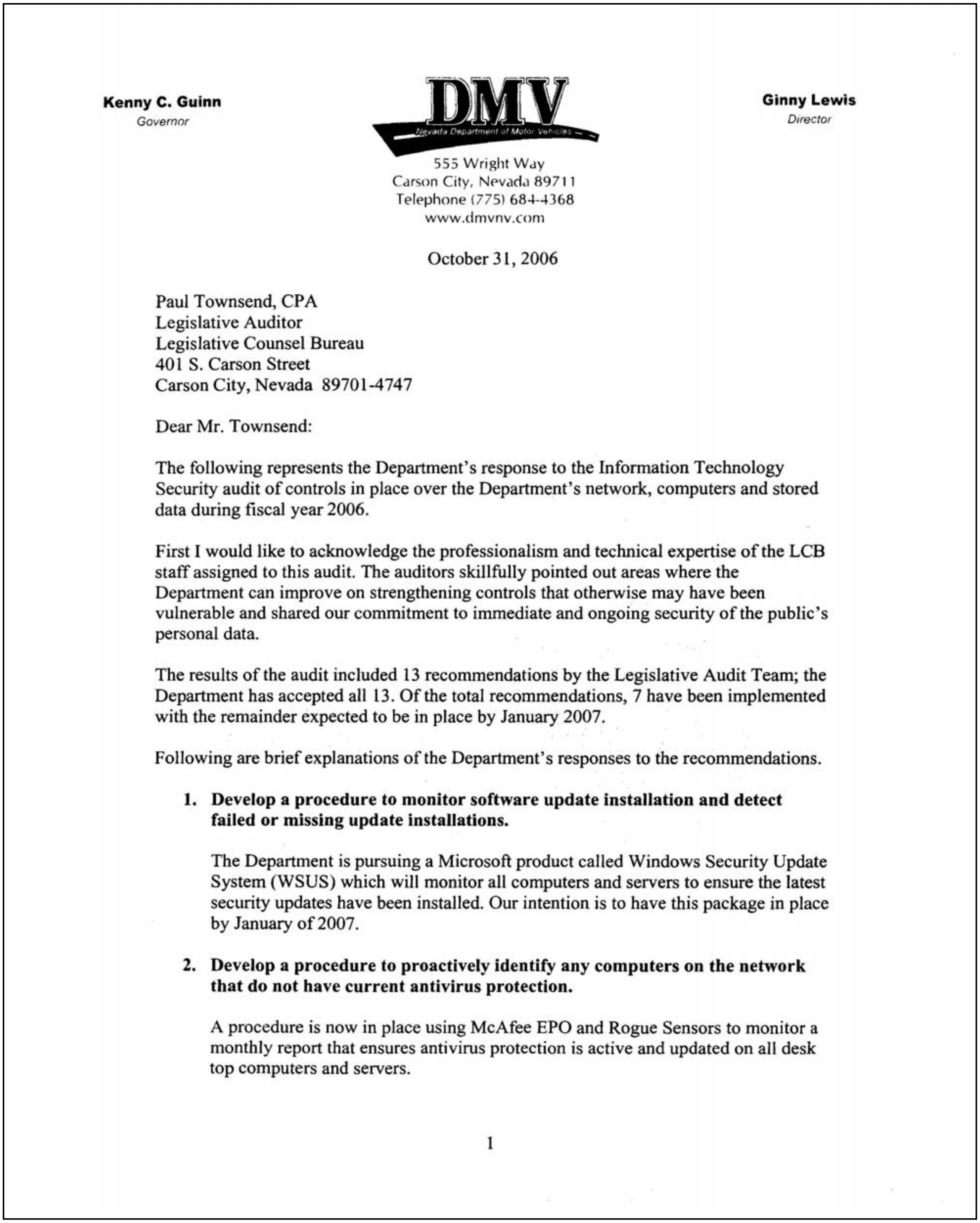
System Administrator (SA) An individual responsible for maintaining a multi-user computer system, including a local area network (LAN). Typical duties include: 1) adding and configuring new workstations, 2) setting up user accounts, 3) installing system-wide software, 4) performing procedures to prevent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

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.

Appendix C

Response From the Department of Motor Vehicles



Kenny C. Guinn
Governor

DMV
Nevada Department of Motor Vehicles

Ginny Lewis
Director

555 Wright Way
Carson City, Nevada 89711
Telephone (775) 684-4368
www.dmvnv.com

October 31, 2006

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

Dear Mr. Townsend:

The following represents the Department's response to the Information Technology Security audit of controls in place over the Department's network, computers and stored data during fiscal year 2006.

First I would like to acknowledge the professionalism and technical expertise of the LCB staff assigned to this audit. The auditors skillfully pointed out areas where the Department can improve on strengthening controls that otherwise may have been vulnerable and shared our commitment to immediate and ongoing security of the public's personal data.

The results of the audit included 13 recommendations by the Legislative Audit Team; the Department has accepted all 13. Of the total recommendations, 7 have been implemented with the remainder expected to be in place by January 2007.

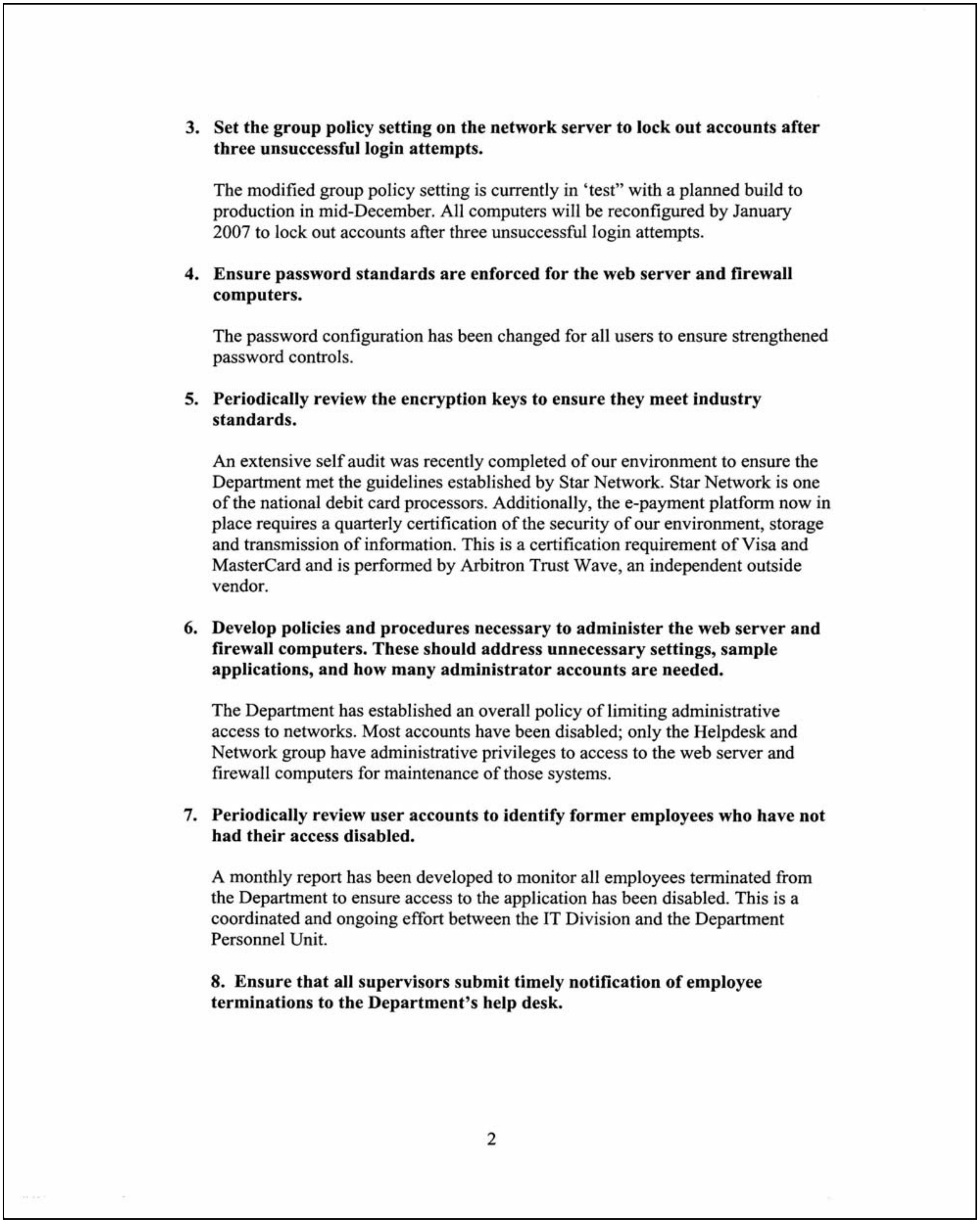
Following are brief explanations of the Department's responses to the recommendations.

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

   The Department is pursuing a Microsoft product called Windows Security Update System (WSUS) which will monitor all computers and servers to ensure the latest security updates have been installed. Our intention is to have this package in place by January of 2007.

2. **Develop a procedure to proactively identify any computers on the network that do not have current antivirus protection.**

   A procedure is now in place using McAfee EPO and Rogue Sensors to monitor a monthly report that ensures antivirus protection is active and updated on all desk top computers and servers.



3. **Set the group policy setting on the network server to lock out accounts after three unsuccessful login attempts.**

   The modified group policy setting is currently in 'test" with a planned build to production in mid-December. All computers will be reconfigured by January 2007 to lock out accounts after three unsuccessful login attempts.

4. **Ensure password standards are enforced for the web server and firewall computers.**

   The password configuration has been changed for all users to ensure strengthened password controls.

5. **Periodically review the encryption keys to ensure they meet industry standards.**

   An extensive self audit was recently completed of our environment to ensure the Department met the guidelines established by Star Network. Star Network is one of the national debit card processors. Additionally, the e-payment platform now in place requires a quarterly certification of the security of our environment, storage and transmission of information. This is a certification requirement of Visa and MasterCard and is performed by Arbitron Trust Wave, an independent outside vendor.

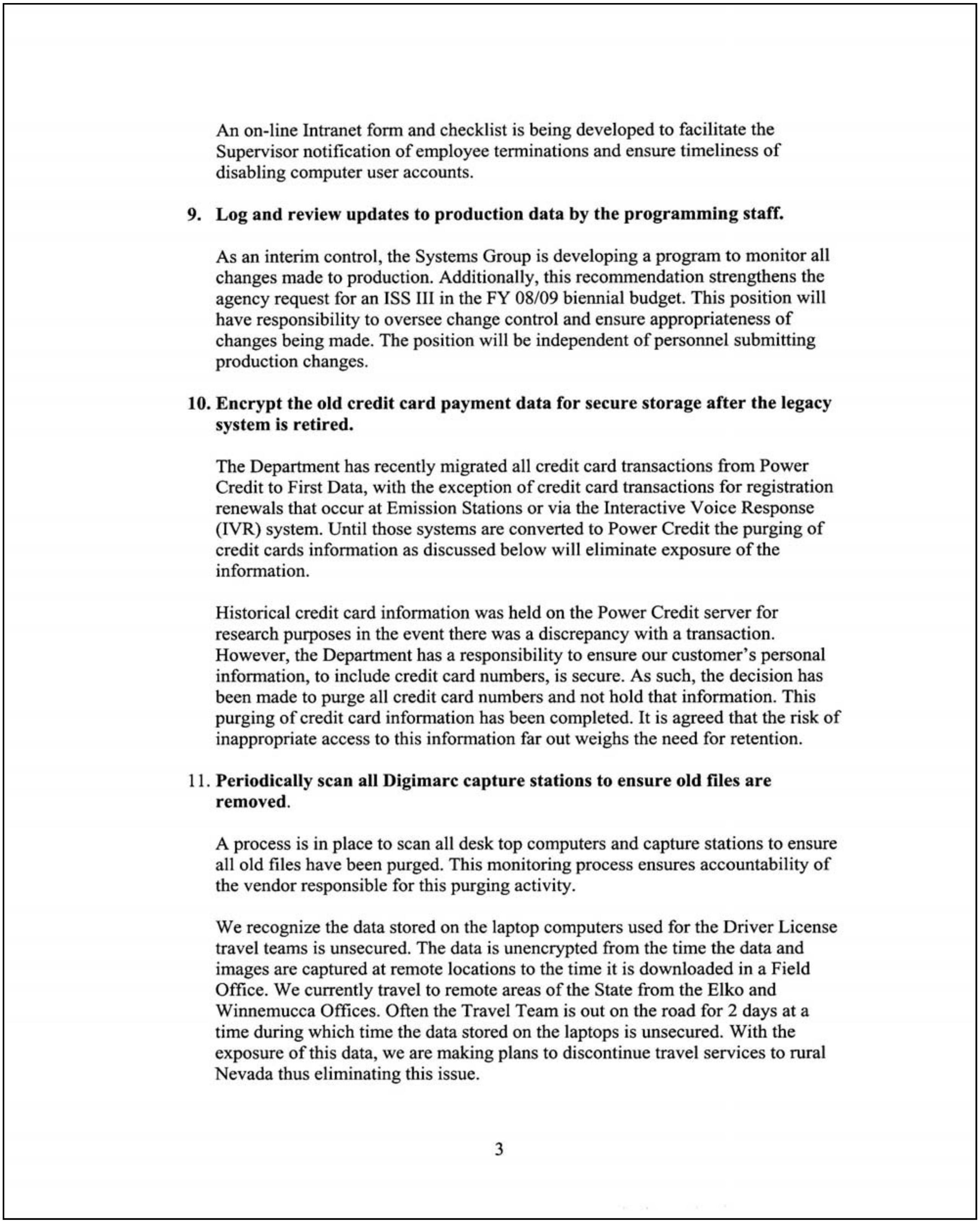
6. **Develop policies and procedures necessary to administer the web server and firewall computers. These should address unnecessary settings, sample applications, and how many administrator accounts are needed.**

   The Department has established an overall policy of limiting administrative access to networks. Most accounts have been disabled; only the Helpdesk and Network group have administrative privileges to access to the web server and firewall computers for maintenance of those systems.

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

   A monthly report has been developed to monitor all employees terminated from the Department to ensure access to the application has been disabled. This is a coordinated and ongoing effort between the IT Division and the Department Personnel Unit.

8. **Ensure that all supervisors submit timely notification of employee terminations to the Department's help desk.**



An on-line Intranet form and checklist is being developed to facilitate the Supervisor notification of employee terminations and ensure timeliness of disabling computer user accounts.

9. **Log and review updates to production data by the programming staff.**

   As an interim control, the Systems Group is developing a program to monitor all changes made to production. Additionally, this recommendation strengthens the agency request for an ISS III in the FY 08/09 biennial budget. This position will have responsibility to oversee change control and ensure appropriateness of changes being made. The position will be independent of personnel submitting production changes.

10. **Encrypt the old credit card payment data for secure storage after the legacy system is retired.**

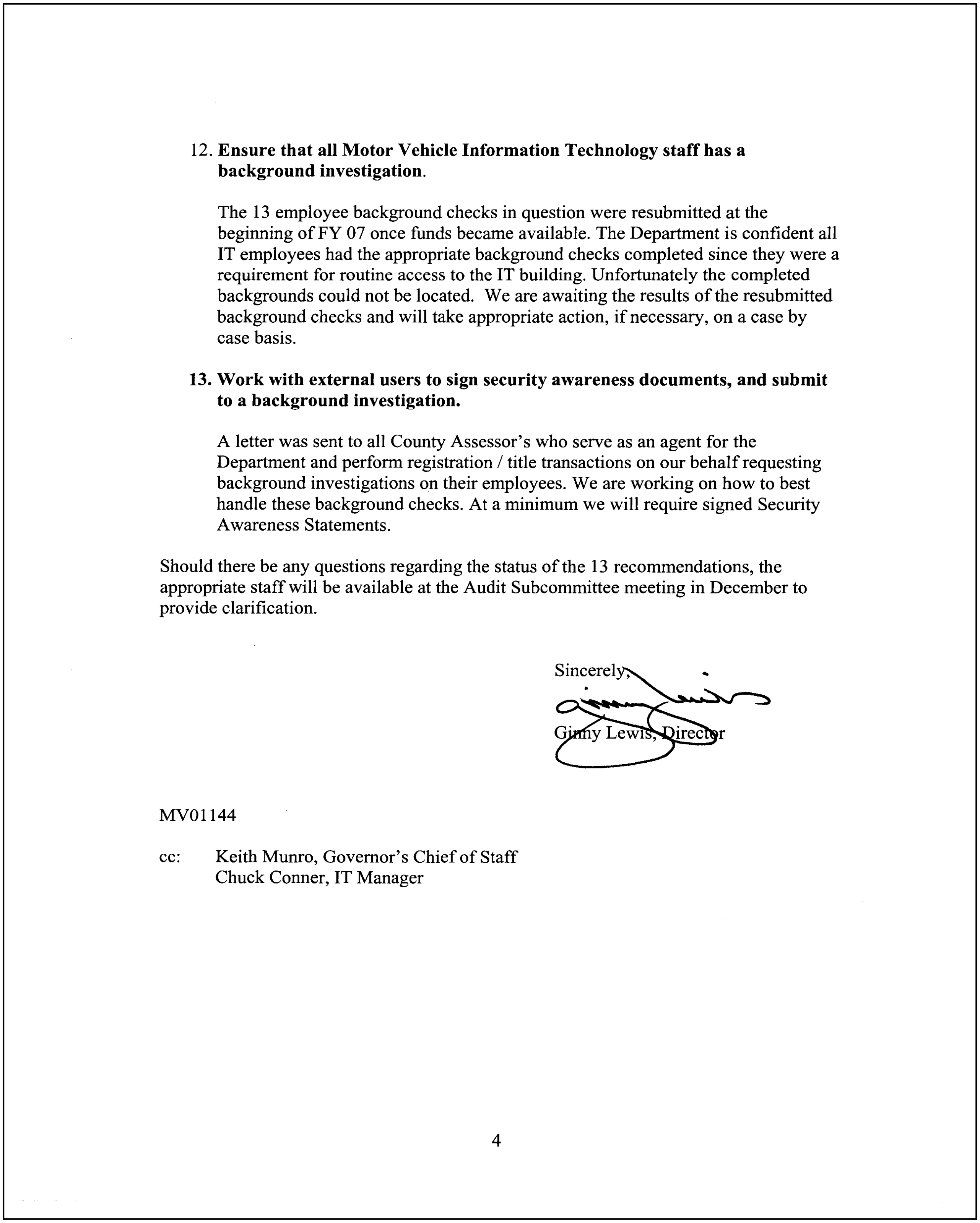
    The Department has recently migrated all credit card transactions from Power Credit to First Data, with the exception of credit card transactions for registration renewals that occur at Emission Stations or via the Interactive Voice Response (IVR) system. Until those systems are converted to Power Credit the purging of credit cards information as discussed below will eliminate exposure of the information.

    Historical credit card information was held on the Power Credit server for research purposes in the event there was a discrepancy with a transaction. However, the Department has a responsibility to ensure our customer's personal information, to include credit card numbers, is secure. As such, the decision has been made to purge all credit card numbers and not hold that information. This purging of credit card information has been completed. It is agreed that the risk of inappropriate access to this information far out weighs the need for retention.

11. **Periodically scan all Digimarc capture stations to ensure old files are removed**.

    A process is in place to scan all desk top computers and capture stations to ensure all old files have been purged. This monitoring process ensures accountability of the vendor responsible for this purging activity.

    We recognize the data stored on the laptop computers used for the Driver License travel teams is unsecured. The data is unencrypted from the time the data and images are captured at remote locations to the time it is downloaded in a Field Office. We currently travel to remote areas of the State from the Elko and Winnemucca Offices. Often the Travel Team is out on the road for 2 days at a time during which time the data stored on the laptops is unsecured. With the exposure of this data, we are making plans to discontinue travel services to rural Nevada thus eliminating this issue.



12. **Ensure that all Motor Vehicle Information Technology staff has a background investigation.**

    The 13 employee background checks in question were resubmitted at the beginning of FY 07 once funds became available. The Department is confident all IT employees had the appropriate background checks completed since they were a requirement for routine access to the IT building. Unfortunately the completed backgrounds could not be located. We are awaiting the results of the resubmitted background checks and will take appropriate action, if necessary, on a case by case basis.

13. **Work with external users to sign security awareness documents, and submit to a background investigation.**

    A letter was sent to all County Assessor's who serve as an agent for the Department and perform registration / title transactions on our behalf requesting background investigations on their employees. We are working on how to best handle these background checks. At a minimum we will require signed Security Awareness Statements.

Should there be any questions regarding the status of the 13 recommendations, the appropriate staff will be available at the Audit Subcommittee meeting in December to provide clarification.

Sincerely,

Ginny Lewis, Director

MV01144

cc: Keith Munro, Governor's Chief of Staff
Chuck Conner, IT Manager

Department of Motor Vehicles
Response to Audit Recommendations

Recommendation Number		Accepted	Rejected
1	Develop a procedure to monitor software update installation and detect failed or missing update installations	X	
2	Develop a procedure to proactively identify any computers on the network that do not have current antivirus protection	X	
3	Set the group policy setting on the network server to lock out accounts after three unsuccessful login attempts	X	
4	Ensure password standards are enforced for the web server and firewall computers	X	
5	Periodically review the encryption keys to ensure they meet industry standards	X	
6	Develop policies and procedures necessary to administer the web server and firewall computers. These should address unnecessary settings, sample applications, and how many administrator accounts are needed	X	
7	Periodically review user accounts to identify former employees who have not had their access disabled	X	
8	Ensure that all supervisors submit timely notification of employee terminations to the Department's help desk	X	
9	Log and review updates to production data by the programming staff	X	
10	Encrypt the old credit card payment data for secure storage after the legacy system is retired	X	
11	Periodically scan all Digimarc capture stations to ensure old files are removed	X	
12	Ensure that all Motor Vehicle Information Technology staff have a background investigation	X	
13	Work with external users to sign security awareness documents, and submit to a background investigation.	X	
	TOTALS	13	0