Audit Highlights

Highlights of Legislative Auditor report on the Department of Motor Vehicles Information Technology Security, issued on December 14, 2006. Report # LA06-23.

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 of Audit

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.

Audit 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.

The Department, in its response to our report, accepted all 13 recommendations.

Status of Recommendations

The Department's 60-day plan for corrective action is due on March 14, 2007. In addition, the six-month report on the status of audit recommendations is due on September 14, 2007.

Department of Motor Vehicles Information Technology Security

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, 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.

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.

The Department's network servers were set to allow six unsuccessful login attempts before locking 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.

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.

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.

When the Department disabled departing employees' computer user accounts, it often took longer than the Department's policy of 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.

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.

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.

Although required by Department policy and state standards, the Department did not have evidence that a background investigation had been conducted on 13 of 52 information technology staff. Additionally, 23 non-state users such as county assessors and auto dealerships were allowed access to Department databases containing sensitive information without background investigations.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Audit Division
Legislative Counsel Bureau