Audit Highlights

Highlights of Legislative Auditor report on the Department of Business and Industry, Information Technology Security issued on December 8, 2010. Report # LA10-25.

Background

The Department of Business and Industry consists of a Director's Office and 14 subordinate agencies, commissions, and programs with a main objective of encouraging and promoting growth, development, and the legal operation of businesses within the State of Nevada. The Department's activities also include regulation of business and industrial enterprises; promotion of worker safety, protection, and rights; and administration of bond programs to encourage growth and development of businesses within the state. The 14 organization subdivisions include:

- Athletic Commission
- Attorney for Injured Workers
- Dairy Commission
- Employee Management Relations Board
- Financial Institutions Division
- Housing Division
- Industrial Relations Division
- Insurance Division
- Labor Commission
- Manufactured Housing Division
- Mortgage Lending Division
- Nevada Transportation Authority
- Real Estate Division
- Taxicab Authority

For fiscal year 2010 the Department was authorized 673 full-time employees statewide and had authorized expenditures of approximately $144 million.

Purpose of Audit

The purpose of this audit was to determine if the confidentiality, integrity, and availability of the Department's sensitive information and information systems were properly protected. This audit included a review of information technology controls at the Department during fiscal year 2010.

Audit Recommendations

This audit report contains 11 recommendations to improve the information security at the Department of Business and Industry. These recommendations address controls over security of confidential information. In addition, these recommendations address controls over managing network users, network maintenance, and other security-related controls.

The Department accepted the 11 recommendations.

Status of Recommendations

The Department's 60-day plan for corrective action is due on March 8, 2011. In addition, the six-month report on the status of audit recommendations is due on September 8, 2011.

Information Technology Security

Department of Business and Industry

Results in Brief

Weaknesses existed in controls designed to protect the confidentiality, integrity, and availability of the Department's sensitive information and information systems. These weaknesses included computers storing unencrypted sensitive personal identifying information. In addition, computers did not have adequate virus protection and lacked current critical software updates. Furthermore, former employees had current network access and background investigations were not conducted on staff with the greatest access to confidential information.

Other security-related controls need improvement. For example, ongoing security awareness training was not conducted to maintain staff awareness of information security risks. In addition, some servers were not properly protected, a wireless network was not adequately secured, and web servers had vulnerabilities.

Principal Findings

Confidential personal information was stored unencrypted on Department computers. Six Department divisions had application databases containing substantial amounts of unencrypted personal information such as social security numbers. In addition, we identified 23 other computers storing unencrypted personal information. This included 7 servers and 16 individual desktop computers that contained this personal information. If this information is inadvertently accessed or released, the Department would be required to contact all of the affected persons.

Virus protection software was not current or not installed on some computers. Of the 161 desktop computers sampled, we found 24 computers or 15% of our sample that lacked adequate antivirus protection. We found additional computers without virus protection during other tests. Virus definition ages averaged over 206 days old. State security standards require that all computers have antivirus software and current virus definition files. Without current virus protection, there is increased risk that computers will become infected.

Seven computers were missing critical software security patches. This included four desktop computers and three servers. One computer had not been updated for 438 days. If critical software security updates are not installed, there is increased risk that computers will be vulnerable to various hacker attacks and exploits.

Five former employees' network access had not been disabled in a timely manner. The duration these five accounts remained enabled after the employee had left the agency ranged from 102 days to 7.5 years. State security standards require the prompt removal of users who are no longer in the Department's service in order to reduce the risk of someone gaining unauthorized access to the state's network and data.

Background investigations are not conducted throughout the Department. State security standards require that state employees in positions identified as sensitive have background investigations conducted. Without conducting background investigations on staff with the greatest access to sensitive information and systems, the risk increases that a person with an unsuitable background could be hired or granted access to these systems.

Ongoing security awareness training was not being conducted throughout the Department. The intent of this training is to ensure that all new and existing employees, consultants, and contractors are aware of their responsibilities in protecting the state's information systems and information processed through them. Without annual information security refresher training, there is greater risk that employees will not adequately protect state information systems.

Six of the 26 (23%) network servers or server rooms were not adequately protected. This included unrestricted access to equipment and one room with a leaky roof. Unrestricted physical access to network servers increases the risk of accidental damage and theft or vandalism. Such problems could also result in the release of confidential data or the loss of use of the computer network.

We identified three web servers whose configurations could be made more secure. Scans of these web servers revealed several vulnerabilities in their configurations. These vulnerabilities could allow hackers to modify the web servers and cause them to malfunction. Staff indicated they had not previously conducted vulnerability scans on these web servers.

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