Audit Highlights

Highlights of performance audit report on the Department of Taxation, Information Security issued on October 29, 2018. Legislative Auditor report # LA18-23.

Background

The mission of the Department of Taxation (Department) is to provide fair, efficient, and effective administration of tax programs for the State of Nevada in accordance with applicable statutes, regulations, and policies.

The Department has four offices located in Carson City, Henderson, Las Vegas, and Reno.

For fiscal year 2017, the Department had 429 authorized employees statewide, with 27 filled positions comprising the Information Technology (IT) unit.

The Department collects 17 taxes and administers the collection and distribution of more than $6 billion annually. The revenue collected by the Department provides funding to all levels of Nevada government, including school districts, cities, counties, and the State.

Purpose of Audit

The purpose of our audit was to determine if the Department has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information systems. Our audit focused on the systems and practices in place during fiscal year 2018.

Audit Recommendations

This audit report contains 17 recommendations to improve the security of the Department's information systems.

The Department accepted the 17 recommendations.

Recommendation Status

The Department's 60-day plan for corrective action is due on January 29, 2019. In addition, the six-month report on the status of audit recommendations is due on July 29, 2019.

Information Security

Department of Taxation

Summary

The Department needs to strengthen information system controls to ensure adequate protection of information systems and the data processed therein. By taking action to address control weaknesses, the Department can better protect its physical resources, minimize security vulnerabilities, and ensure continuation of mission-critical services.

Control weaknesses included: (1) inadequate protection of server and telecommunications rooms to prevent unauthorized access and maintain optimum temperatures; (2) building access cards not routinely monitored; (3) inadequate monitoring of the status of security updates on laptop computers; (4) not adequately managing network users, including not disabling accounts of former employees; (5) incomplete backup and recovery documentation; (6) incomplete IT contingency planning; and (7) noncompliance with annual security awareness training requirements.

Key Findings

The Department needs to provide better protection for four of its five server and telecommunications rooms. For example, three rooms housing servers and networking equipment were not secured from unauthorized access. In addition, two rooms lacked controls to maintain optimum temperatures. As a result, network infrastructure is at risk of being stolen, damaged, or improperly accessed. (page 4)

The Department's building card access system, which controls access to the building's main entrances, is not routinely monitored. We identified 23 building access cards that needed to be deactivated. The Department needs sufficient measures in place to issue, replace, activate, and deactivate building access cards. (page 6)

The Department did not monitor the status of security updates on its 113 laptop computers to assist in protecting against security vulnerabilities. During our audit, most laptops had not received security updates. Staff in the Department's IT unit utilize a systems management application to update its laptops twice a month. However, after a scheduled update, we found only 2 of 66 laptops had successfully received the updates. (page 7)

The Department did not ensure Virtual Private Networking (VPN) accounts of former staff were disabled when employees transferred or terminated. A VPN allows users to connect to the Department's network resources through the Internet. We identified 33 of 120 VPN accounts that needed to be deactivated after employees transferred or terminated. Seven of the 33 accounts remained enabled for over 1 year after employees had left the Department. (page 8)

The Department does not review user access privileges for two of its four mission-critical applications that collect and distribute tax monies. In one application with 406 accounts, we identified 50 active accounts whose access was no longer appropriate based on the employees' status. Fourteen of the 50 accounts remained active for over 12 months after employees had left the Department and access should have been terminated. In addition, the Department does not maintain a current list of authorized users for these two applications. Without a current list of authorized users and annual evaluation of system access privileges, the Department is unable to periodically review if user access is appropriate. (page 9)

Background checks were not always completed for the Department's contractors. There was no evidence showing 6 of the Department's 12 contractors had background checks conducted. These contractors had specific responsibilities that gave them access to the Department's critical systems. State security standards indicate contractors who work for or provide IT services to the State and are identified as sensitive, require background checks. (page 10)

The Department does not have adequate documentation of its backup and recovery process. Without adequate documentation of its existing backup and recovery process, the Department cannot develop comprehensive recovery procedures for each system, application, and associated data. Clearly documented procedures bring more predictability to the backup and recovery process and ensure the consistent protection of Department data. (page 11)

The Department does not have a complete IT contingency plan. An IT contingency plan should contain sufficient information and instruction to enable management to assure its ability to continue its critical business services and operations. Without a current IT contingency plan, the Department cannot prioritize and categorize recovery of its critical systems. (page 12)

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