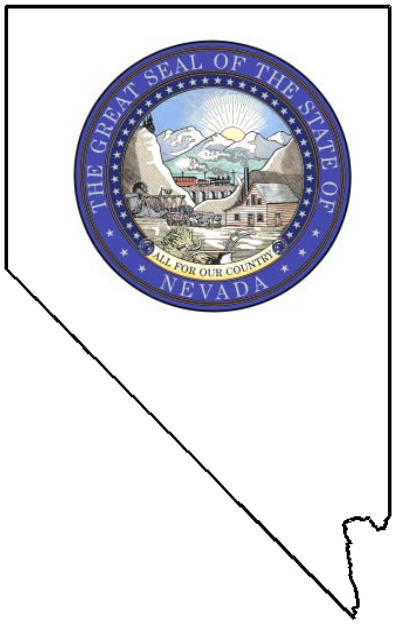
LA18-23

STATE OF NEVADA

Performance Audit

Department of Taxation
Information Security

2018



Legislative Auditor
Carson City, Nevada

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

STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747

RICK COMBS, *Director*
(775) 684-6800

LEGISLATIVE COMMISSION (775) 684-6800
JASON FRIERSON, *Assemblyman, Chairman*
Rick Combs, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
JOYCE WOODHOUSE, *Senator, Chair*
Mark Krmpotic, *Fiscal Analyst*
Cindy Jones, *Fiscal Analyst*

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830
ROCKY COOPER, *Legislative Auditor* (775) 684-6815
MICHAEL J. STEWART, *Research Director* (775) 684-6825

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Department of Taxation, Information Security. This audit was conducted pursuant to 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.

This report includes 17 recommendations to improve the security of the Department's information systems. We are available to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other state officials.

Respectfully submitted,

Rocky Cooper, CPA
Legislative Auditor

October 9, 2018
Carson City, Nevada

Department of Taxation
Information Security
Table of Contents

Introduction

Background

The Department of Taxation (Department), established in 1975, is responsible for the general supervision and control over the state's revenue system. The mission of the 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 Department's Information Technology (IT) unit.

The IT unit is responsible for the operation, maintenance, and on-going enhancements of:

- The Unified Tax System (UTS) which includes the Tax Accounting System (TAS);
- The Nevada Tax Center, the online tax filing service; and
- The Discover Tax data warehouse and other UTS dependent software.

In addition to UTS, the IT unit supports the official website for Taxation, Masters Settlement Agreement (MSA) Tobacco System; the Department's Intranet site; statewide Local Area Network/Wide Area Network (LAN/WAN); and desktop applications. The IT unit is also responsible for supporting the Marijuana Enforcement Division's Tax Agent Portal.

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.

Scope and Objective

The scope of our audit included a review of the systems and practices in place during fiscal year 2018. Our audit objective 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.

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 218G.010 to 218G.350. 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.

Summary

The Department of Taxation (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.

Server and Telecommunications Rooms Need Better Protection

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.

Server and telecommunications rooms were not adequately secured from unauthorized access. In the Reno office, the server and telecommunications room did not have a lock to prevent unauthorized access. In the Carson City office, the telecommunications room was secured with a key lock; however, IT staff were not aware of how many individuals had a key. The Department utilizes a building card access system to control access to some offices, and server and telecommunications rooms. Access to the primary server room in the Carson City office is managed by this system. Through multiple discussions with staff, we determined they did not routinely review personnel accounts within their card access system. Only seven IT staff were authorized to have access to the primary server room. We determined 19 employees were inadvertently given access to this room. Of the 19 employees, all were current staff except for 1 former employee.

State security standards indicate that appropriate controls must be implemented to ensure rooms that contain IT resources that process, transmit, or store sensitive or private information are protected. Rooms shall be protected from unauthorized access,

physically secure, and environmentally sound in accordance with industry and manufacturers' standards.

Additionally, the server and telecommunications rooms in the Carson City and Henderson offices lacked controls to maintain optimum temperatures. Without employing such controls, possible fluctuations in temperature could lead to equipment overheating and being damaged. Staff in the Henderson office were aware of the elevated temperatures in the server room, while staff in the Carson City office indicated they rarely accessed the telecommunications room and were not aware of the elevated temperatures. State security standards require networking equipment be operated within a temperature controlled environment to reduce the risk of equipment failure due to overheating.

Recommendations

1. Ensure all server and telecommunications rooms have locked doors.
2. Review existing access and determine a viable method to monitor personnel entering the Carson City telecommunications room.
3. Ensure personnel accounts within the card access system are periodically monitored.
4. Perform an on-site review and develop a plan to ensure the server and telecommunications rooms are maintaining optimum temperatures in accordance with industry and manufacturers' standards.

Building Access System Administration Needs Improvement

The Department's building card access system, which also controls access to the building's main entrances, is not routinely monitored. We identified 23 building access cards that needed to be deactivated. The access cards requiring deactivation included 11 former Department employees, 9 former contractors, and 3 employees from other State agencies. Three building access cards remained active for 2 years after employees had left the Department. The Department was collecting access cards upon employee departure; however, the building access administrator did not routinely review building card access against active employee assignments.

The Department needs sufficient measures in place to issue, replace, activate, and deactivate building access cards. Without proper distribution, documentation, and physical security of building access cards, unauthorized persons could gain building access. State security standards indicate building access administrators are responsible for the input and review of all personnel records within their building.

Recommendation

5. Implement procedures to review building card access within each secured area, delete inactive cards, and disable cards upon termination or transfer.

Administration of Laptop Computers Can Be Improved

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. The Department utilizes laptops for its auditors and abatement officers that work remotely. Because these laptops are used in the field, it is important they stay current with security updates to reduce vulnerabilities that could be exploited.

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 laptop computers had successfully received the updates. Through discussions with staff, we determined there was a lack of review to verify updates were completing successfully. Staff acknowledged additional training and vendor support is needed to gain more familiarity with the systems management application and its capabilities.

The Department needs to ensure laptops are kept current with the latest security updates. The Department increases its risk of a security breach by running software that is not current. State security standards require state entities to establish and implement an update management process for all systems and networks in a manner that ensures maximum protection against security vulnerabilities and minimizes impact on entity business operations.

Recommendations

6. Obtain additional training to utilize full capabilities of the systems management application to improve laptop computer administration.
7. Develop procedures to routinely detect and correct failed laptop computer security update installations.

Weaknesses Exist in Managing Network Users

Weaknesses exist in managing the Department's network users. These weaknesses include not disabling former employees' Virtual Private Network (VPN) accounts, as well as not removing network user accounts after employees transferred or terminated. Additionally, the Department does not review user access privileges nor maintain a current user list for two of its four mission-critical applications. Furthermore, some contractors did not complete the required background checks. Background checks investigate a candidate's background and identify potential hiring risks for safety and security reasons.

Virtual Private Network Access Was Not Disabled

Former employees' VPN accounts were not disabled in a timely manner. 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. The Department should revise its existing help desk process to include disabling VPN accounts for departing employees. Untimely disabling of VPN accounts increases the risk that someone could gain unauthorized access.

IT systems and networks must have logical access controls to provide protection from unauthorized access, alteration, loss, disclosure, and availability of information. State security standards indicate termination of an employee must cause immediate revocation of all system and information access privileges. In addition, user accounts must be reviewed quarterly to ensure the continued need for access to a system and that disabled accounts have been deleted.

User Access Privileges Need Greater Review

The Department does not review user access privileges for two of its four mission-critical applications that collect and distribute tax monies. We reviewed the Department's four applications for authorized user account access. 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.

Furthermore, 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. This increases the risk for unauthorized access to the Department's critical applications. State security standards dictate system managers shall re-evaluate system access privileges granted to all users annually, at a minimum. In addition, a master user list of all users shall be maintained, kept secured, and up-to-date, reflecting all systems to which they have access.

Network User Accounts Were Not Removed in a Timely Manner

The Department did not always remove former employee network user accounts in a timely manner. The Department was disabling network accounts upon employee departure; however, it did not perform routine account maintenance to remove obsolete accounts. We identified 707 disabled user accounts in the Department's user directory that were not removed. Removing obsolete user accounts on a regular basis is one way to protect the user directory from threats of unauthorized access.

State security standards indicate user accounts must be reviewed quarterly to ensure the continued need for access to a system and that transferred or resigned users have been deleted. IT systems and networks must have logical access controls to provide protection from unauthorized access, alteration, loss, disclosure, and availability of information.

Background Checks of Some Contractors Were Not Occurring

Background checks were not always completed for the Department's contractors. There was no evidence showing that 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. We determined there was not a follow-up process in place with the Department of Administration's Division of Human Resource Management to ensure contractors completed the required background check.

Background checks investigate a candidate's background and identify potential hiring risks for safety and security reasons. The greatest harm to a system comes from the actions of individuals, both intentional and unintentional. State security standards indicate contractors who work for or provide IT services to the State and are identified as sensitive, require background checks.

Recommendations

8. Revise the current help desk process to include disabling and removal of VPN accounts.

9. Maintain a current list of all VPN accounts and verify its accuracy quarterly.

10. Revise the Department's existing user access review process to include all applications.

11. Maintain a current list of all user accounts for each application and verify its accuracy at least annually.

12. Develop a procedure to ensure routine review and removal of obsolete network user accounts.

13. Develop a process to ensure all contractors have required background checks.

Data Backup and Recovery Process Needs to Be Documented

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. Department staff indicated they lack adequate documentation of the backup and recovery process and plan to enhance existing documentation.

State security standards state the owner of applications or data is responsible for coordinating, scheduling, and ensuring that appropriate backups are accomplished. In addition, the owner is responsible for ensuring appropriate backup and recovery plans, procedures, retention schedules, and testing is accomplished and documented.

Recommendations

14. Update the Department's existing backup process documentation.

15. Develop recovery process documentation for each system, application, and associated data.

Information Technology Contingency Plan Can Be Improved

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 the agency's ability to continue its critical business services and operations, including those used by branch or remote offices. Through discussions with staff, and a review of the Department's IT contingency documentation, we determined the Department has not adopted an official IT contingency plan. Furthermore, the Department acknowledges that any IT contingency plan in place is deficient and needs more attention.

Without a current IT contingency plan, the Department cannot prioritize and categorize recovery of its critical systems. State security standards state that each agency must be able to continue to provide mission-critical services that are supported by IT resources should a situation occur that renders the resources inaccessible due to a system or application malfunction or hardware failure.

Recommendation

16. Update the existing IT contingency plan to include the recovery priority of the Department's mission-critical systems.

Staff Did Not Always Complete Required Security Awareness Training

Forty-five of the Department's 381 employees and contractors had never taken the State's annual security awareness training. In addition, we identified 223 employees who had not completed the required annual security awareness refresher training for 2017. During the audit, we determined the quarterly report by which Department staff were notified of security awareness training status was discontinued. Since that time, the status of employees' security awareness training has not been monitored. In addition, there was a lack of follow-up to ensure training occurred.

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 the information processed through them. Without completing such training, there is a greater risk that users will not properly protect the information and information systems they have access to. State security standards require all state employees to have security awareness refresher training at least annually. In addition to employees, standards require all consultants and contractors to attend an orientation program that introduces information security awareness and informs them of information security policies and procedures.

Recommendation

17. Revise existing procedures to ensure all employees, consultants, and contractors receive security awareness training and maintain an updated list of completed trainings.

Appendix A
Audit Methodology

To gain an understanding of the Department of Taxation (Department), we interviewed Department management and staff. We also interviewed the Department's Information Technology (IT) support staff to gain a broad understanding of the Department's information technology resources and how they are organized, managed, and utilized. In addition, we reviewed generally accepted IT standards and guidelines from the State of Nevada and the National Institute of Standards and Technology (NIST). We also reviewed financial information, budgets, legislative committee minutes, and other information describing the Department's activities. Furthermore, we documented and assessed internal controls over IT systems, users, and data resources.

We assessed all server and telecommunications rooms housing the Department's equipment for physical security including adequate access controls and effective environmental controls. We also evaluated the Department's building access card system to verify that access was being properly monitored.

To determine if security controls over laptops were adequate, we tested a nonstatistical sample of 66 laptops from the Department's 113 laptops. We reviewed security updates on laptops included in the Department's update process on a selected date to verify if they were current with operating system and anti-virus software updates.

We examined the Department's network user population to determine if only current employees had access to the network. In addition, we determined if all Department staff and contractors had conducted their annual security awareness training. Furthermore, we determined if the Department was conducting

background checks on all staff and contractors who had access to sensitive information.

Our selection of application access controls were made based on an assessment of key critical applications. We tested and reviewed the security of the Department's four mission-critical applications to determine if access to sensitive data was authorized and appropriate.

Finally, for our review of data backup and recovery procedures and the Department's IT contingency plan we assessed the existing documentation.

For testing of laptop security controls, we used nonstatistical audit sampling, which was the most appropriate and cost-effective method for concluding on our audit objective. We did not project our results because the sample may not be representative of the population. Based on our professional judgment, review of authoritative sampling guidance, and careful consideration of underlying statistical concepts, we believe that nonstatistical sampling provides sufficient, appropriate audit evidence to support the conclusion in our report.

Our audit work was conducted from November 2017 to June 2018. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Department of Taxation. On September 27, 2018, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B, which begins on page 17.

Contributors to this report included:

Shirlee Eitel-Bingham, CISA
Deputy Legislative Auditor

Sarah R. Gasporra, BBA
Deputy Legislative Auditor

S. Douglas Peterson, CISA, MPA
Information Systems Audit Supervisor

Daniel L. Crossman, CPA
Chief Deputy Legislative Auditor

Appendix B

Response From the Department of Taxation

STATE OF NEVADA
DEPARTMENT OF TAXATION
Web Site: https://tax.nv.gov
1550 College Parkway, Suite 115
Carson City, Nevada 89706-7937
Phone: (775) 684-2000 Fax: (775) 684-2020

RENO OFFICE
4600 Kietzke Lane
Building L, Suite 235
Reno, Nevada 89502
Phone: (775) 687-9999
Fax: (775) 688-1303

BRIAN SANDOVAL
Governor
JAMES DEVOLLD
Chair, Nevada Tax Commission
WILLIAM D. ANDERSON
Executive Director

LAS VEGAS OFFICE
Grant Sawyer Office Building, Suite1300
555 E. Washington Avenue
Las Vegas, Nevada 89101
Phone: (702) 486-2300 Fax: (702) 486-2373

HENDERSON OFFICE
2550 Paseo Verde Parkway, Suite 180
Henderson, Nevada 89074
Phone: (702) 486-2300
Fax: (702) 486-3377

October 5, 2018

Rocky Cooper, Legislative Auditor
Legislative Council Bureau
Legislative Building
401 S. Carson Street
Carson City, NV 89701-4747

Dear Mr. Cooper,

Thank you for the information provided in your audit report of 27 September, 2018. We appreciate the Legislative Council Bureau's professionalism during this audit process and the opportunity to improve the security posture of the Department's IT systems. Please see our response to your recommendations below. We have also attached the "Department of Taxation's Response to Audit Recommendations" indicating our acceptance of the recommendations.

Recommendation 1: Ensure all server and telecommunication rooms have locked doors.

Response: We accept this recommendation

The Department has addressed this recommendation by installing a card-reader lock with restricted access on the server room in the Reno office. Although the Carson City location has locks on the doors, we are researching additional options to further secure the Carson City office telecommunications room.

Recommendation 2: Review existing access and determine a viable method to monitor personnel entering the Carson City telecommunications room.

Response: We accept this recommendation

The Department is researching various options to ensure access monitoring for the Carson City office telecommunications room.

Recommendation 3: Ensure personnel accounts within the card access system are periodically monitored.

Response: We accept this recommendation

The Department has implemented a procedure to review people in the card access system on a bi-weekly basis. Any discrepancies are investigated and resolved.

Recommendation 4: Perform an on-site review and develop a plan to ensure the server and telecommunications rooms are maintaining optimum temperatures in accordance with industry and manufacturers' standards.

Response: We accept this recommendation

The Department will perform an on-site review within 90 days and develop a plan by 1/1/2020.

Recommendation 5: Implement procedures to review building card access within each secured area, delete inactive cards, and disable cards upon termination or transfer.

Response: We accept this recommendation

We have implemented a process for secured area access reports to be submitted to the Department's ISO and Technical Team Lead on a monthly basis.

The Department has implemented a procedure to review people in the card access system on a bi-weekly basis. Any discrepancies are investigated and resolved.

Recommendation 6: Obtain additional training to utilize full capabilities of systems management application to improve laptop computer administration.

Response: We accept this recommendation

The Department's helpdesk staff has completed additional training on the systems management application and are working through the process to ensure the new configuration will function properly. Additionally, we are working closely with EITS on a couple of alternatives to improve the laptop security patching process in the event our systems management application will not be able to achieve the functional level we require.

Recommendation 7: Develop procedures to routinely detect and correct failed laptop computer security update installations.

Response: We accept this recommendation

The Department has implemented a script-based procedure to check the current patch level of laptop systems prior to and after system patching. The Department's helpdesk staff is working through the process to ensure new systems management application configuration settings will function properly. Additionally, we are working closely with EITS on a couple of alternatives to improve the laptop security patching process in the event our systems management application will not be able to achieve the functional level we require.

Recommendation 8: Revise the current help desk process to include disabling and removal of VPN accounts.

Response: We accept this recommendation

The Department will enhance the helpdesk's onboarding/off-boarding workflow process to ensure VPN accounts are disabled and removed as personnel leave the agency.

Recommendation 9: Maintain a current list of all VPN accounts and verify its accuracy quarterly.

Response: We accept this recommendation

The Department will maintain a list of all current VPN accounts and implement a process to verify all active VPN accounts on a quarterly basis.

Recommendation 10: Revise the Department's existing user access review process to include all applications.

Response: We accept this recommendation

We run a quarterly user report against our main user directory access database for the Internal Auditor. We have implemented a process to provide active user reports for our other critical applications to the Internal Auditor at the same time.

We removed all old user accounts for employees no longer with the agency and trued up the applications with the agency's directory access database.

Recommendation 11: Maintain a current list of all user accounts for each application and verify its accuracy at least annually

Response: We accept this recommendation

The Department will develop a process to review existing user accounts' databases for each application on an annual basis.

Recommendation 12: Develop a procedure to ensure routine review and removal of obsolete network user accounts.

Response: We accept this recommendation

We will develop a procedure for the review and removal of obsolete network user accounts.

Recommendation 13: Develop a process to ensure all contractors have required background checks.

Response: We accept this recommendation

The agency is currently working with Agency HR to improve the background check process for contractors and employees alike.

Recommendation 14: Update the Department's existing backup process documentation.

Response: We accept this recommendation

The Department is working to enhance the backup process documentation.

Recommendation 15: Develop recovery process documentation for each system, application, and associated data.

Response: We accept this recommendation

The Department is working to improve the restore process documentation.

Recommendation 16: Update the existing IT contingency plan to include the recovery priority of the Department's mission-critical systems.

Response: We accept this recommendation

The deputy director for IT signed off on the updated IT Contingency Planning Policy.

The Department is currently updating the Business Impact Analysis (BIA) on each of our IT systems using NIST and State Standards. We will use the information gleaned from the BIA process to update our system prioritization and incorporate that data into the updated IT Contingency Plan.

Recommendation 17: Revise existing procedures to ensure all employees, consultants, and contractors receive security awareness training and maintain an updated list of completed trainings.

Response: We accept this recommendation

The Department's existing procedures have been revised to include a quarterly security awareness training report to the ISO. As of 13 August, 2018, we are 97% compliant with annual security awareness training requirements.

Thank you again for the recommendations to improve the Department of Taxation's IT systems security.

Sincerely,

William D. Anderson, Executive Director
Nevada Department of Taxation

Department of Taxation's Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Ensure all server and telecommunications rooms have locked doors	X	
2.	Review existing access and determine a viable method to monitor personnel entering the Carson City telecommunications room	X	
3.	Ensure personnel accounts within the card access system are periodically monitored	X	
4.	Perform an on-site review and develop a plan to ensure the server and telecommunications rooms are maintaining optimum temperatures in accordance with industry and manufacturers' standards	X	
5.	Implement procedures to review building card access within each secured area, delete inactive cards, and disable cards upon termination or transfer	X	
6.	Obtain additional training to utilize full capabilities of the systems management application to improve laptop computer administration	X	
7.	Develop procedures to routinely detect and correct failed laptop computer security update installations	X	
8.	Revise the current help desk process to include disabling and removal of VPN accounts	X	
9.	Maintain a current list of all VPN accounts and verify its accuracy quarterly	X	
10.	Revise the Department's existing user access review process to include all applications	X	
11.	Maintain a current list of all user accounts for each application and verify its accuracy at least annually	X	
12.	Develop a procedure to ensure routine review and removal of obsolete network user accounts	X	
13.	Develop a process to ensure all contractors have required background checks	X	
14.	Update the Department's existing backup process documentation	X	
15.	Develop recovery process documentation for each system, application, and associated data	X	

Department of Taxation's Response to Audit Recommendations (continued)

	Recommendations	Accepted	Rejected
16.	Update the existing IT contingency plan to include the recovery priority of the Department's mission-critical systems	X	
17.	Revise existing procedures to ensure all employees, consultants, and contractors receive security awareness training and maintain an updated list of completed trainings	X	
	TOTALS	17	