LA14-23

STATE OF NEVADA

Performance Audit

Department of Transportation
Information Security

2014

Legislative Auditor
Carson City, Nevada

Audit Highlights

Highlights of performance audit report on the Department of Transportation Information Security issued on December 2, 2014. Legislative Auditor report # LA14-23.

Background

The mission of the Nevada Department of Transportation is to provide a better transportation system for Nevada through unified and dedicated efforts. The Department has numerous offices located throughout the State. These locations include administrative offices, maintenance stations, and construction offices. The primary administrative locations include the Department headquarters located in Carson City, and the three district offices located in Las Vegas (District 1), Reno/Sparks (District 2), and Elko (District 3).

For fiscal year 2014 the Department was authorized 1,782 full-time employees statewide. In addition, the Department had expenditures of over $616 million for fiscal year 2014.

Purpose of Audit

The purpose of this audit was to determine 1) if the Department's information security controls were adequate to protect the confidentiality, integrity, and availability of sensitive information and information systems; and 2) if the controls on the use of procurement cards were adequate to reasonably mitigate the risks of fraudulent use.

The primary focus of our audit work included the systems and practices in place from January through September of 2014. However, our procurement card audit work included a review of selected procurement card transactions from prior to June of 2013.

Audit Recommendations

This audit report contains eight recommendations to improve the security of the Department's information systems and its procurement card procedures.

The Department of Transportation accepted the eight recommendations.

Recommendation Status

The Department of Transportation's 60-day plan for corrective action is due on March 2, 2015. In addition, the six-month report on the status of audit recommendations is due on September 2, 2015.

Information Security

Department of Transportation

Summary

Weaknesses exist in managing network computer users. These weaknesses include not disabling former employee and contractor computer accounts when these persons leave Department employment. In addition, the Department did not conduct criminal background investigations on all staff occupying sensitive positions with access to confidential information or systems.

The Department needs to provide better protection for important computer and radio hardware. For example, some server rooms lacked adequate temperature monitoring and alerting capabilities. In addition, some telecommunications and radio equipment is not secured in locked rooms. As a result, sensitive equipment is at risk of being damaged or stolen.

Weaknesses in Department procurement card controls enabled a stock room employee to commit fraudulent procurement card purchases over a four year period. Although procurement card procedures have been revised to lessen the risk of similar fraud, the revisions have not yet been formalized in the Department's corresponding Transportation Policy. Furthermore, the proposed procedure revisions are not being followed by all purchase card holders throughout the Department.

Key Findings

Former employee and contractor computer accounts were not disabled when these persons left the Department. We identified 34 former staff whose network credentials (login identification and passwords) had not been disabled. These included 28 former Nevada Department of Transportation (NDOT) employee and 6 NDOT contractor computer accounts. Sixteen of these had left the Department over 1 year ago. Untimely disabling of former employees' or contractors' computer accounts increases the risk someone could gain unauthorized access to the NDOT network and the information systems therein. (page 4)

The Department did not conduct criminal background investigations on staff occupying sensitive positions. State security standards require criminal background investigations be conducted on all persons in sensitive positions. Those standards define "sensitive" positions as those employees with access to confidential information or important information systems. We identified at least 66 positions, primarily in the Information Technology Division, that should be defined as sensitive. Conducting these fingerprint-based criminal history background investigations reduces the likelihood that a person with an unsuitable criminal background will be hired into a position where they are granted access to the state's confidential information or important information systems. (page 4)

Two server rooms lacked adequate temperature monitoring and alerting systems. One was in the Department's primary server room located in Carson City. State security standards require computer networking equipment be operated within a temperature controlled environment to reduce the risk of equipment failure due to overheating. In addition, temperature monitoring and alerting systems which were operational in other server rooms around the State were not configured to alert staff of overheating events after normal business hours. Also, we identified two rooms containing telecommunications and radio equipment that were not locked. Security standards indicate access to such equipment should be controlled by locked doors. (page 7)

Weak controls over procurement cards allowed fraud to occur. For example, purchases did not require supervisory review and often the purchaser was also the person receiving the merchandise. As a result, over a 4-year period a stockroom employee made over $250,000 in fraudulent purchases. The Department has proposed changes to the procurement card procedures. However these changes have not been formally incorporated into the Department's policy 11 months after the fraud occurred. (page 9)

STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747
~~Fax No.: (775) 684-6600~~

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

LEGISLATIVE COMMISSION (775) 684-6800
MARILYN K. KIRKPATRICK, *Assemblywoman, Chairman*
Rick Combs, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
DEBBIE SMITH, *Senator, Chairman*
Mark Krmpotic, *Fiscal Analyst*
Cindy Jones, *Fiscal Analyst*

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830
PAUL V. TOWNSEND, *Legislative Auditor* (775) 684-6815
DONALD O. WILLIAMS, *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 Transportation 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 eight recommendations to improve information security and procurement card usage. 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,

Paul V. Townsend

Paul V. Townsend, CPA
Legislative Auditor

November 13, 2014
Carson City, Nevada

Department of Transportation Information Security Table of Contents

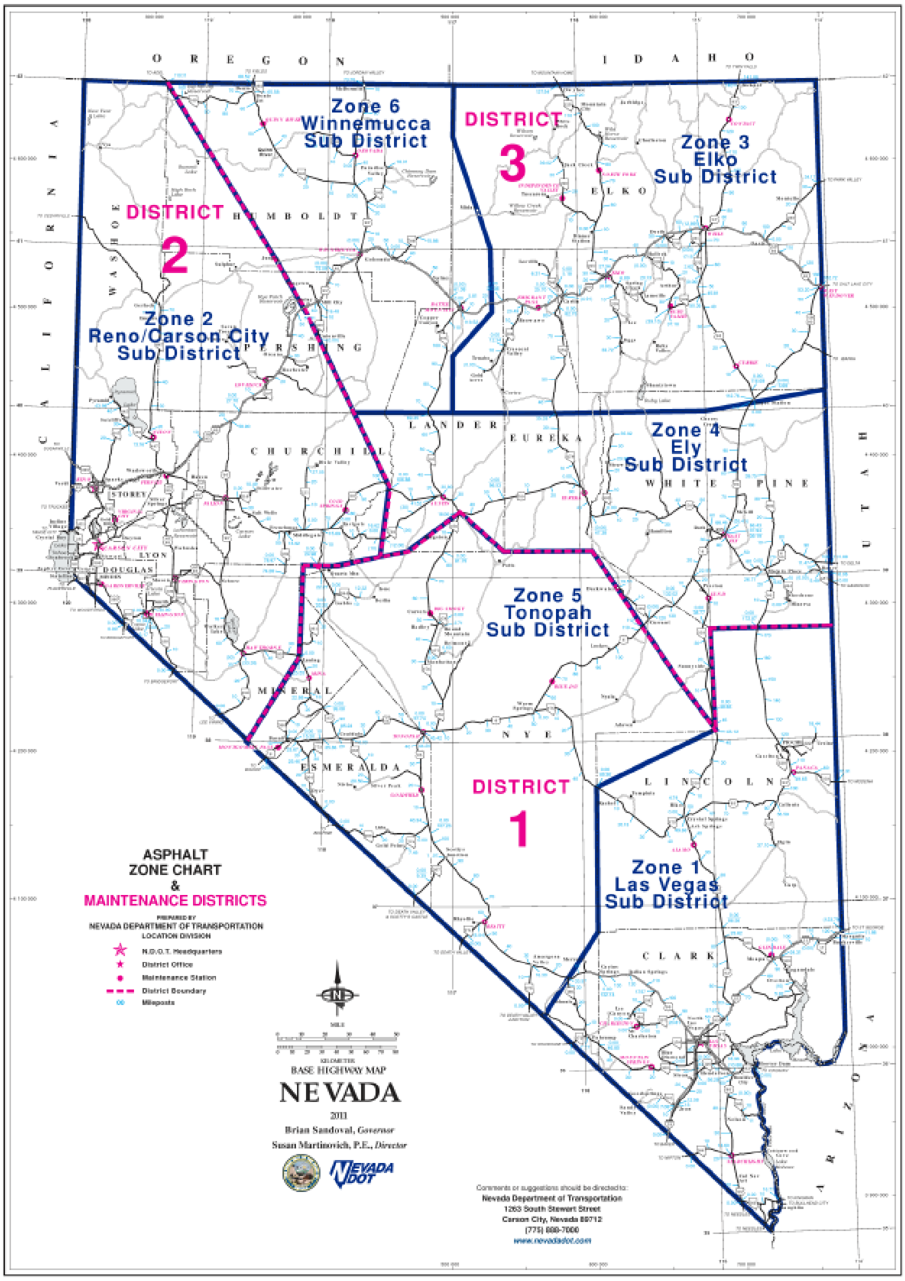
Appendices

Introduction

Background

The mission of the Nevada Department of Transportation (NDOT) is to provide a better transportation system for Nevada through unified and dedicated efforts. The Department has numerous offices located throughout the State. These locations include administrative offices, maintenance stations, and construction offices. The primary administrative locations include the Department headquarters located in Carson City, and the three district offices located in Las Vegas (District 1), Reno/Sparks (District 2), and Elko (District 3). Exhibit 1 shows the location of the districts.

Exhibit 1



Source: Nevada Department of Transportation.

For fiscal year 2014 the Department was authorized 1,782 full-time employees statewide. In addition, the Department had actual expenditures of over $616 million for fiscal year 2014.

Scope and Objectives

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.

The primary focus of our audit work included the systems and practices in place from January through September of 2014. However, our procurement card audit work included a review of selected procurement card transactions from prior to June of 2013.

Our audit objectives included:

- Determining if the Department of Transportation has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems; and

- Determining if controls over the use of procurement cards within the Department were adequate to minimize the risks of fraud or abuse.

Weaknesses Exist in Managing Network Users

Weaknesses exist in managing network computer users. These weaknesses include not disabling former employee and contractor computer accounts when these persons leave Department employment. In addition, the Department did not conduct criminal background investigations on all staff occupying sensitive positions with access to confidential information or systems.

Former Staff and Contractors Had Current Network Access

Former employee and contractor computer accounts were not disabled when these persons left the Department. We identified 34 former staff whose network credentials (login identification and passwords) had not been disabled. These included 28 former NDOT employee and 6 NDOT contractor computer accounts. Sixteen of these had left the Department over 1 year ago.

Department policy requires NDOT division managers or district engineers to notify the Information Technology Division of the need to terminate access of an employee or contractor prior to, or immediately upon, that person's termination of employment. Untimely disabling of former employees' or contractors' computer accounts increases the risk someone could gain unauthorized access to the NDOT network and the information systems therein.

Information technology (IT) staff indicated there were multiple reasons why this occurred. These included processing errors by IT staff, inaccurate reporting of terminated employees by the Human Resources Division, and the lack of notification when contractors left Department service.

Background Investigations of Staff in Sensitive Positions Need Greater Emphasis

The Department did not conduct criminal background investigations on staff occupying sensitive positions. Specifically, NDOT has only conducted one criminal background investigation during the past 4 years despite having an average annual turnover rate of over 11%, thus hiring approximately 200 replacements annually.

State security standards require criminal background investigations be conducted on all persons in sensitive positions. Those standards define “sensitive” positions as those employees with access to privileged information or important information systems. During our audit, we identified at least 66 positions, primarily in the Information Technology Division, that should be defined as sensitive according to the state security standard criteria. However, there may be more sensitive positions in other divisions. Furthermore, other security assessments of NDOT in January 2012 and in November 2013 indicated NDOT was not in compliance with the state security standard related to conducting criminal background investigations on staff in sensitive positions.

The 2012 security assessment identified 67 sensitive positions in the Department requiring criminal background checks. However, the Department’s policy for conducting criminal background checks only identifies 16 of 1,782 employees who require pre-employment criminal background investigations. As an example, the Department has an Over Dimensional Vehicle (ODV) permit call center that accepts credit card payment information over the phone from truck drivers needing ODV permits. None of the NDOT staff processing this credit card information have had criminal background investigations. In addition, the Department’s Information Technology Division has 60 staff with access to confidential information and systems whose positions should also require criminal background investigations. Conducting these fingerprint-based criminal history background investigations reduces the likelihood that a person with an unsuitable criminal background will be hired into a position where they are granted access to the state’s confidential information or important information systems.

Recommendations

1. Revise the current process used by help desk staff to disable terminating users’ network accounts to ensure that all

departing employee or contractor computer accounts are disabled timely.

2. Implement a periodic backup procedure to identify and disable former staff computer accounts that have not been disabled when they left employment.
3. Identify sensitive positions Department-wide needing criminal background investigations.
4. Conduct criminal background investigations on all positions identified as sensitive as people are hired or promoted into those positions.

Computer and Radio Equipment Rooms Need Better Protection

The Department needs to provide better protection for important computer and radio hardware. For example, some server rooms lacked adequate temperature monitoring and alerting capabilities. In addition, some telecommunications and radio equipment is not secured in locked rooms. As a result, sensitive equipment is at risk of being damaged or stolen.

Server Rooms Lacked Adequate Temperature Monitoring and Alerting Capabilities

Two server rooms lacked adequate temperature monitoring and alerting systems. One of these was the Department's primary server room located in the Carson City headquarters building. Department IT staff initially indicated they believed room temperature was monitored by the Department's Buildings and Grounds (B&G) staff. However, when we inquired with B&G staff they indicated they had no temperature monitoring equipment installed that could provide overheating alerts for the computer equipment. We also found the temperature sensor in the Ely server room was not operational. State security standards require computer networking equipment be operated within a temperature controlled environment so as to reduce the risk of equipment failure due to overheating.

In addition, the temperature monitoring and alerting systems which were operational in other server rooms around the State were not configured to alert staff of overheating events after normal business hours. The alerts were configured to go to staff email accounts which might not be monitored after normal business hours. Subsequent to our inquiry, the IT staff reconfigured these systems to send the overheating alerts to staff in one of the Department's 24-hour road operations centers. Staff at the centers will then phone the on-call IT staff member to respond to the temperature alert warnings.

The primary server room in the Carson City headquarters contains computer equipment that is critical to many of the Department's functions. The server room temperature must be monitored to detect equipment cooling problems that may arise when HVAC cooling equipment fails such as during power outages or brownouts on excessively hot days. Server room overheating problems can be resolved by installing temporary cooling devices such as fans or by shutting down the computer equipment. Both of these responses require timely notification of IT staff that there is a potential equipment overheating event. Failure to take timely action to reduce excess heat, or to power down computer equipment can lead to failure of expensive and critical network and radio equipment.

Telecommunications and Radio Equipment Rooms Need Locked Doors

Some telecommunications and radio equipment was not secured in locked rooms. We identified two rooms containing telecommunications and two-way radio equipment that were not locked. The first, a rural highway maintenance station lacked an adequate locking mechanism on the door to the room containing the location's telecommunications cabinet. The other involved another maintenance facility where the telecommunications and radio equipment room was normally left unlocked. State security standards indicate that access to such equipment should be controlled by locked doors in order to prevent theft or accidental damage to equipment.

Recommendations

5. Ensure temperature sensing hardware is installed and operational in key server and telecommunications rooms to provide alerts to staff of temperature conditions that exceed equipment operation ratings.
6. Revise the after-hours notification system to ensure key IT staff are immediately notified when server room temperatures exceed recommended alert levels.
7. Ensure all telecommunications and radio rooms have locked doors.

Revisions to Procurement Card Procedures Have Not Yet Been Fully Implemented

Weaknesses in Department procurement card controls enabled a stock room employee to commit fraudulent procurement card purchases over a 4-year period. Although procurement card procedures have been revised to lessen the risk of similar fraud, the revisions have not yet been formalized in the Department's corresponding Transportation Policy. Furthermore, the proposed procedure revisions are not followed by all purchase card holders throughout the Department.

Weak Controls Over Procurement Card Usage Allowed Fraud to Occur

A Department stockroom employee was able to commit procurement card fraud over a 4-year period, resulting in over $250,000 in fraudulent purchases. This fraud was identified by the Department in October of 2013 during the employee's absence from work.

During our audit, we examined the procurement card controls to determine if we could identify internal control weaknesses that contributed to the employee's ability to perpetuate the fraud. We found that the procurement card procedures during the period of the fraud had several weaknesses. These included:

- Procurement card purchases did not require supervisory review and approval which would have required the purchaser to explain the purchases.

- The original purchase request and receipt documents were not required as supporting documentation when the purchase paperwork was submitted for payment processing. This allowed the employee to alter documents using photocopied requests and receipts, thus masking the actual items purchased.

- There were no routine monthly audits of purchases which might have deterred fraudulent intentions.
- Often times the purchaser was also the person receiving the merchandise which facilitated the concealment of the fraudulently purchased items.

Procurement Card Procedures Are Being Revised but the Revisions Have Not Yet Been Fully Implemented

Subsequent to the fraud's discovery, the Department's Equipment Division, which manages procurement card procedures within the Department proposed several changes to the procurement card procedures. This should reduce the risk of similar fraud occurring. These changes include the following:

- Supervisors will now review and approve all procurement card holders' purchases before the paperwork is submitted for payment.
- The supporting payment documentation will now require original purchase receipts. Any payment requests without original purchase receipts will be investigated.
- Five percent of each month's purchases will be audited by Equipment Division auditors.
- The supporting payment documentation will now include signature evidence that the individual purchasing the item (the procurement card holder), and the person receiving the item, are two different employees.

Federal standards indicate that identified control weaknesses, such as those that allowed this fraud to occur, should be corrected timely. Also, NRS 353A.020 requires a plan to safeguard agency assets. However, according to staff, as of October 2014, the changes to the procurement card procedures have not been formally incorporated into the Department's procurement card policy. Furthermore, the proposed procedure revisions are not being followed by all procurement card holders throughout the Department 11 months after the fraud was discovered. For example, we tested 12 transactions with at least 1 from each of the 3 districts to determine if the person who made a purchase was different from the person who received the item. We found six transactions, at least one from each of the districts, where the same person both signed for and received merchandise. To ensure these changes are made, the Equipment Division's procurement card administrator will need to monitor compliance with the proposed changes throughout the Department.

Recommendation

8. Implement the proposed revisions to the Department's procurement card policy and ensure these changes are being followed by all purchase card holders throughout the Department.

Appendix A

Audit Methodology

To gain an understanding of the Department of Transportation, we interviewed Department management and staff. We interviewed the Department's information technology staff to gain a broad understanding of the Department's information technology resources and how they are organized, managed, and utilized.

To determine if controls over desktop computer security were adequate, we tested a judgmental sample of 174 of the Department's desktop computers. The sample was based on the location and was selected from 15 different Department locations throughout the State to ensure they had current virus protection as well as the latest operating system security updates.

Our sample size and methodology provide a reasonable basis for estimating desktop computer security controls. However, because we did not conduct a statistical sample of the entire population of desktop computers, the results of our testing cannot be projected to the entire population.

We examined each of the 15 locations' telecommunications rooms to ensure the equipment contained in them was adequately secured. We also examined the Department's network user accounts to determine if only current employees had access to the network. To assess the security of the Department's network servers we tested to ensure they were configured to enforce state password standards for all accounts. In addition, we reviewed the environmental controls within key server rooms to ensure these controls were adequate to protect the computer hardware in them from overheating.

We reviewed key database software to ensure it had the latest security updates installed so as to adequately protect the sensitive and valuable data stored within these databases. Finally, we reviewed the controls over the use of procurement cards within the Department in order to ensure these controls were adequate to minimize the risks of fraud or abuse.

Our audit work was conducted from April to October of 2014. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Department of Transportation. On November 3, 2014, 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 14.

Contributors to this report included:

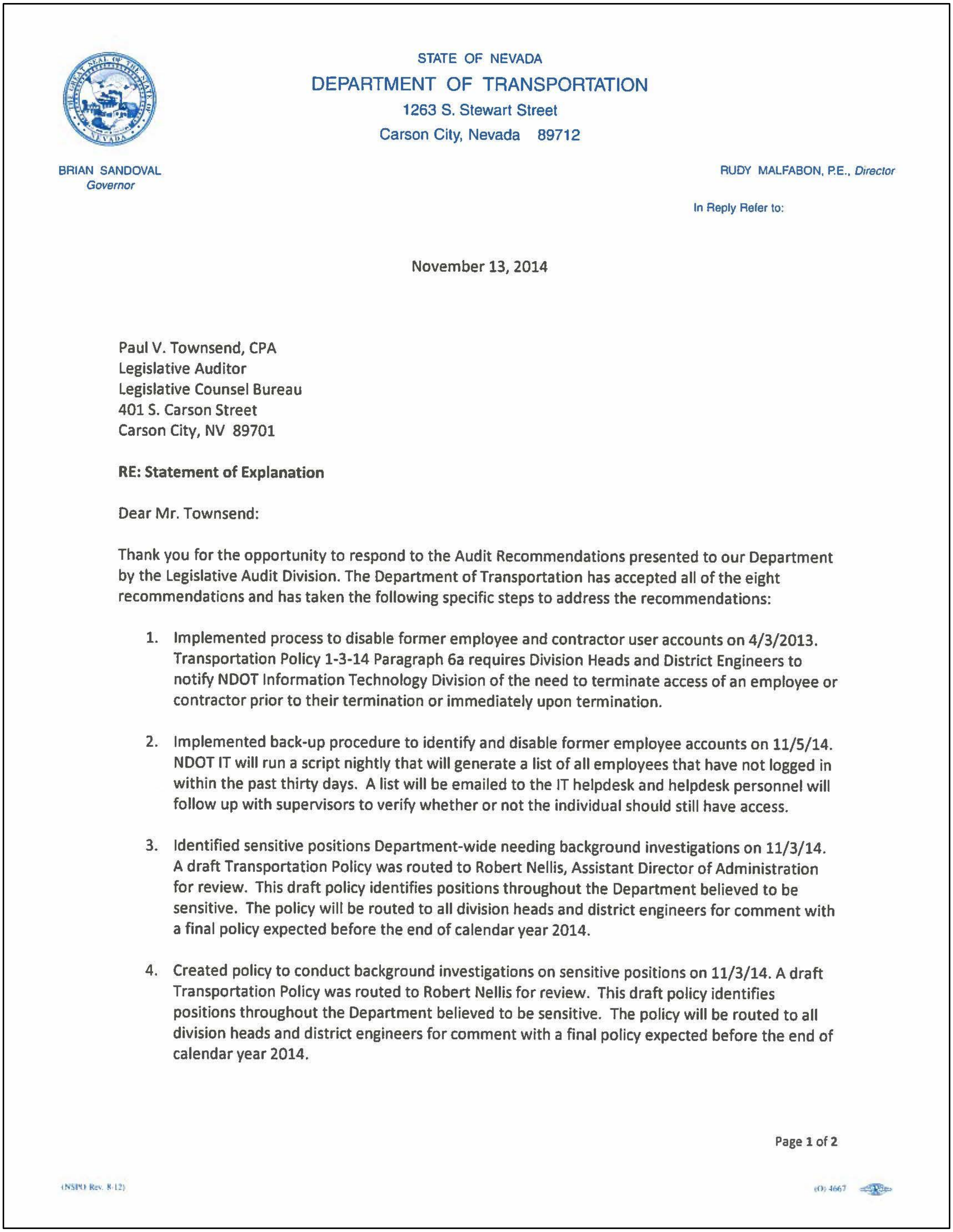
Jeff Rauh, CISA, CIA, MBA
Deputy Legislative Auditor

Tom Tittle, CPA, CIA, CFE
Deputy Legislative Auditor

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

Appendix B

Response From the Department of Transportation



STATE OF NEVADA
DEPARTMENT OF TRANSPORTATION
1263 S. Stewart Street
Carson City, Nevada 89712

BRIAN SANDOVAL
Governor

RUDY MALFABON, P.E., *Director*

In Reply Refer to:

November 13, 2014

Paul V. Townsend, CPA
Legislative Auditor
Legislative Counsel Bureau
401 S. Carson Street
Carson City, NV 89701

RE: Statement of Explanation

Dear Mr. Townsend:

Thank you for the opportunity to respond to the Audit Recommendations presented to our Department by the Legislative Audit Division. The Department of Transportation has accepted all of the eight recommendations and has taken the following specific steps to address the recommendations:

1. Implemented process to disable former employee and contractor user accounts on 4/3/2013. Transportation Policy 1-3-14 Paragraph 6a requires Division Heads and District Engineers to notify NDOT Information Technology Division of the need to terminate access of an employee or contractor prior to their termination or immediately upon termination.

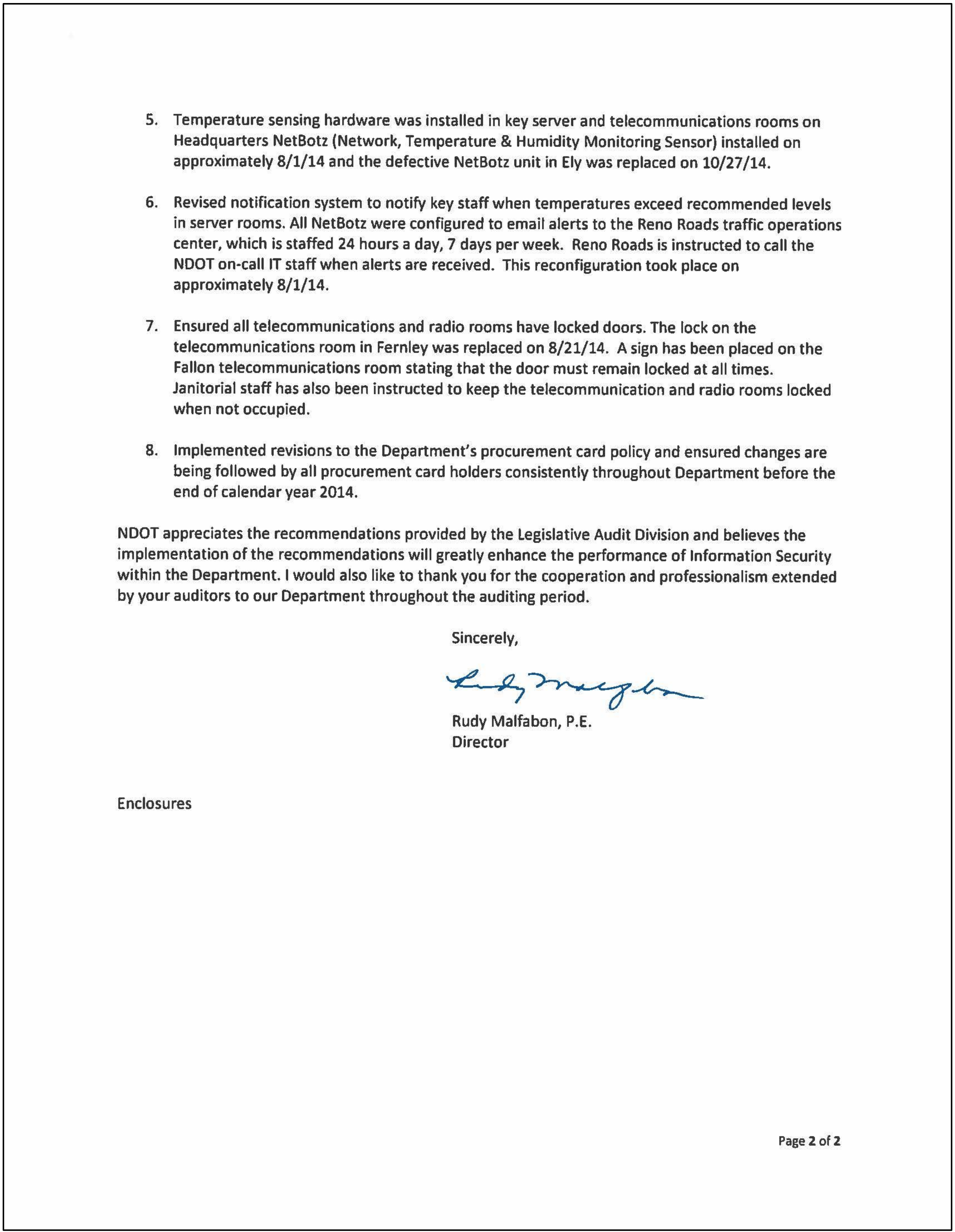
2. Implemented back-up procedure to identify and disable former employee accounts on 11/5/14. NDOT IT will run a script nightly that will generate a list of all employees that have not logged in within the past thirty days. A list will be emailed to the IT helpdesk and helpdesk personnel will follow up with supervisors to verify whether or not the individual should still have access.

3. Identified sensitive positions Department-wide needing background investigations on 11/3/14. A draft Transportation Policy was routed to Robert Nellis, Assistant Director of Administration for review. This draft policy identifies positions throughout the Department believed to be sensitive. The policy will be routed to all division heads and district engineers for comment with a final policy expected before the end of calendar year 2014.

4. Created policy to conduct background investigations on sensitive positions on 11/3/14. A draft Transportation Policy was routed to Robert Nellis for review. This draft policy identifies positions throughout the Department believed to be sensitive. The policy will be routed to all division heads and district engineers for comment with a final policy expected before the end of calendar year 2014.

Page **1** of **2**

(NSPO Rev. 8-12) (O) 4667



5. Temperature sensing hardware was installed in key server and telecommunications rooms on Headquarters NetBotz (Network, Temperature & Humidity Monitoring Sensor) installed on approximately 8/1/14 and the defective NetBotz unit in Ely was replaced on 10/27/14.

6. Revised notification system to notify key staff when temperatures exceed recommended levels in server rooms. All NetBotz were configured to email alerts to the Reno Roads traffic operations center, which is staffed 24 hours a day, 7 days per week. Reno Roads is instructed to call the NDOT on-call IT staff when alerts are received. This reconfiguration took place on approximately 8/1/14.

7. Ensured all telecommunications and radio rooms have locked doors. The lock on the telecommunications room in Fernley was replaced on 8/21/14. A sign has been placed on the Fallon telecommunications room stating that the door must remain locked at all times. Janitorial staff has also been instructed to keep the telecommunication and radio rooms locked when not occupied.

8. Implemented revisions to the Department's procurement card policy and ensured changes are being followed by all procurement card holders consistently throughout Department before the end of calendar year 2014.

NDOT appreciates the recommendations provided by the Legislative Audit Division and believes the implementation of the recommendations will greatly enhance the performance of Information Security within the Department. I would also like to thank you for the cooperation and professionalism extended by your auditors to our Department throughout the auditing period.

Sincerely,

Rudy Malfabon, P.E.
Director

Enclosures

Department of Transportation's Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Revise the current process used by help desk staff to disable terminating users' network accounts to ensure that all departing employee or contractor computer accounts are disabled timely	X	
2.	Implement a periodic backup procedure to identify and disable former staff computer accounts that have not been disabled when they left employment	X	
3.	Identify sensitive positions Department-wide needing criminal background investigations	X	
4.	Conduct criminal background investigations on all positions identified as sensitive as people are hired or promoted into those positions	X	
5.	Ensure temperature sensing hardware is installed and operational in key server and telecommunications rooms to provide alerts to staff of temperature conditions that exceed equipment operation ratings.	X	
6.	Revise the after-hours notification system to ensure key IT staff are immediately notified when server room temperatures exceed recommended alert levels.	X	
7.	Ensure all telecommunications and radio rooms have locked doors	X	
8.	Implement the proposed revisions to the Department's procurement card policy and ensure these changes are being followed by all purchase card holders throughout the Department	X	
	TOTALS	8	