STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU

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

LORNE J. MALKIEWICH, *Director*
(775) 684-6800

LEGISLATIVE COMMISSION (775) 684-6800
RANDOLPH J. TOWNSEND, *Senator, Chairman*
Lorne J. Malkiewich, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
BERNICE MATHEWS, *Senator, Co-Chair*
STEVEN HORSFORD, *Senator, Co-Chair*
Gary L. Ghiggeri, *Fiscal Analyst*
Mark W. Stevens, *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

We have completed an audit of the Department of Employment, Training and Rehabilitation, Information Technology Security. This audit is part of 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. The results of our audit, including findings, conclusions, recommendations, and the Department's response, are presented in this report.

We wish to express our appreciation to the management and staff of the Department of Employment, Training and Rehabilitation for their assistance during the audit.

Respectfully presented,

Paul V. Townsend

Paul V. Townsend, CPA
Legislative Auditor

May 19, 2009
Carson City, Nevada

STATE OF NEVADA
DEPARTMENT OF EMPLOYMENT, TRAINING AND REHABILITATION
INFORMATION TECHNOLOGY SECURITY

AUDIT REPORT

Table of Contents

Page

STATE OF NEVADA
DEPARTMENT OF EMPLOYMENT, TRAINING AND REHABILITATION
INFORMATION TECHNOLOGY SECURITY

AUDIT REPORT

Table of Contents
(continued)

Page

Appendices

EXECUTIVE SUMMARY

DEPARTMENT OF EMPLOYMENT, TRAINING AND REHABILITATION
INFORMATION TECHNOLOGY SECURITY

Background

The mission of the Department of Employment, Training and Rehabilitation (DETR) is to provide Nevada's businesses with access to a qualified workforce and encourage equal employment opportunities. The Department employs approximately 800 staff in its 21 office locations statewide with primary locations in Carson City, Reno, Sparks, Las Vegas, Henderson, and Elko.

The Department consists of the Director's Office and five divisions including:

- Employment Security Division
- Rehabilitation Division
- Nevada Equal Rights Commission
- Research and Analysis Bureau
- Information Development and Processing Division

The Department, especially its Employment Security Division, relies heavily on information technology and the Internet to deliver services to Nevada residents and employers. The Department stores and processes large amounts of confidential information including names and social security numbers of people working throughout the state.

Purpose

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 DETR through September 30, 2008.

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: Information technology (IT) staff having unrestricted access to the State's Unemployment Insurance Trust Fund application and database; insufficient security of sensitive information downloaded onto agency laptop computers; and needing more timely removal of mainframe access of former employees. Security of magnetic tapes containing sensitive information also needs improvement.

In addition, routine network maintenance could be improved. For example, virus definitions were not current, the firewall's management needs greater attention, server rooms need better physical security, and wireless laptop security configurations should be strengthened. Finally, more effort needs to be expended to properly screen and manage network users. We noted that the Department's information technology staff either fixed or reduced the risks associated with many of the conditions we identified during the audit.

Principal Findings

- DETR's Employment Security Division had access control weaknesses in its Unemployment Insurance (UI) system. Forty-seven information technology staff had either unrestricted or inappropriate user rights to the UI program and its corresponding database. This UI program is used to process unemployment claims and distribute unemployment compensation funds from the state's Unemployment Insurance Trust Fund. Although Department officials have the responsibility to determine who has access, only those users with a business need should be granted authority. (page 9)

- Thirty-four former DETR employees retained current access to the mainframe computer used to process the unemployment insurance transactions. These employees' access remained enabled more than 100 days after they had left DETR employment. State IT 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. (page 10)

- The Department had 16 laptop computers used by DETR field auditors that contained unencrypted records from employer payroll files. State IT security standards require such confidential information be encrypted to prevent unauthorized disclosure if the laptop is lost or stolen. (page 11)

- Computer tapes containing confidential new hire data were not encrypted while being sent from employers and returned from DETR through the U.S. Postal System. Staff indicated these tapes are not erased after processing. State law requires agencies to implement reasonable security measures to protect the confidential information they collect. (page 11)

- Twenty-seven former employees, partners, and contractors retained access to DETR's computer network after they had left the service of the Department. State IT 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. (page 12)

- The Department does not conduct routine background investigations on staff with access to IT systems or sensitive data. Background investigations are required by state information technology standards to ensure that unsuitable individuals do not gain access to confidential information or sensitive systems. (page 13)

- Sixteen of 144 computers sampled did not have current antivirus protection. The virus definition files on these computers ranged in age from 25 to 421 days old. State IT security standards require virus definition files be kept current to ensure that threats from the Internet will not corrupt state computing resources. (page 14)

- DETR's internal firewall could be improved in both configuration and management. Compliance with best practices such as those issued by the Center for Internet Security will facilitate routine maintenance and administration of the firewall. (page 14)

- We found 16 of 32 laptops sampled did not have wireless configurations recommended by industry best practices. In addition, none of the laptop users indicated they had received security awareness training related to the risks of using wireless networking. Without secure configuration or risk awareness training, the likelihood of sensitive laptop data being accessed by unauthorized persons is increased. (page 15)

- Four application developers had direct update access to production data on the Rehabilitation Division's primary application. Access to production data should be restricted to properly segregate incompatible functions. By allowing application developers update access to production data, the risks of accidental or intentional corruption of the corresponding data is increased. (page 16)

- Network servers at 4 of the 15 locations we examined did not have adequate physical security. These servers were not properly secured in locked rooms. State IT security standards require access to these servers be restricted to prevent accidental or intentional damage. (page 16)

- The Department's network group policy settings allowed six unsuccessful log-in attempts before a network account was locked rather than the state standard of three. Locking an account after several unsuccessful login attempts prevents password guessing by unauthorized persons. Password controls represent fundamental security controls that prevent unauthorized access to computer networks. (page 17)

Recommendations

This audit report contains 17 recommendations to improve the information technology security at the Department of Employment, Training and Rehabilitation. These recommendations address application and access controls over the Employment Security Division's Unemployment Insurance System, data encryption, and managing user accounts. In addition, these recommendations address controls over laptop and server computers as well as wireless networks. (page 27)

Agency Response

The Department, in response to the audit report, accepted the 17 recommendations. (page 21)

Introduction

Background

The mission of the Department of Employment, Training and Rehabilitation (DETR) is to provide Nevada's businesses with access to a qualified workforce and encourage equal employment opportunities. The Department consists of the Director's Office and five divisions that offer assistance in job training and placement, vocational rehabilitation, workplace discrimination, and in collecting and analyzing workforce and economic data. The five divisions include:

- **Employment Security Division**: The mission of the Employment Security Division is to provide a statewide labor exchange, conduct programs that promptly pay unemployment benefits, improve the employment stability of those collecting unemployment insurance, and administer an effective unemployment tax system.
- **Rehabilitation Division**: The Rehabilitation Division provides options and choices for individuals with disabilities to work and live independently.
- **Nevada Equal Rights Commission**: The mission of the Nevada Equal Rights Commission is to foster the rights of all persons to seek, obtain, and maintain employment and access services in places of public accommodation without discrimination.
- **Research and Analysis Bureau**: The Research and Analysis Bureau (R&A) provides information related to Nevada's workforce and economic conditions. R&A serves as Nevada's primary provider of workforce information.
- **Information Development and Processing Division**: The Information Development and Processing Division provides data processing and information technology support services to DETR and its customers.

In fiscal year 2008, total unemployment insurance payments processed exceeded $400 million. In addition, Department expenditures were $113.4 million. In all, the Department has over 800 employees staffing 21 office locations statewide. Primary locations include Carson City, Reno, Sparks, Las Vegas, Henderson, and Elko. The Department, especially its Employment Security Division, relies heavily on information technology and the Internet to deliver services to Nevada residents and employers. The Department stores and processes large amounts of confidential information including names and social security numbers of people working throughout the State.

Scope and Objective

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 218.737 to 218.893. 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.

This audit included a review of information technology controls at the Department of Employment, Training and Rehabilitation through September 30, 2008. The objective of our audit was to determine if the Department's information technology security controls were adequate to protect the confidentiality, integrity, and availability of its information and information systems.

Findings and Recommendations

Weaknesses existed in controls designed to protect the confidentiality, integrity, and availability of the Department's sensitive information and information systems. These weaknesses included: Information technology (IT) staff having unrestricted access to the state's Unemployment Insurance Trust Fund application and database; insufficient security of sensitive information downloaded onto agency laptop computers; and needing more timely removal of mainframe access of former employees. Security of magnetic tapes containing sensitive information also needs improvement.

In addition, routine network maintenance could be improved. For example, virus definitions were not current, the firewall's management needs greater attention, server rooms need better physical security, and wireless laptop security configurations should be strengthened. Finally, more effort needs to be expended to properly screen and manage network users. We noted that the Department's information technology staff either fixed or reduced the risks associated with many of the conditions we identified during the audit.

Staff Had Inappropriate Access to the Unemployment Insurance System

DETR did not adequately restrict access of numerous information technology (IT) personnel to the Unemployment Insurance system. In addition, the Department did not have an effective procedure for removing former employees' access to the mainframe.

A basic principle for the security of computer systems and data is the concept of least privilege, which means that users are granted only those access rights and permissions they need to perform their official duties. Organizations establish access rights and permissions to restrict legitimate users' access to only those programs and files that they need to do their work. Assignment of these rights and permissions must be carefully considered to avoid giving users unnecessary access to sensitive data and transactions.

Employees Had Unrestricted Transaction and Data Access

DETR's Employment Security Division had access control weaknesses in its Unemployment Insurance (UI) system. Forty-seven IT staff had either unrestricted or inappropriate user rights to the Unemployment Insurance program and its corresponding database. Neither the mainframe's security controls nor the General Unemployment Insurance Development Effort (GUIDE) application controls restricted these employees' access. These employees could initiate and execute transactions to file false unemployment insurance benefit claims or alter mainframe GUIDE Adaptable Data Base System (ADABAS) data without detection. Although Department officials have the responsibility to determine who has access, only those users with a business need should be granted authority.

In addition, we could not identify controls to compensate for this condition such as supervisory review of staff data changes or of employee transaction log files. Furthermore, Department officials indicated they are considering installing an ADABAS security utility that would restrict access to data. However, the utility has not yet been installed. These controls could identify or prevent unauthorized transactions made by staff. Agency management indicated this situation has existed for several years and was originally intended to facilitate data and program maintenance by IT staff. When brought to their attention, management said they had removed some user accounts with future changes planned to improve security.

The UI system consists of GUIDE application software and an ADABAS database. This UI system is used to process unemployment claims and distribute unemployment compensation funds from the state's Unemployment Insurance Trust Fund. According to U.S. Treasury Department information, the balance in this fund was about $680 million as of October 31, 2008.

State information technology security standards require that employees be given the minimum set of privileges required to perform their job functions. To prevent abuse of this system it is critical that IT staff have their user rights properly restricted and transaction capabilities properly segregated.

Removal of Mainframe User Accounts Needs Greater Attention

We identified 34 former DETR employees who had either left state employment or had transferred to another state agency that were listed with current mainframe access. These employees' access remained enabled more than 100 days after they had left DETR employment. In addition, we identified over 200 former employee accounts that had not been accessed in over 100 days that, although disabled, should be removed to make the listing more manageable.

State information technology security standards require the prompt removal of users who are no longer in the Department's service. If former employees' computer access is not promptly terminated when they depart, it could result in them gaining unauthorized access to the state's network and confidential data the State collects from the public. DETR indicated its current employee departure notification procedure needs improvement to ensure more timely notification and subsequent removal of these former employee accounts.

Recommendations

1. Implement GUIDE application controls or mainframe security controls to properly restrict transaction capabilities.
2. Implement available ADABAS and mainframe security utilities to reduce risks of unrestricted database access.
3. Develop automated system auditing and corresponding logging procedures to reduce the risk that employees will gain unauthorized access. Ensure these logs are systematically reviewed for unauthorized or suspicious transactions.
4. Revise current procedures for disabling terminated employees' mainframe access to ensure these accounts are disabled timely.

Sensitive Information Was Not Always Protected

DETR did not always provide adequate protection to data stored and transported on Department laptops. In addition, the Department did not adequately protect tapes containing confidential personal information that were returned to employers through the

U.S. Postal System. Unauthorized access to such data can lead to identity theft or other privacy related issues.

Laptops Contained Unencrypted Confidential Information

During our review of agency controls, we noted that staff used laptop computers containing unencrypted personal identifying information. This data sometimes included employees' names and social security numbers. Subsequent inquiries indentified 16 laptops had unencrypted data.

Audit staff in the Employment Security Division's Contributions Section use laptop computers to periodically store and transport employment data needed for employer unemployment insurance rate audits. The field auditors download employers' employment data from where it is stored on the mainframe computer onto their laptops during field audits.

When confidential data on laptops is not encrypted the risk is increased that a lost or stolen laptop will also result in the unintentional release of confidential information. Release of this information, which includes individual identity information that can be used in identity theft, could cause loss of public trust. In addition, since state law requires each person whose information is released be contacted, considerable time and resources would be expended.

State information technology security standards require that confidential data be controlled by the use of encryption software or other evolving security methods. Encrypting the data on these laptop computers helps ensure the information is protected, even if the laptop is lost or stolen.

Tapes Containing Confidential Information Were Not Transported Securely

The Department processes and mails computer tapes containing unencrypted personal information, including employee names and social security numbers. These computer tapes are received through the mail from various employers as part of the state's new hire directory program. During a typical month, the Department receives 19 unencrypted tapes, totaling nearly 33,000 employee records. While these tapes are in the Department's custody, the security of this confidential information remains a Department responsibility.

Department staff indicated that after processing the tapes, they are returned to the employers. The process of returning these tapes to the originating employers uses regular mail through the U.S. Postal System. The information on the returned tapes is neither erased nor encrypted. DETR IT staff said that tapes are not erased after processing in order to rerun the tape if the original processing fails.

State law requires agencies to implement reasonable security measures to protect the confidential personal information they collect. If one of these tapes is lost or stolen during its return to the employer, the state could be responsible for contacting those whose confidential information has been compromised.

Recommendations

5. Encrypt all sensitive data stored on laptop computers in accordance with state IT security standards.
6. Develop procedures to ensure the security of new hire directory information received by and sent from the Department.

Weaknesses Exist in Managing Network Users

The Department did not always remove former employees' network access. In addition, DETR did not conduct background investigations on employees. These weaknesses increase the risk of unauthorized individuals gaining access to sensitive data.

<u>Former Staff Had Current Network Access</u>

Twenty-seven former employees, partners[1], and contractors retained access to DETR's computer network after they had left the service of the Department. This included 5 former employees, 20 former partners, and 2 former contractors. Fifteen of these accounts were enabled over one year after the individuals either last logged on or left employment.

In addition, we found that when former employees' accounts were disabled, it was often not timely. For example, we reviewed 31 network user accounts of

[1] A partner is an employee of a non-government organization that assists DETR in finding employment for individuals. An example of a partner organization is Job Opportunities in Nevada (JOIN).

employees departing the Department between January 1 and April 19, 2008, and found 10 of these accounts remained enabled from 7 to 18 days after their last day of employment.

State standards require agencies to promptly remove users who are no longer in the Department's service. This action reduces the risk that a former employee could gain unauthorized access to the confidential information stored in the agency's network. DETR indicated its procedure for the removal of former employees, partners, and contractors network access needed improvement.

Background Investigations Were Not Conducted on Employees

The Department does not conduct routine background investigations on staff with access to IT systems or sensitive data. We noted the Department had not conducted background investigations on any of the 50 information technology staff. In addition, background investigations had not been conducted on newly hired employees who have access to sensitive information. The Department stores and processes large amounts of sensitive information which includes names and social security numbers. State IT security standards require background investigations on employees with access to this sensitive information. Granting people access to sensitive data without appropriate background investigations increases the risk that unsuitable individuals could gain access to sensitive information, use it inappropriately, or destroy it.

Department officials informed us that they had not yet implemented these background investigations due to a combination of privacy concerns and funding issues. However, officials said they are committed to following state policy and will conduct background investigations on all new hires immediately and will conduct these checks on existing IT staff over an 18 month period.

Recommendations

7. Develop a more effective procedure to disable former network accounts timely.
8. Periodically review user accounts to identify former employees, partners, and contractors.

9. Ensure all IT staff and any new hires with access to sensitive information have background investigations in accordance with state IT security standards.

Routine Network Maintenance Needs Improvement

The Department lacks adequate procedures to ensure various network security features are maintained. This includes ensuring virus definitions are current and the firewall is appropriately configured. In addition, laptop computers should have their network cards configured to avoid connecting to unknown networks.

Computer Virus Definitions Were Not Up-to-date

Some DETR computers did not have current antivirus protection. Of the 144 computers we sampled statewide at various DETR offices, we found 16 computers or 11% of our sample lacking adequate antivirus protection. These virus definition files ranged from 25 to 421 days old. This condition was caused by missing or malfunctioning antivirus software on these computers.

State IT security standards require antivirus software to be installed on each computer to protect from computer viruses that typically come from the Internet. The software needs to be periodically updated with new virus definitions. These definitions allow the software to more easily identify viruses and ensure protection from current threats.

Firewall Configuration and Management Could Be Improved

The Department's internal firewall could be improved in both configuration and management. Examples include lack of descriptive names for various rules and rule settings that should be more restrictive. These changes facilitate routine firewall maintenance and become especially important when someone is newly selected to administer the firewall. We also identified firewall rules that were not used, and a setting that should not be allowed. These weaknesses reduce the security of the sensitive data and systems that reside behind this firewall. Compliance with best practices such as those issued by the Center for Internet Security will enhance security.

A firewall is a device that prevents all computer traffic from entering a network unless that traffic has been specifically allowed by a set of rules established by the agency. Although most firewalls act as a barrier between the Internet and the agency's internal network, DETR's does not. Protection from the Internet is provided by the Department of Information Technology's firewall. Instead, DETR uses its firewall to segregate parts of its internal network. This firewall represents an additional layer of security for the critical applications and data that reside behind the firewall.

Laptops Did Not Have Secure Wireless Configurations

Sixteen of the 32 laptop computers we sampled did not have secure wireless configurations. These laptops' wireless configuration settings were set to "Any available network" or "Peer-to-Peer" instead of the recommended best practice setting of "Access Point (Infrastructure) networks only" setting. In addition, none of the laptop users indicated they had received security awareness training related to the risks of using wireless networking.

Wireless communication, commonly referred to as Wi-Fi, allows users the freedom to move around an office with their computers while staying connected to a network. This occurs because the computer's wireless hardware is communicating with a device known as an "access point" which is connected to a network. However, there are risks associated with this technology that could allow unauthorized access to an agency's network and data.

Modern laptop computers frequently have wireless network hardware pre-installed even if the agency has no business requirement for its use. However, these wireless devices can act as unintended 'backdoors' into the computer and any networks they are connected to. If these wireless cards are not disabled or properly configured, the laptops can connect to unknown networks, thereby allowing unauthorized individuals access to data on the laptops or on the network.

Recommendations

10. Create adequate procedures and periodically review to ensure computers have antivirus programs installed and that virus definitions are frequently updated.
11. Periodically review the firewall to ensure it is properly configured and maintained.

12. Ensure laptop computers have secure wireless configurations.

13. Train wireless laptop users on the risks associated with using wireless networking.

Other Security-related Concerns

We found several other areas where security could be improved. For example, the Department does not adequately restrict some application developers' access to production data. In addition, physical access to important servers at some locations is not restricted. Finally, password controls can be strengthened.

Some Application Developers Had Inappropriate Access to Production Data

We identified four Information System Application (ISA) developers who had inappropriate access to the Rehabilitation Automated Information System of Nevada (RAISON) application's corresponding production database. Access to the production database should be restricted to properly segregate incompatible functions. By allowing this group update access to production data, the risks of accidental or intentional corruption of the corresponding data is increased.

We also identified a shared generic account used by these same ISA developers. This account provided access to a tool which also allows the developers to directly access the production data. Department officials indicated these two conditions were the result of implementing procedures that facilitated application and data maintenance at the cost of reduced security.

Computer programmers that create and maintain computer programs used by agency employees are called application developers. A fundamental rule in application security is that developers should not have access to production databases in order to prevent undesirable and unintended changes to the data. The production data should only be modified by authorized users through the intended application interface.

Some Servers Were Located in Unsecured Rooms

Network servers at 4 of the 15 locations we examined did not have their network servers properly secured in locked rooms or locked metal cabinets as required by state information security standards. These four locations included Fallon, Elko, Henderson, and North Las Vegas.

Servers “serve up” information and data to networks, people, and other computers. Examples include web servers, network servers, or servers that store files. Because these servers are critical to an agency’s network and data, their protection is extremely important. To avoid accidental or intentional damage to the servers, physical access should be limited to those individuals who maintain them.

Password Controls Need Strengthening

A password setting allowed too many unsuccessful login attempts to the Department’s network. The Department’s network group policy settings allowed six unsuccessful log-in attempts before a network account was locked rather than the state standard of three. Locking an account after several unsuccessful login attempts prevents password guessing by unauthorized persons. Password controls represent fundamental security controls that prevent unauthorized access to computer networks.

Recommendations

14. Restrict ISA developers’ direct access to production data.
15. Remove shared generic account.
16. Ensure physical access to critical servers is properly restricted.
17. Enforce state IT security standards for password controls.

Appendices

Appendix A

Audit Methodology

To gain an understanding of the Department of Employment, Training and Rehabilitation, we interviewed Department management and staff. We reviewed legislation, committee minutes, and state and Department policies. We interviewed the Department's information technology staff to gain a broad understanding of the Department's network resources and how they are managed and utilized. We discussed how the Department interconnects and interacts with the Department of Information Technology, other state agencies, and third party service providers.

To ensure our audit tests were representative of the Department's statewide operations, we conducted tests at 15 of the Department's offices located throughout the state. During our audit, we examined adherence to the state's IT security standards as well as the Department's own IT security policies and procedures.

To determine if controls over desktop computer security were adequate, we tested a judgmental sample of 96 Department desktop computers to ensure they had the latest operating system updates as well as having current antivirus protection. Computers selected were based on location throughout the state. We also examined the Department's network user accounts to determine if only current employees had access to the network. We then determined if the Department's computer network users had background investigations conducted and if they had signed security awareness statements.

To assess the security of the Department's network servers, we tested their security settings. Specifically, we tested to ensure they were configured to enforce state password standards for all accounts. We also examined the physical security over the network servers at each location we visited.

We conducted tests on a judgmental sample of 32 laptop computers to ensure they had the latest operating system updates and current antivirus protection. The sample was based on location throughout the state. In addition, we identified ‘backdoors’ into the network through unauthorized or misconfigured wireless devices on laptops. We also examined the administration of the Department’s firewall to determine if it was properly configured and maintained.

Finally, we identified and tested controls over sensitive data the Department collects to determine if access to the data was appropriately restricted.

Our audit work was conducted from January to November 2008. 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 218.821, we furnished a copy of our preliminary report to the Director of the Department of Employment, Training and Rehabilitation. On May 7, 2009, 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 C which begins on page 21.

Contributors to this report included:

Jeff Rauh, CIA, CISA
Deputy Legislative Auditor

Tom Tittle, CPA, CIA, CFE
Deputy Legislative Auditor

Eugene Allara, CPA
Deputy Legislative Auditor

S. Douglas Peterson, CISA
Information Systems Audit Supervisor

Stephen M. Wood, CPA
Chief Deputy Legislative Auditor

Appendix B

Glossary of Terms

Backdoors Undocumented ways of gaining access to a program, online service, or an entire computer system. An unauthorized wireless access point is an example.

Developers Developers are computer programmers who plan, create, and maintain an information system application.

Domain Controller A network server used to administer users of the computer network, to set parameters such as password length, duration, and complexity as well as to implement user access restrictions.

Encryption The process of transforming information to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

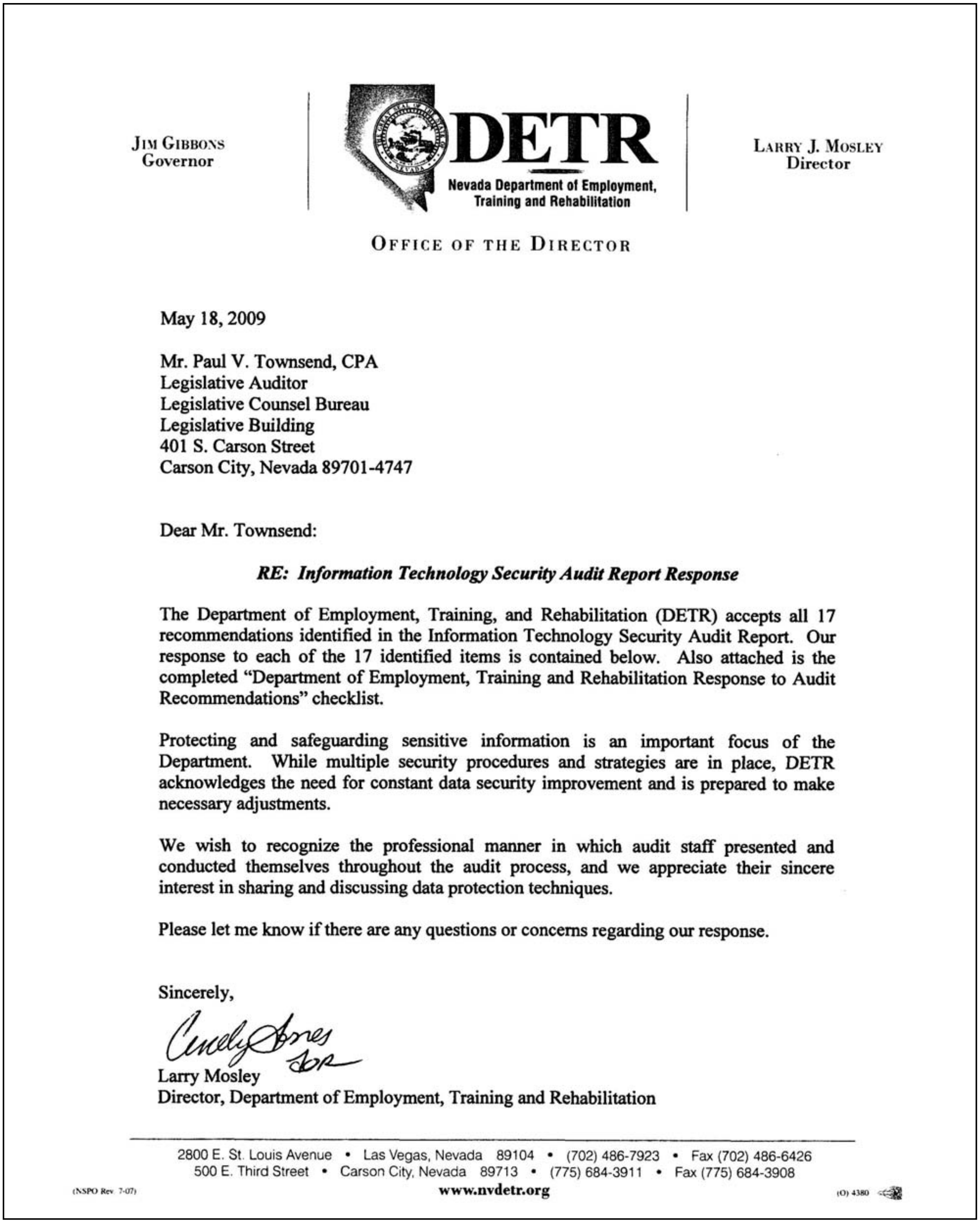
Firewall A firewall is a computer hardware device or software application that prevents all network traffic from passing through unless it is specifically allowed by a set of rules created by the organization’s information technology staff.

PII Personally Identifiable Information such as name, date of birth, address, social security numbers, etc.

Server A computer more powerful than a typical desktop computer that can be used to provide a variety of specialized functions: Common server functions include: network servers (domain controllers), file servers, e-mail servers, web servers, domain name system (DNS) servers, and application servers.

Appendix C

Response From the Department of Employment, Training and Rehabilitation



JIM GIBBONS
Governor

DETR
Nevada Department of Employment,
Training and Rehabilitation

LARRY J. MOSLEY
Director

OFFICE OF THE DIRECTOR

May 18, 2009

Mr. Paul V. Townsend, CPA
Legislative Auditor
Legislative Counsel Bureau
Legislative Building
401 S. Carson Street
Carson City, Nevada 89701-4747

Dear Mr. Townsend:

RE: Information Technology Security Audit Report Response

The Department of Employment, Training, and Rehabilitation (DETR) accepts all 17 recommendations identified in the Information Technology Security Audit Report. Our response to each of the 17 identified items is contained below. Also attached is the completed "Department of Employment, Training and Rehabilitation Response to Audit Recommendations" checklist.

Protecting and safeguarding sensitive information is an important focus of the Department. While multiple security procedures and strategies are in place, DETR acknowledges the need for constant data security improvement and is prepared to make necessary adjustments.

We wish to recognize the professional manner in which audit staff presented and conducted themselves throughout the audit process, and we appreciate their sincere interest in sharing and discussing data protection techniques.

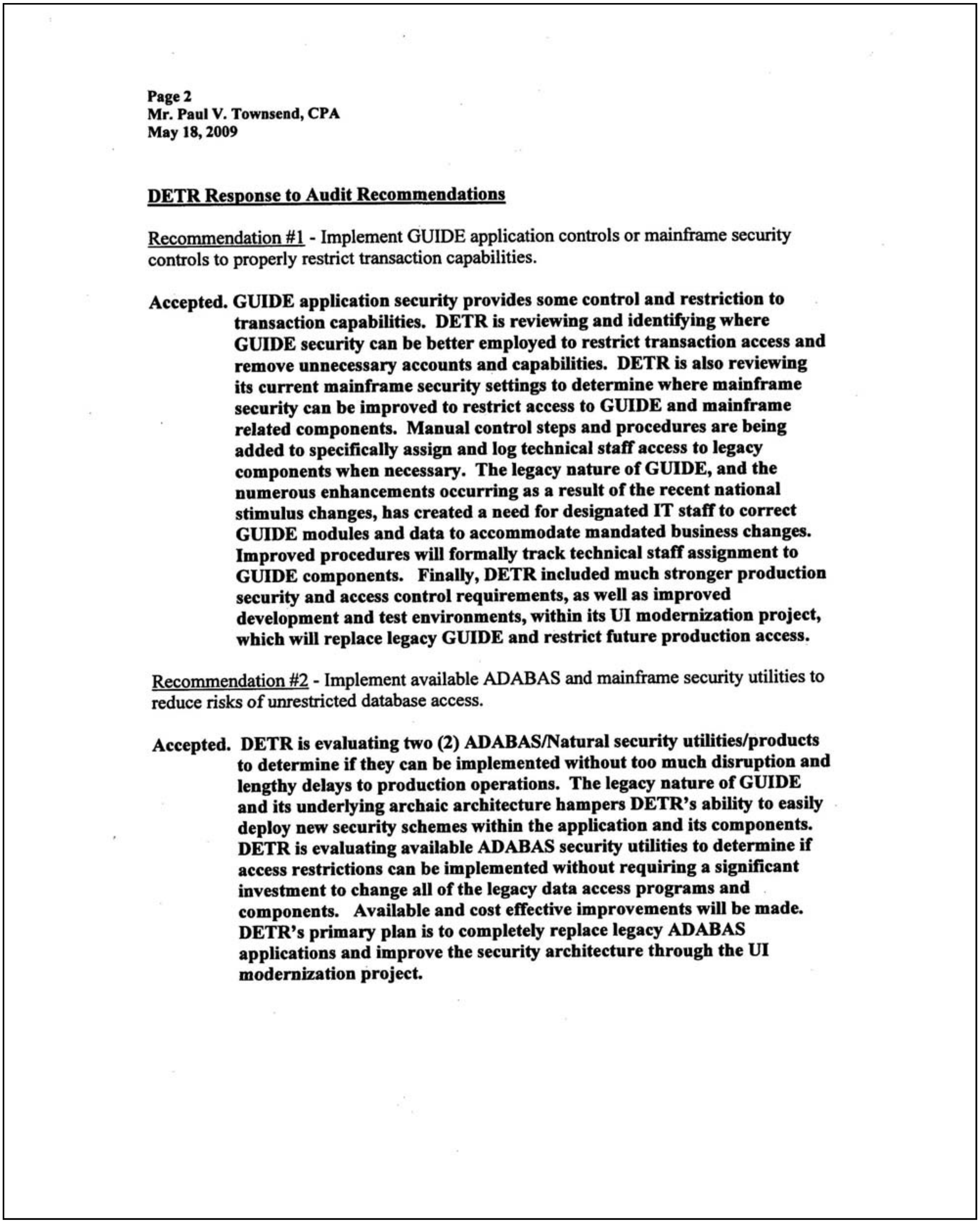
Please let me know if there are any questions or concerns regarding our response.

Sincerely,

Cindy Jones
for

Larry Mosley
Director, Department of Employment, Training and Rehabilitation

2800 E. St. Louis Avenue • Las Vegas, Nevada 89104 • (702) 486-7923 • Fax (702) 486-6426
500 E. Third Street • Carson City, Nevada 89713 • (775) 684-3911 • Fax (775) 684-3908
(NSPO Rev. 7-07) **www.nvdetr.org** (O) 4380



Page 2
Mr. Paul V. Townsend, CPA
May 18, 2009

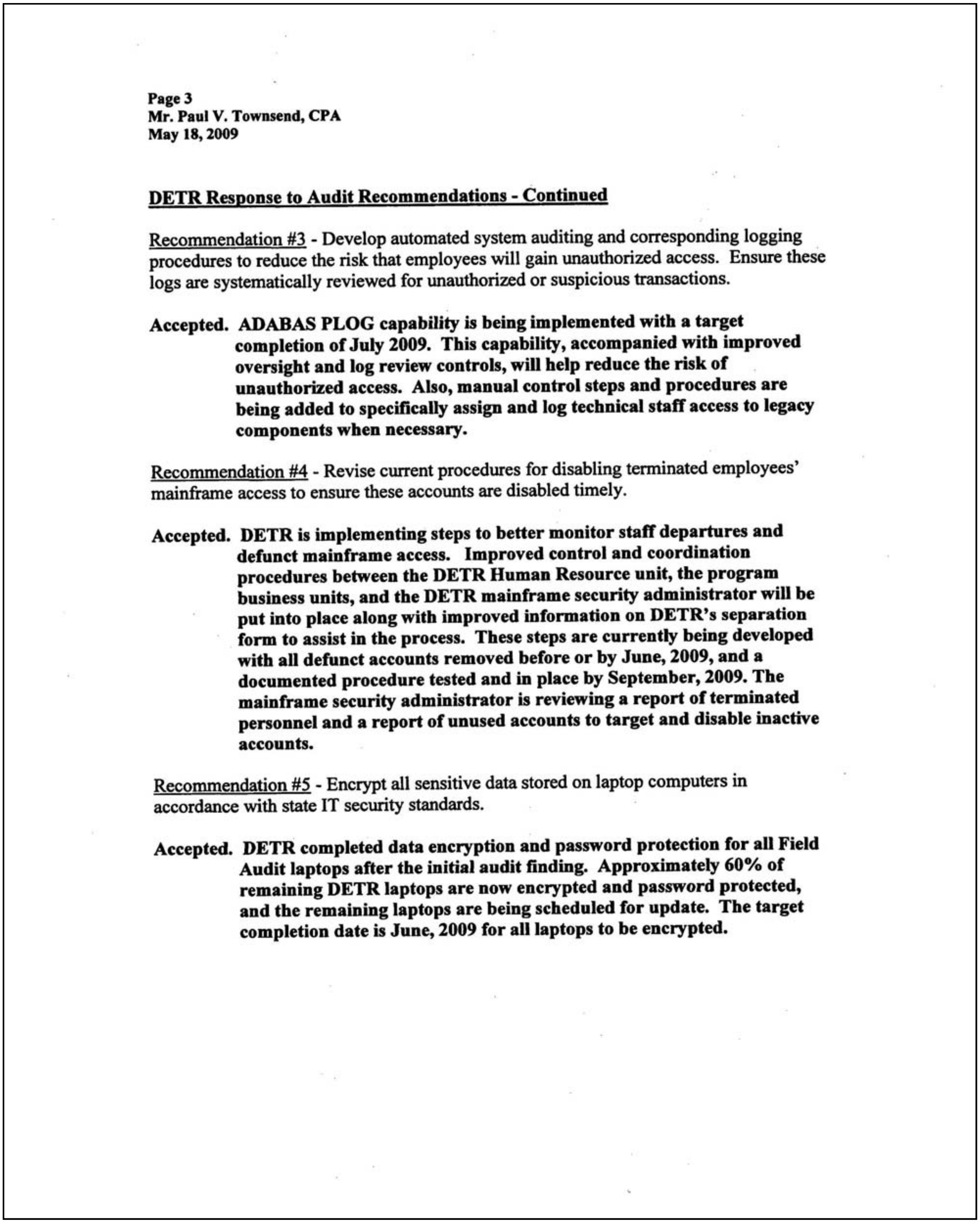
DETR Response to Audit Recommendations

Recommendation #1 - Implement GUIDE application controls or mainframe security controls to properly restrict transaction capabilities.

Accepted. GUIDE application security provides some control and restriction to transaction capabilities. DETR is reviewing and identifying where GUIDE security can be better employed to restrict transaction access and remove unnecessary accounts and capabilities. DETR is also reviewing its current mainframe security settings to determine where mainframe security can be improved to restrict access to GUIDE and mainframe related components. Manual control steps and procedures are being added to specifically assign and log technical staff access to legacy components when necessary. The legacy nature of GUIDE, and the numerous enhancements occurring as a result of the recent national stimulus changes, has created a need for designated IT staff to correct GUIDE modules and data to accommodate mandated business changes. Improved procedures will formally track technical staff assignment to GUIDE components. Finally, DETR included much stronger production security and access control requirements, as well as improved development and test environments, within its UI modernization project, which will replace legacy GUIDE and restrict future production access.

Recommendation #2 - Implement available ADABAS and mainframe security utilities to reduce risks of unrestricted database access.

Accepted. DETR is evaluating two (2) ADABAS/Natural security utilities/products to determine if they can be implemented without too much disruption and lengthy delays to production operations. The legacy nature of GUIDE and its underlying archaic architecture hampers DETR's ability to easily deploy new security schemes within the application and its components. DETR is evaluating available ADABAS security utilities to determine if access restrictions can be implemented without requiring a significant investment to change all of the legacy data access programs and components. Available and cost effective improvements will be made. DETR's primary plan is to completely replace legacy ADABAS applications and improve the security architecture through the UI modernization project.



DETR Response to Audit Recommendations - Continued

Recommendation #3 - Develop automated system auditing and corresponding logging procedures to reduce the risk that employees will gain unauthorized access. Ensure these logs are systematically reviewed for unauthorized or suspicious transactions.

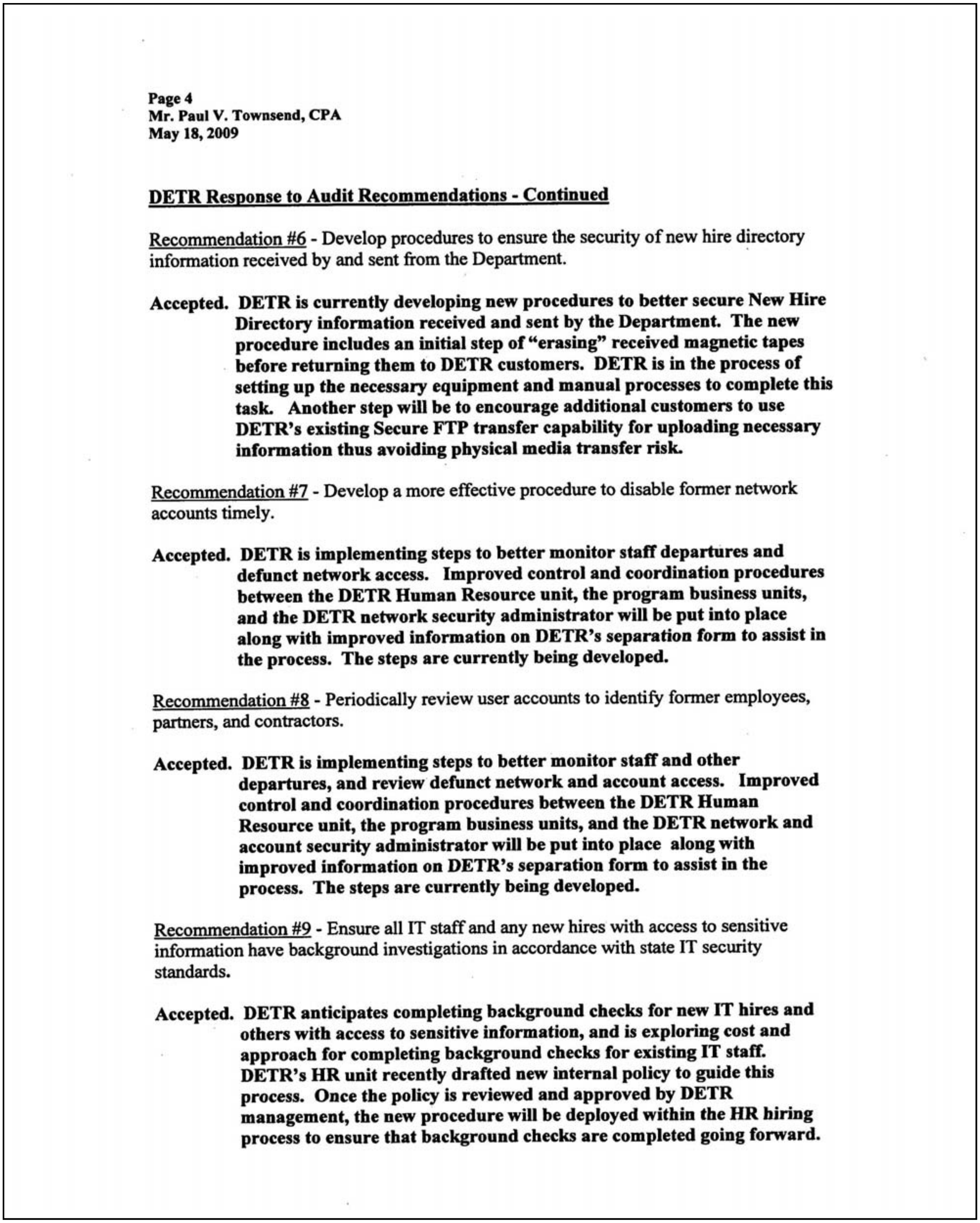
Accepted. ADABAS PLOG capability is being implemented with a target completion of July 2009. This capability, accompanied with improved oversight and log review controls, will help reduce the risk of unauthorized access. Also, manual control steps and procedures are being added to specifically assign and log technical staff access to legacy components when necessary.

Recommendation #4 - Revise current procedures for disabling terminated employees' mainframe access to ensure these accounts are disabled timely.

Accepted. DETR is implementing steps to better monitor staff departures and defunct mainframe access. Improved control and coordination procedures between the DETR Human Resource unit, the program business units, and the DETR mainframe security administrator will be put into place along with improved information on DETR's separation form to assist in the process. These steps are currently being developed with all defunct accounts removed before or by June, 2009, and a documented procedure tested and in place by September, 2009. The mainframe security administrator is reviewing a report of terminated personnel and a report of unused accounts to target and disable inactive accounts.

Recommendation #5 - Encrypt all sensitive data stored on laptop computers in accordance with state IT security standards.

Accepted. DETR completed data encryption and password protection for all Field Audit laptops after the initial audit finding. Approximately 60% of remaining DETR laptops are now encrypted and password protected, and the remaining laptops are being scheduled for update. The target completion date is June, 2009 for all laptops to be encrypted.



DETR Response to Audit Recommendations - Continued

Recommendation #6 - Develop procedures to ensure the security of new hire directory information received by and sent from the Department.

Accepted. DETR is currently developing new procedures to better secure New Hire Directory information received and sent by the Department. The new procedure includes an initial step of "erasing" received magnetic tapes before returning them to DETR customers. DETR is in the process of setting up the necessary equipment and manual processes to complete this task. Another step will be to encourage additional customers to use DETR's existing Secure FTP transfer capability for uploading necessary information thus avoiding physical media transfer risk.

Recommendation #7 - Develop a more effective procedure to disable former network accounts timely.

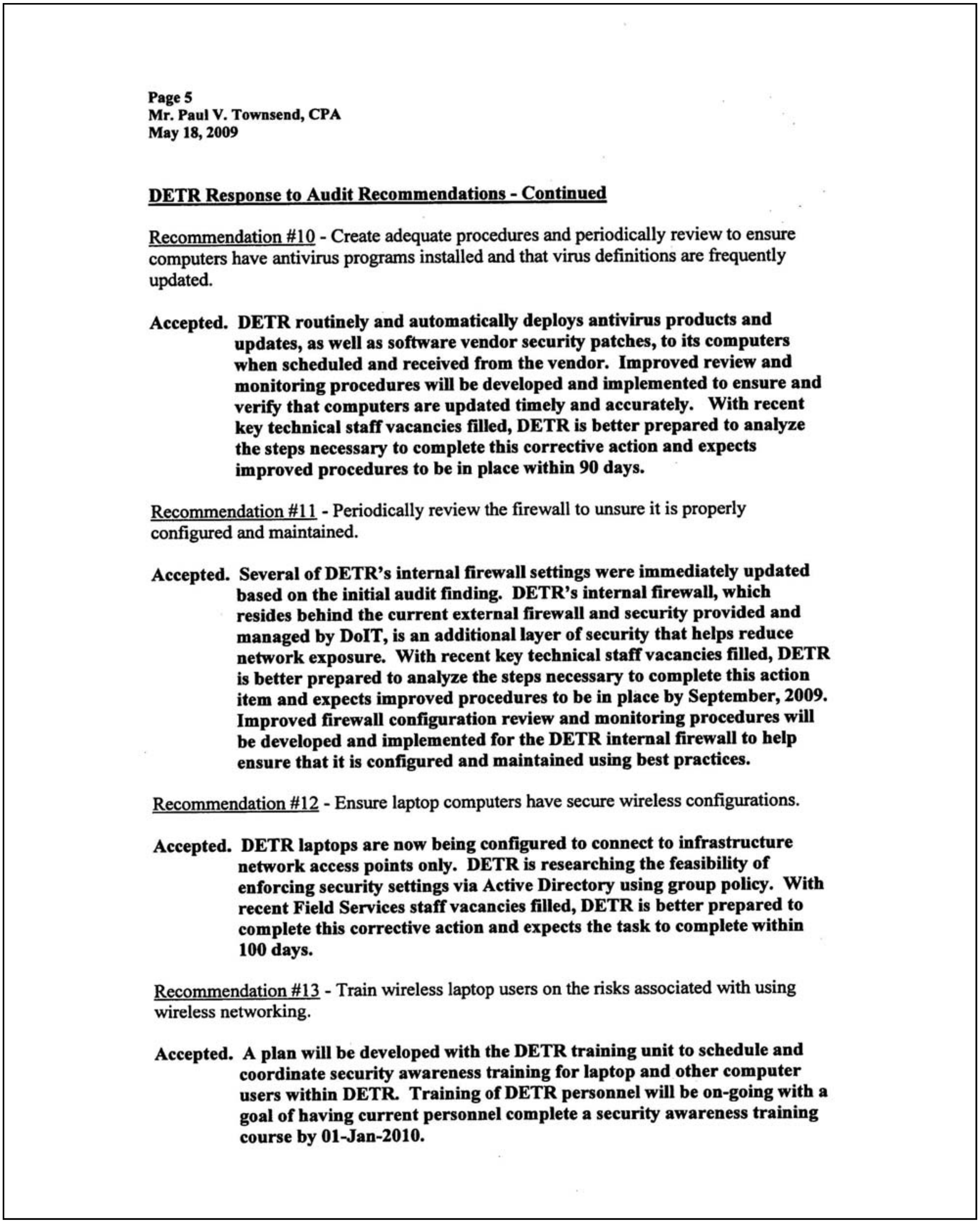
Accepted. DETR is implementing steps to better monitor staff departures and defunct network access. Improved control and coordination procedures between the DETR Human Resource unit, the program business units, and the DETR network security administrator will be put into place along with improved information on DETR's separation form to assist in the process. The steps are currently being developed.

Recommendation #8 - Periodically review user accounts to identify former employees, partners, and contractors.

Accepted. DETR is implementing steps to better monitor staff and other departures, and review defunct network and account access. Improved control and coordination procedures between the DETR Human Resource unit, the program business units, and the DETR network and account security administrator will be put into place along with improved information on DETR's separation form to assist in the process. The steps are currently being developed.

Recommendation #9 - Ensure all IT staff and any new hires with access to sensitive information have background investigations in accordance with state IT security standards.

Accepted. DETR anticipates completing background checks for new IT hires and others with access to sensitive information, and is exploring cost and approach for completing background checks for existing IT staff. DETR's HR unit recently drafted new internal policy to guide this process. Once the policy is reviewed and approved by DETR management, the new procedure will be deployed within the HR hiring process to ensure that background checks are completed going forward.



DETR Response to Audit Recommendations - Continued

Recommendation #10 - Create adequate procedures and periodically review to ensure computers have antivirus programs installed and that virus definitions are frequently updated.

Accepted. DETR routinely and automatically deploys antivirus products and updates, as well as software vendor security patches, to its computers when scheduled and received from the vendor. Improved review and monitoring procedures will be developed and implemented to ensure and verify that computers are updated timely and accurately. With recent key technical staff vacancies filled, DETR is better prepared to analyze the steps necessary to complete this corrective action and expects improved procedures to be in place within 90 days.

Recommendation #11 - Periodically review the firewall to unsure it is properly configured and maintained.

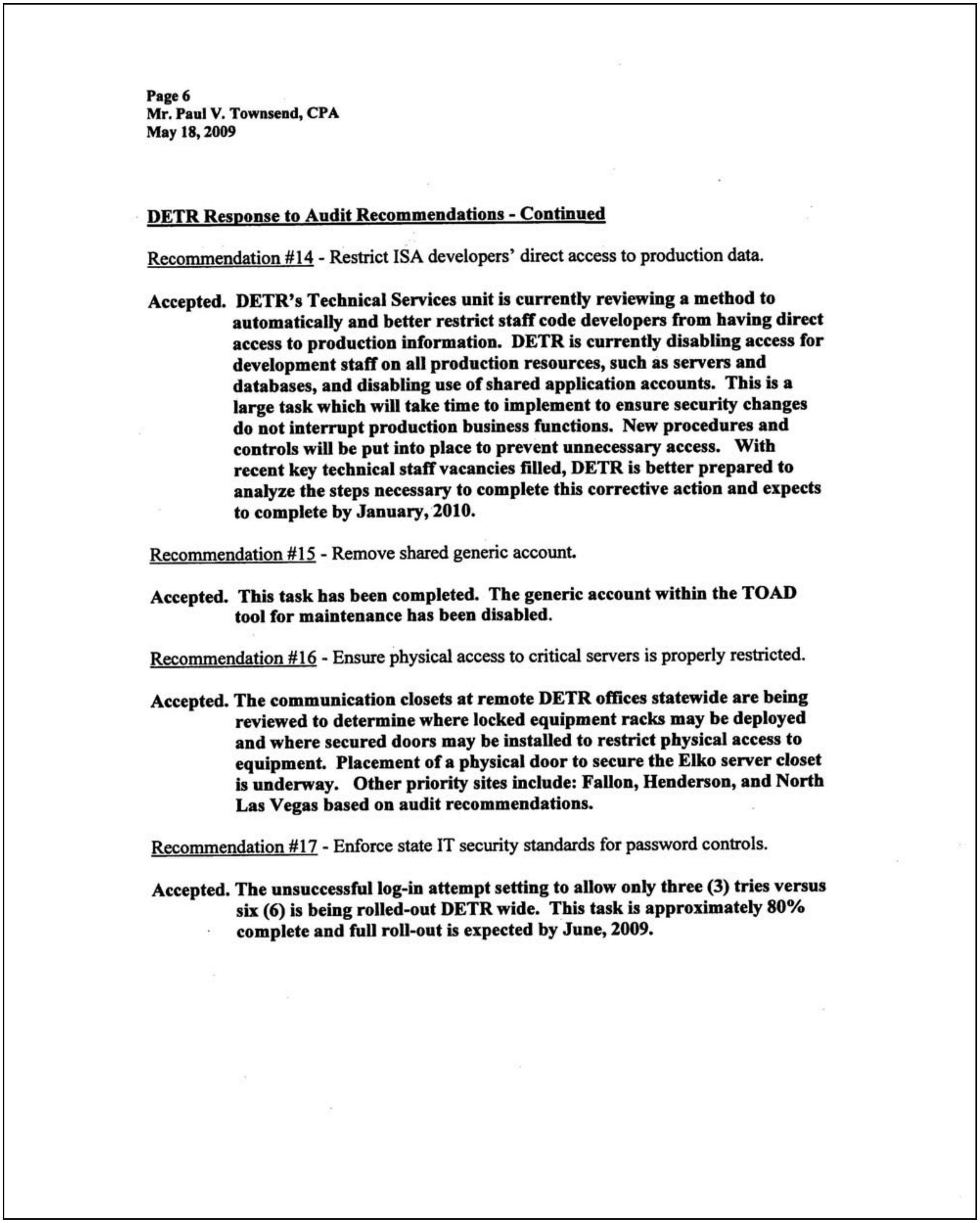
Accepted. Several of DETR's internal firewall settings were immediately updated based on the initial audit finding. DETR's internal firewall, which resides behind the current external firewall and security provided and managed by DoIT, is an additional layer of security that helps reduce network exposure. With recent key technical staff vacancies filled, DETR is better prepared to analyze the steps necessary to complete this action item and expects improved procedures to be in place by September, 2009. Improved firewall configuration review and monitoring procedures will be developed and implemented for the DETR internal firewall to help ensure that it is configured and maintained using best practices.

Recommendation #12 - Ensure laptop computers have secure wireless configurations.

Accepted. DETR laptops are now being configured to connect to infrastructure network access points only. DETR is researching the feasibility of enforcing security settings via Active Directory using group policy. With recent Field Services staff vacancies filled, DETR is better prepared to complete this corrective action and expects the task to complete within 100 days.

Recommendation #13 - Train wireless laptop users on the risks associated with using wireless networking.

Accepted. A plan will be developed with the DETR training unit to schedule and coordinate security awareness training for laptop and other computer users within DETR. Training of DETR personnel will be on-going with a goal of having current personnel complete a security awareness training course by 01-Jan-2010.



DETR Response to Audit Recommendations - Continued

Recommendation #14 - Restrict ISA developers' direct access to production data.

Accepted. DETR's Technical Services unit is currently reviewing a method to automatically and better restrict staff code developers from having direct access to production information. DETR is currently disabling access for development staff on all production resources, such as servers and databases, and disabling use of shared application accounts. This is a large task which will take time to implement to ensure security changes do not interrupt production business functions. New procedures and controls will be put into place to prevent unnecessary access. With recent key technical staff vacancies filled, DETR is better prepared to analyze the steps necessary to complete this corrective action and expects to complete by January, 2010.

Recommendation #15 - Remove shared generic account.

Accepted. This task has been completed. The generic account within the TOAD tool for maintenance has been disabled.

Recommendation #16 - Ensure physical access to critical servers is properly restricted.

Accepted. The communication closets at remote DETR offices statewide are being reviewed to determine where locked equipment racks may be deployed and where secured doors may be installed to restrict physical access to equipment. Placement of a physical door to secure the Elko server closet is underway. Other priority sites include: Fallon, Henderson, and North Las Vegas based on audit recommendations.

Recommendation #17 - Enforce state IT security standards for password controls.

Accepted. The unsuccessful log-in attempt setting to allow only three (3) tries versus six (6) is being rolled-out DETR wide. This task is approximately 80% complete and full roll-out is expected by June, 2009.

Department of Employment, Training and Rehabilitation
Response to Audit Recommendations

Recommendation Number		Accepted	Rejected
1	Implement GUIDE application controls or mainframe security controls to properly restrict transaction capabilities	X	
2	Implement available ADABAS and mainframe security utilities to reduce risks of unrestricted database access	X	
3	Develop automated system auditing and corresponding logging procedures to reduce the risk that employees will gain unauthorized access. Ensure these logs are systematically reviewed for unauthorized or suspicious transactions	X	
4	Revise current procedures for disabling terminated employees' mainframe access to ensure these accounts are disabled timely	X	
5	Encrypt all sensitive data stored on laptop computers in accordance with state IT security standards	X	
6	Develop procedures to ensure the security of new hire directory information received by and sent from the Department	X	
7	Develop a more effective procedure to disable former network accounts timely	X	
8	Periodically review user accounts to identify former employees, partners, and contractors	X	
9	Ensure all IT staff and any new hires with access to sensitive information have background investigations in accordance with state IT security standards	X	
10	Create adequate procedures and periodically review to ensure computers have antivirus programs installed and that virus definitions are frequently updated	X	
11	Periodically review the firewall to ensure it is properly configured and maintained	X	
12	Ensure laptop computers have secure wireless configurations	X	
13	Train wireless laptop users on the risks associated with using wireless networking	X	

Department of Employment, Training and Rehabilitation
Response to Audit Recommendations
(continued)

Recommendation Number		Accepted	Rejected
14	Restrict ISA developers' direct access to production data	X	
15	Remove shared generic account	X	
16	Ensure physical access to critical servers is properly restricted	X	
17	Enforce state IT security standards for password controls	X	
	TOTALS	17	0