LA12-12

STATE OF NEVADA

Audit Report

Department of Administration
Division of Enterprise
Information Technology Services

2012

Legislative Auditor
Carson City, Nevada

Audit Highlights

Highlights of Legislative Auditor report on the Division of Enterprise Information Technology Services Information Technology Security issued on February 2, 2012.
Report # LA12-12

Background

With legislation in 2011, the Department of Information Technology was changed to the Division of Enterprise Information Technology Services and was transferred to the Department of Administration. The mission of the Division of Enterprise Information Technology Services is to provide services to coordinate efficient, effective, and secure use of information systems and personnel. The Division consists of the following units: Administrative Services, Information Security, and Technical Operations. The Administrative Services unit supports the Division's budgeting, personnel, service rate billing, and purchasing functions. The Information Security Unit, known as the Office of Information Security, provides statewide information security services. The Technical Operations unit provides programming, web services, mainframe and server services, telecommunication services, and numerous other information technology services. For fiscal year 2011, the Division employed 130 full-time employees statewide and had authorized expenditures of over $28 million.

Purpose of Audit

This audit included a review of information technology controls at the Division of Enterprise Information Technology Services during fiscal year 2011. The objective of our audit was to determine if the Division's information security controls were adequate to protect the confidentiality, integrity, and availability of sensitive information and information systems.

Audit Recommendations

This audit report contains 15 recommendations to improve the confidentiality, integrity, and availability of state information systems.

The Division accepted the 15 recommendations.

Recommendation Status

The Division's 60-day plan for corrective action is due on April 26, 2012. In addition, the six-month report on the status of audit recommendations is due on October 29, 2012.

Division of Enterprise Information Technology Services

Department of Administration

Summary

The Division needs to strengthen information system controls to ensure adequate protection over systems and data. The availability of key state information systems can be better ensured by updating and testing the state's primary computing facility's emergency plans. Also, the security of confidential personal information could be improved with better security oversight of occupational licensing agencies or boards. In addition, web server content should be better monitored to prevent accidental release of confidential information. Furthermore, a systematic process to identify statewide information security risks could improve use of security resources.

Former employees had current network access and better controls are needed over the computing facility access cards. Computer virus protection and critical security updates need to be better monitored. In addition, stronger security can be achieved by encrypting data in newly developed software applications, alerting state agencies more timely about newly identified risks, and enforcing state password standards.

Key Findings

The State's primary computing facility did not have a written disaster recovery plan. In addition, the facility's disaster recovery capability has not been tested since 2006. Such testing reduces the time needed to restore critical IT services such as those that may impact public health and safety. In addition, the contingency plan we were provided by the Division had not been updated in over 10 years despite numerous changes in the state's information technology infrastructure and changes in employees responsible for enacting parts of the plan. Without periodic updating and testing of these plans, there is greater risk that mission critical IT resources will not be restored in an efficient and timely manner when a disaster or other major system failure occurs. (page 3)

Most state occupational licensing boards that collect confidential personal information of licensees do not currently receive security oversight from the state's Office of Information Security. The Division indicates that state boards and commissions have avoided any assistance or oversight by them. These boards normally collect applicant social security numbers used in determining if the applicants have any unpaid child support payments. Given the confidential nature of the data collected, the Division's security oversight could help prevent unintended disclosure of the information. (page 6)

We found Division hosted state websites were not monitored for the release of sensitive confidential information as recommended in our prior audit. As a result, we found confidential personal information was again posted on a state website that was viewable to anyone on the Internet. While the primary responsibility for monitoring website content is the agency owning the website, a backup monitoring process is needed to detect any confidential personal information that is unintentionally posted on the websites. (page 7)

We identified nine computer user accounts of former employees whose network access had not been disabled. These accounts could have been identified and disabled if the Division was conducting quarterly reviews of user lists as required by state information security standards. (page 9)

We identified 18 Personal Identity Verification (PIV) cards that needed to be deactivated. These PIV cards are used by Division employees to gain access to restricted office or computing locations. The PIV cards needing deactivation could have been identified and deactivated if the Division was conducting the quarterly audits of the PIV card system as required by the Division's own policies. (page 9)

Four of the 32 Division computers we sampled did not have current virus protection as required by state security standards. Without current virus protection, there is increased risk that employees with infected computers will lose productive time while their computers are purged of the infected files. In addition, we identified 7 of 32 computers that did not have critical software security patches installed as required by state security standards. (page 11)

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
~~Fax No.: (775) 684-6600~~

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

LEGISLATIVE COMMISSION (775) 684-6800
STEVEN A. HORSFORD, *Senator, Chairman*
Lorne J. Malkiewich, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
DEBBIE SMITH, *Assemblywoman, Chair*
Rick Combs, *Fiscal Analyst*
Mark Krmpotic, *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 completed audit of the Department of Administration, Division of Enterprise Information Technology Services. 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.

During our audit, administration of information technology security was performed by the Department of Information Technology. With the passage of Senate Bill 427 during the 2011 Legislative Session, the Department was changed to the Division of Enterprise Information Technology Services within the Department of Administration. This report includes 15 recommendations to the Division of Enterprise Information Technology Services to improve the confidentiality, integrity, and availability of state information systems and data. 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, CPA
Legislative Auditor

January 18, 2012
Carson City, Nevada

Division of Enterprise Information Technology Services
Table of Contents

Division of Enterprise Information Technology Services
Table of Contents
(continued)

Appendices

Introduction

Background

The mission of the Division of Enterprise Information Technology Services (Division) is to provide services to coordinate efficient, effective, and secure use of information systems and personnel[1]. When the audit began, the Division consisted of an Administrator's office and the following units: Administrative Services, Information Security, and Technical Operations. The Administrative Services unit supports the Division's budgeting, personnel, service rate billing, and purchasing functions. The Information Security unit, known as the Office of Information Security, provides statewide information security services. The Technical Operations unit provides programming, web services, mainframe and server services, telecommunication services, and numerous other information technology services.

For fiscal year 2011, the Division employed 130 full-time employees statewide and had authorized expenditures of over $28 million.

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 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.

This audit included a review of information technology controls at the Division of Enterprise Information Technology Services during fiscal year 2011. The objective of our audit was to determine if the

[1] With legislation in 2011, the Department of Information Technology was changed to the Division of Enterprise Information Technology Services and was transferred to the Department of Administration.

Division's information security controls were adequate to protect the confidentiality, integrity, and availability of sensitive information and information systems.

State Information Technology Emergency Plans Need Strengthening

The State's primary computing facility's disaster recovery and contingency plans need strengthening. These plans need to be updated, tested, and prioritized. Disaster recovery plans and contingency plans help ensure the rapid and orderly recovery from major information system failures that may periodically occur. Periodic testing of these plans enables Information Technology (IT) staff to retain familiarity with the restoration process, identify plan shortcomings, incorporate new applications in the process, and familiarize new staff with the process. Such testing reduces the time needed to restore critical IT services, such as those that may impact public health and safety.

Agency management indicated they could not locate a written disaster recovery plan. Furthermore, the state's primary computing facility's disaster recovery capability was last tested in November of 2006. State information security standards require written plans and at least biennial testing of the plans.

We also found that the disaster recovery computer hardware that is currently available is not adequate to restore all state server based computing operations. Therefore, a prioritization of state information systems is needed to ensure that those agencies with the most critical information technology missions are recovered first. The agency indicated no such prioritization currently exists.

Contingency plans have a function similar to disaster recovery plans. However, contingency plans do not assume the computing facilities have been destroyed as in a disaster recovery plan. The state's contingency plan is used to minimize the impact on the state business activities from the effects of major information system failures, whatever their cause. For example, if a construction backhoe were to sever the fiber optic cables entering the Carson City computing facility, services provided by the facility would be unavailable even though the other computing resources are still operational. A contingency plan would indicate how to rapidly restore essential services until the fiber optic cables are repaired.

The contingency plan we were provided by the Division had not been updated in over ten years. For example, various addendums to the plan include the names and phone numbers of staff responsible for specific functions in the event of a major system failure. The plan listed employees who had retired or departed the Division over ten years ago. Most of the plan's contents had not been updated in over ten years despite numerous changes in the state's information technology infrastructure.

These weaknesses have resulted from the Division's Office of Information Security (OIS) not having a current systematic process to identify and prioritize statewide information security risks. The authoritative technology standards published by organizations such as the National Institute of Standards and Technology (NIST) indicate that a risk assessment process is critical to properly manage information security risks.

Updating these plans will help ensure an orderly recovery from a disaster or other major system outage. In addition, without periodic updating, testing and prioritization of these plans, there is greater risk that mission critical IT resources will not be restored in an efficient and timely manner when a disaster or other major system failure occurs.

Recommendations

1. Update the state's primary computing facility's contingency plan and ensure the plan includes a prioritized disaster recovery component.
2. Develop a plan to periodically test the state's primary computing facility's IT emergency plans to ensure critical IT resources can be restored in an orderly and timely manner.

3. Conduct an initial high-level statewide risk assessment to identify and prioritize information security risks, establishing a baseline that can be built upon in subsequent years.

Sensitive Data Needs Better Protection

Sensitive data stored by the state needs better protection. For example, occupational licensing boards collecting licensee social security numbers (SSNs) do not receive adequate security oversight from the Division. In addition, content on state web servers is not monitored for the accidental release of confidential personal information.

Occupational Licensing Boards Need Greater Information Security Oversight

Most state occupational licensing boards that collect confidential personal information of licensees do not currently receive security oversight from the state's Office of Information Security (OIS). State security standards indicate that OIS has security oversight responsibility for all state entities within the Executive Branch of government and that all state information must be adequately secured.

Of the over 30 boards that collect applicant data, only five have their servers and data in Division facilities. The remaining boards store their data in servers in their offices. Occupational licensing boards normally collect applicant SSNs used in determining if the applicants have any unpaid child support payments.

As an example, the State Board of Optometry collects licensee information including SSNs and stores that data in a computerized database in its one-person office in Carson City. Our discussions with the Optometry Board's manager indicated the computer used to store this confidential information has never had any security checks since it was installed over five years ago.

The Division's OIS could review these servers to ensure they have current software security updates, current virus protection and are configured in accordance with state security policies. The Division agrees that these boards need its security oversight but indicated that state boards and commissions have avoided any assistance or oversight by the Division. Given the confidential nature of the data collected, the Division's security oversight could help prevent unintended disclosure of the information.

Web Server Content Is Not Monitored for the Release of Confidential Information

We found websites hosted by the Division were not monitored for the release of confidential information. As a result, confidential information, in the form of social security numbers, was posted on a state website that was viewable to anyone on the Internet. The responsible agency removed the information as soon as we brought this to their attention. This is a repeat finding from our prior audit of the Department of Information Technology in 2004.

Nationwide, confidential information is often accidentally released on public websites. For example, in March of 2011, the Texas State Comptroller reported that the State of Texas accidentally posted millions of social security numbers of state residents to a state web site.

A similar release of confidential information on a Nevada state website would be costly to the state. Nevada state law requires the state contact each person whose personal identifying information is accidentally released or is accessed by unauthorized persons. This can be a time consuming, costly, and embarrassing process. It also undermines public trust of state agencies that collect confidential personal information.

While the primary responsibility for monitoring website content is the agency owning the website, a backup monitoring process is also needed to detect any confidential personal information that is unintentionally posted on the websites.

The Division has indicated it plans to implement a process to periodically review state websites for confidential content. The Division also indicated it is considering use of an automated scanning tool that could identify such information. Either approach should reduce the risk that confidential content will remain exposed on state web servers.

Recommendations

4. Review the security of occupational licensing board servers storing confidential licensee data.
5. Offer information security services to occupational licensing boards and ensure they are aware of the state's information security standards.
6. Implement a process to periodically review state web servers for confidential information that may be accidently posted on them.

Weaknesses Exist in Managing Network Users and Facility Access

Weaknesses over managing network users and access to the state's primary computing facility could result in unauthorized access to state information systems or facilities. For example, former staff had current network access. In addition, the administration of the facility access card system needs improvement.

Former Staff Had Current Network Access

We identified nine computer user accounts of former employees whose network access had not been disabled. Five of the nine former employee accounts had been left enabled for over three years since the employees left the Division. One employee had been gone over seven years. In addition, we identified six other enabled user accounts that needed to be disabled. These six included two user accounts for persons the Division could not identify, three accounts for state employees no longer at the Division, and one current employee with two separate enabled accounts. These accounts could have been identified and disabled if the Division was conducting quarterly reviews of user lists as required by state information security standards.

Without conducting these quarterly reviews of user accounts, there is increased risk that former employees or other unauthorized persons may gain access to state information systems and confidential data.

Administration of Facility Access Card System Needs Improvement

A key card system is used to control access to the Division's offices and computing facilities. We identified 18 Personal Identity Verification (PIV) cards that needed to be deactivated. The access cards requiring deactivation included 1 former state employee whose PIV card access remained active 145 days after he had left state service, and 13 PIV card accounts for employees who no longer needed the Division's facility access. Four employees had more than one active PIV card and needed to have their additional cards deactivated.

The Division's own policy requires quarterly audits of the PIV card system. PIV cards that needed deactivation could have been identified if the Division was conducting these quarterly audits. Failure to conduct these quarterly audits increases the risks that someone will gain unauthorized access to the Division's secure facilities.

Recommendations

7. Conduct quarterly reviews of user lists as indicated in state information security standards.
8. Conduct quarterly audits of PIV card accounts as required by existing policy to ensure cards are only issued to current employees or contractors.

Routine Network Maintenance Needs Improvement

Routine maintenance needs greater attention to ensure adequate security is maintained. This includes ensuring virus protection is current and critical operating system security updates are installed.

Virus Definitions Were Not Up-to-Date

Of the 32 individual computers we sampled, we found 4 computers, or 13% of our sample, lacked adequate antivirus protection. State information security standards require all state agency computers to have virus protection software installed, and that it should be updated as new virus definition files are released. Computers without current virus protection are at risk of being corrupted by computer viruses from the Internet or attached to incoming emails. Furthermore, without current virus protection, there is increased risk that employees with infected computers will lose productive time while their computers are purged of the infected files. In addition, there is a risk that the infections could allow unauthorized access to confidential data stored on these computers.

Security Updates Were Not Always Installed

Seven computers out of 32 sampled, or 22% of our sample, did not have critical software security updates installed as required by state information security standards. State information security standards indicate that agencies must demonstrate an installation process in progress for vendor designated critical security patches within 72 hours (3 working days) from the date of the vendor’s update release.

Computers without current software security patches represent a weakness in the agency’s computer network defense system. These weaknesses can be exploited by hackers to gain unauthorized access to the Division’s information systems.

Recommendations

9. Develop a procedure to identify computers without current virus protection.
10. Develop a procedure to periodically check software update installations to detect failed or missing updates.

Other Security-related Controls

Other security-related controls need improvement. Control weaknesses included programmers not encrypting confidential data and prolonged exposure to newly identified information security risks. In addition, system administrators were using non-expiring passwords.

Security Could Be Enhanced by Encrypting Confidential Information

Division data base administrators (DBAs) and programmers do not encrypt confidential personal data in database or application development projects even though the capability currently exists at no additional cost. The DBAs and programmers use a software development framework known as .NET. The .NET framework includes the capability to encrypt confidential information in the applications being developed.

The DBAs and programmers indicated they have not been asked or told to encrypt such confidential data by their agency customers. In addition, State Security Standard 4.30, *Security for Software Development*, does not currently address confidential data encryption in software development efforts. To reduce the risk of unauthorized access to confidential data, newly developed applications and databases should implement encryption of confidential data.

Policy Development Period Leaves Risks Unmitigated for Overly Long Duration

The period of time between when an IT security risk is identified and a state policy is approved to mitigate the risk is sometimes over 12 months. For example, we found that two information technology security policies implemented during the past year took over 12 months each to be developed and subsequently approved by the State Information Security Committee. These policies addressed multi-function devices such as photocopiers and mobile devices such as cellular phones.

While the agencies who attend state information security meetings, or those who read the meeting's minutes, might know of the risk, many other state agencies would not. To reduce the risk to the state, an interim notification should be broadcast to all state agencies to alert them of the risk and what they should do to protect themselves until a state policy is agreed upon. However, we did not identify any interim risk notification process in operation that provided notification to all state agencies of the risk or what actions to take to reduce it.

Interim awareness and recommended actions about newly identified information security risks should be shared as soon as possible statewide. Such action could reduce the window of vulnerability and the likelihood of negative impact on state information systems and data. For example, during the twelve-month policy development period for multi-function devices, Division officials indicated that state agencies replaced numerous office photocopiers without knowledge that these office photocopiers contained hard drives that stored images of all the documents copied. These images could have contained confidential information.

Without an interim risk notification process, there is increased risk that a known vulnerability will be exploited to gain access to the state's information systems and confidential data. The Division has since indicated it will use its electronic security list server to send email notifications and recommended actions to all state agency information security officers or agency heads.

Some Password Controls Need Strengthening

Four system administrator accounts had non-expiring passwords. State security standards require passwords be changed at least every 90 days. Not changing passwords on a regular basis increases the chance that a compromised password will lead to a more extensive system intrusion by a hacker. The password settings were changed to the correct settings when we brought this matter to the attention of Division management. In addition, the Division indicated it will begin monitoring these password settings using an automated process.

Recommendations

11. Encrypt sensitive data in all newly developed applications.
12. Encrypt sensitive data in existing applications as is practical or as applications are upgraded.
13. Amend state information security standard to include a provision that confidential personal data be encrypted whenever possible.
14. Implement a process to communicate interim risk awareness and recommended risk mitigation measures to all state entities while a formal policy is being developed to address a state security risk.
15. Enforce state information security policies for all user passwords, including those of staff with administrator level access.

Appendix A
Audit Methodology

To gain an understanding of the Division of Enterprise Information Technology Services, we interviewed Division management and staff. We reviewed legislation, budget documents, committee minutes, and both state and Division information security policies. We interviewed the Division's information technology staff to gain a broad understanding of information technology resources and how they are managed and utilized. We discussed how the Division interconnects and interacts with other state agencies and third party service providers.

To determine if the Division had adequate security plans, we examined its efforts at creating a statewide risk assessment to identify and prioritize the risks to state information systems and data. Next, we examined the status of information technology emergency plans for the state's primary computing facility to determine if they were up-to-date and if they had been recently tested.

In addition, we examined how the Division processes obsolete computers to ensure those computers did not contain any confidential information when they left state control. Then we reviewed the process used to handle security incidents to determine if those incidents were being properly reported, recorded, and analyzed.

To determine if controls over desktop computer security were adequate, we tested a location-based judgmental sample of 32 of the Division's desktop computers to ensure they had current virus protection as well as the latest operating system security updates. We also examined the Division's network user accounts to determine if only current employees had access to the network. We then determined if the Division's facility access card system, that is used to grant access to restricted computing facilities, was being properly administered.

To assess the security of the Division’s network servers, we tested to ensure they were configured to enforce state password standards for all accounts, they had adequate virus protection, and software security updates were installed. Web servers were scanned to identify any confidential information that might be exposed to the Internet. The security policy development process was examined to determine if it effectively addressed statewide security risks.

Finally, we reviewed the controls over sensitive data in application and database development efforts to determine if sensitive data was being properly protected.

Our audit work was conducted from January to October of 2011. 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 Administrator of the Division of Enterprise Information Technology Services. On January 5, 2012, 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 18.

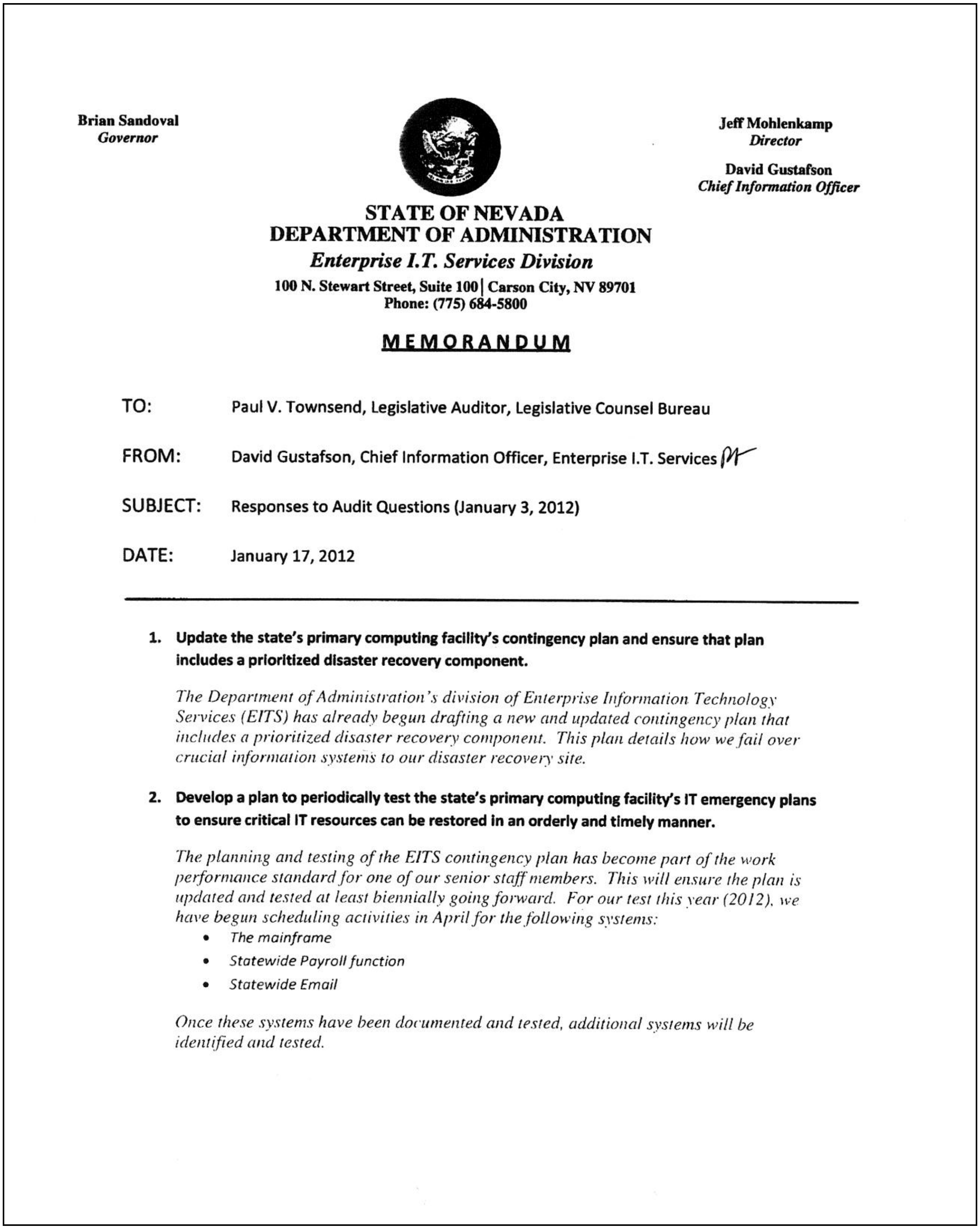
Contributors to this report included:

Jeff Rauh, CIA, CISA
Deputy Legislative Auditor

S. Douglas Peterson, CISA
IS Audit Supervisor

Appendix B

Response From the Division of Enterprise Information Technology Services



Brian Sandoval
Governor

Jeff Mohlenkamp
Director

David Gustafson
Chief Information Officer

STATE OF NEVADA
DEPARTMENT OF ADMINISTRATION
Enterprise I.T. Services Division
100 N. Stewart Street, Suite 100│Carson City, NV 89701
Phone: (775) 684-5800

MEMORANDUM

TO: Paul V. Townsend, Legislative Auditor, Legislative Counsel Bureau

FROM: David Gustafson, Chief Information Officer, Enterprise I.T. Services

SUBJECT: Responses to Audit Questions (January 3, 2012)

DATE: January 17, 2012

1. **Update the state's primary computing facility's contingency plan and ensure that plan includes a prioritized disaster recovery component.**

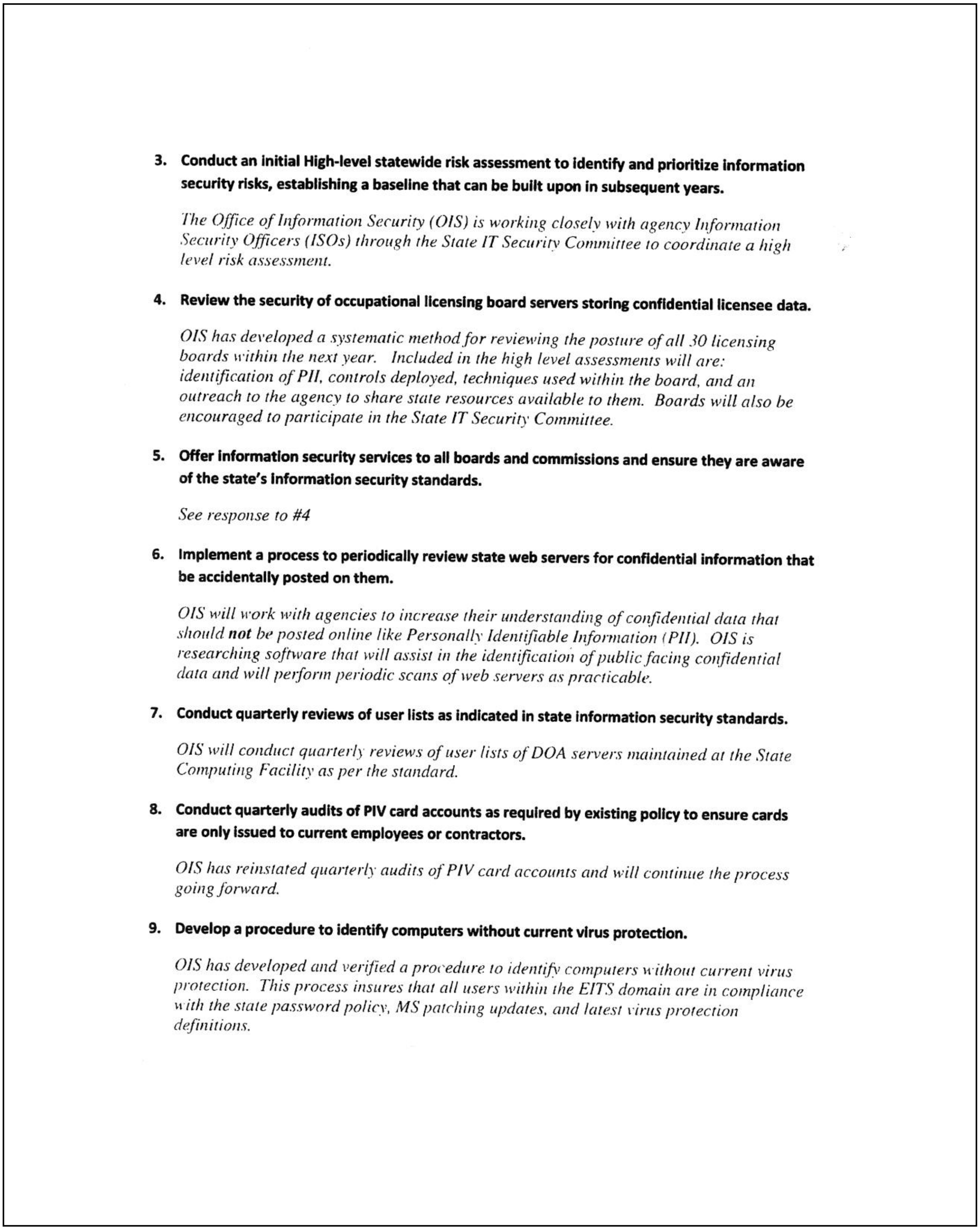
   The Department of Administration's division of Enterprise Information Technology Services (EITS) has already begun drafting a new and updated contingency plan that includes a prioritized disaster recovery component. This plan details how we fail over crucial information systems to our disaster recovery site.

2. **Develop a plan to periodically test the state's primary computing facility's IT emergency plans to ensure critical IT resources can be restored in an orderly and timely manner.**

   The planning and testing of the EITS contingency plan has become part of the work performance standard for one of our senior staff members. This will ensure the plan is updated and tested at least biennially going forward. For our test this year (2012), we have begun scheduling activities in April for the following systems:

   - *The mainframe*
   - *Statewide Payroll function*
   - *Statewide Email*

   Once these systems have been documented and tested, additional systems will be identified and tested.



3. **Conduct an initial High-level statewide risk assessment to identify and prioritize information security risks, establishing a baseline that can be built upon in subsequent years.**

   The Office of Information Security (OIS) is working closely with agency Information Security Officers (ISOs) through the State IT Security Committee to coordinate a high level risk assessment.

4. **Review the security of occupational licensing board servers storing confidential licensee data.**

   OIS has developed a systematic method for reviewing the posture of all 30 licensing boards within the next year. Included in the high level assessments will are: identification of PII, controls deployed, techniques used within the board, and an outreach to the agency to share state resources available to them. Boards will also be encouraged to participate in the State IT Security Committee.

5. **Offer information security services to all boards and commissions and ensure they are aware of the state's information security standards.**

   See response to #4

6. **Implement a process to periodically review state web servers for confidential information that be accidentally posted on them.**

   OIS will work with agencies to increase their understanding of confidential data that should ***not*** *be posted online like Personally Identifiable Information (PII). OIS is researching software that will assist in the identification of public facing confidential data and will perform periodic scans of web servers as practicable.*

7. **Conduct quarterly reviews of user lists as indicated in state information security standards.**

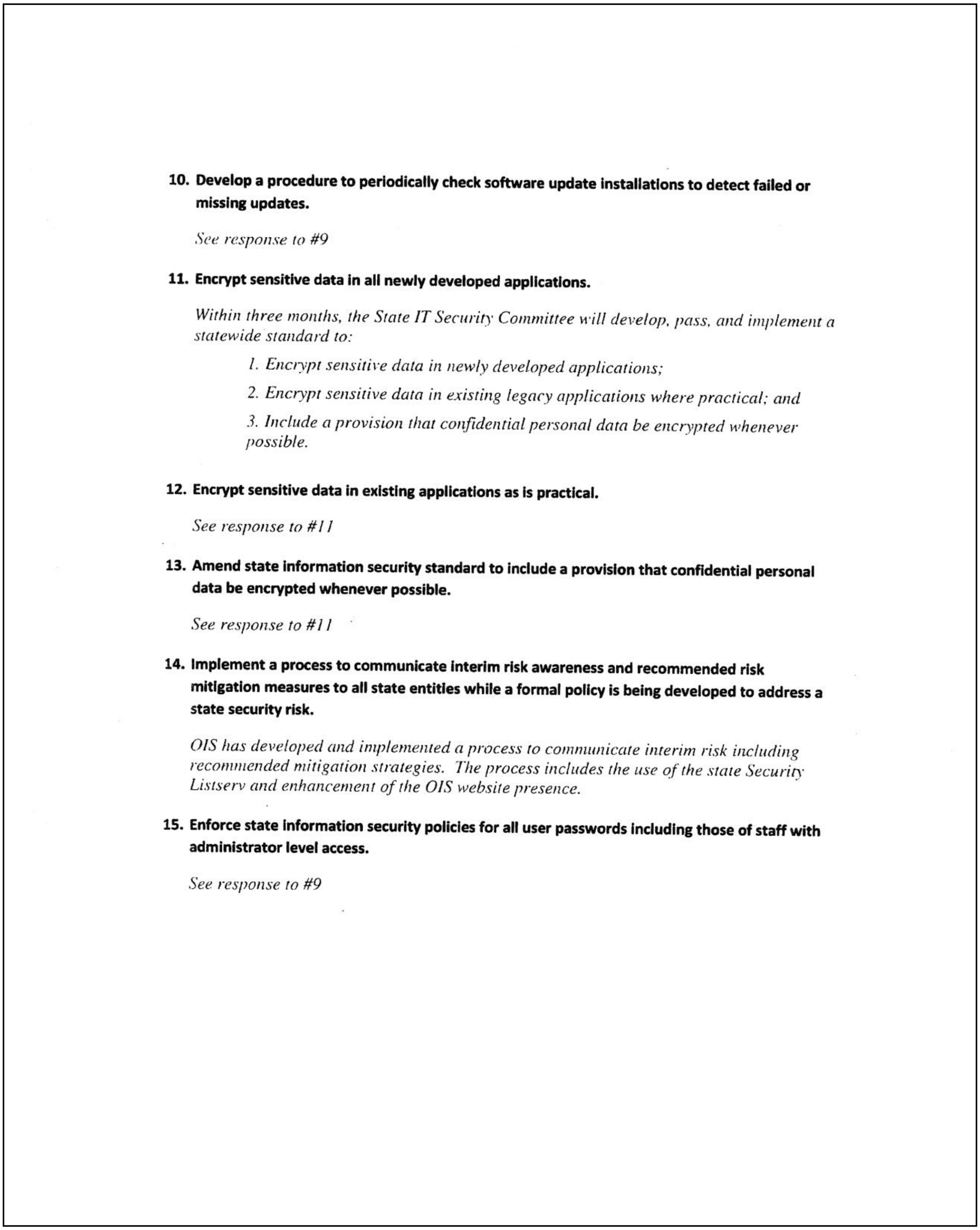
   OIS will conduct quarterly reviews of user lists of DOA servers maintained at the State Computing Facility as per the standard.

8. **Conduct quarterly audits of PIV card accounts as required by existing policy to ensure cards are only issued to current employees or contractors.**

   OIS has reinstated quarterly audits of PIV card accounts and will continue the process going forward.

9. **Develop a procedure to identify computers without current virus protection.**

   OIS has developed and verified a procedure to identify computers without current virus protection. This process insures that all users within the EITS domain are in compliance with the state password policy, MS patching updates, and latest virus protection definitions.



10. Develop a procedure to periodically check software update installations to detect failed or missing updates.

See response to #9

11. Encrypt sensitive data in all newly developed applications.

Within three months, the State IT Security Committee will develop, pass, and implement a statewide standard to:

1. Encrypt sensitive data in newly developed applications;

2. Encrypt sensitive data in existing legacy applications where practical; and

3. Include a provision that confidential personal data be encrypted whenever possible.

12. Encrypt sensitive data in existing applications as is practical.

See response to #11

13. Amend state information security standard to include a provision that confidential personal data be encrypted whenever possible.

See response to #11

14. Implement a process to communicate interim risk awareness and recommended risk mitigation measures to all state entities while a formal policy is being developed to address a state security risk.

OIS has developed and implemented a process to communicate interim risk including recommended mitigation strategies. The process includes the use of the state Security Listserv and enhancement of the OIS website presence.

15. Enforce state information security policies for all user passwords including those of staff with administrator level access.

See response to #9

The Division of Enterprise Information Technology Services' Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Update the state's primary computing facility's contingency plan and ensure the plan includes a prioritized disaster recovery component.	X	
2.	Develop a plan to periodically test the state's primary computing facility's IT emergency plans to ensure critical IT resources can be restored in an orderly and timely manner	X	
3.	Conduct an initial high-level statewide risk assessment to identify and prioritize information security risks, establishing a baseline that can be built upon in subsequent years	X	
4.	Review the security of occupational licensing board servers storing confidential licensee data	X	
5.	Offer information security services to occupational licensing boards and ensure they are aware of the state's information security standards	X	
6.	Implement a process to periodically review state web servers for confidential information that may be accidentally posted on them	X	
7.	Conduct quarterly reviews of user lists as indicated in state information security standards	X	
8.	Conduct quarterly audits of PIV card accounts as required by existing policy to ensure cards are only issued to current employees or contractors	X	
9.	Develop a procedure to identify computers without current virus protection	X	
10.	Develop a procedure to periodically check software update installations to detect failed or missing updates.	X	
11.	Encrypt sensitive data in all newly developed applications	X	
12.	Encrypt sensitive data in existing applications as is practical or as applications are upgraded	X	
13.	Amend state information security standard to include a provision that confidential personal data be encrypted whenever possible	X	

The Division of Enterprise Information Technology Services' Response to Audit Recommendations (continued)

	Recommendations	Accepted	Rejected
14.	Implement a process to communicate interim risk awareness and recommended risk mitigation measures to all state entities while a formal policy is being developed to address a state security risk	X	
15.	Enforce state information security policies for all user passwords, including those of staff with administrator level access	X	
	TOTALS	15	0