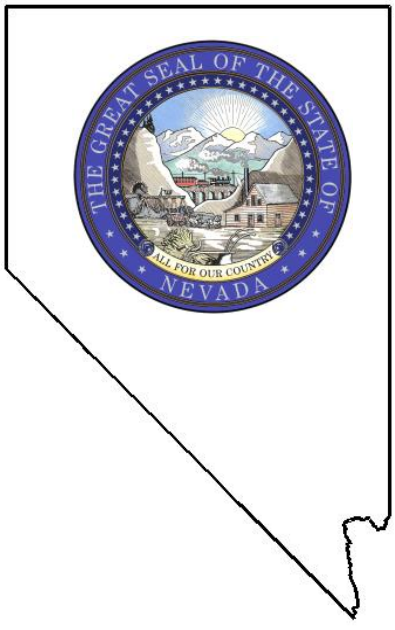
LA14-14

STATE OF NEVADA

Performance Audit

Department of Corrections
Information Technology Security

2014



Legislative Auditor
Carson City, Nevada

Audit Highlights

Highlights of performance audit report on the Department of Corrections Information Technology Security issued on April 28, 2014. Report # LA14-14.

Background

The mission of the Nevada Department of Corrections is to protect the public by confining convicted felons according to the law, while keeping staff and inmates safe. The Department currently manages 18 adult correctional institutions located throughout the State, housing approximately 13,000 inmates. These institutions include seven correctional centers (prisons), nine conservation camps, one restitution center, and one transitional housing center.

The Department's Management Information Systems (MIS) unit's mission includes keeping the Department's technology infrastructure current, providing proficient IT support staff, and providing its statewide facilities with a network infrastructure.

The MIS unit has a current staff of 25 full-time employees and is organized into an MIS Chief's office and four subordinate sections that include: 1) Applications Support, 2) Infrastructure Support, 3) Help Desk, and 4) Telecommunications.

Purpose of Audit

The purpose of this audit was to determine if the Department's information security controls were adequate to protect the confidentiality, integrity, and availability of sensitive information and information systems.

This audit included a review of information technology systems and practices at the Department of Corrections during calendar year 2013. The scope of this audit did not include certain information system controls related to the Department's Nevada Offender Tracking Information System (NOTIS) which were part of LCB audit LA14-02, issued in February 2013.

Audit Recommendations

This audit report contains six recommendations to improve information security controls. These recommendations include three recommendations to improve installation of software security updates, one recommendation to improve virus protection, and two recommendations to improve protection of information stored on photocopier hard drives.

The Department accepted the six recommendations.

Recommendation Status

The Department's 60-day plan for corrective action is due on July 23, 2014. In addition, the six-month report on the status of audit recommendations is due on January 23, 2015.

Department of Corrections Information Technology Security

Summary

The Department needs to strengthen information system controls to ensure adequate protection of information systems and the data processed therein. Software security updates were missing in desktop computers as well as in the Department's mission critical database application software that supports its inmate information system. In addition, some Department computers did not have current virus protection. State security standards require virus protection software be installed on each computer to protect from computer viruses that typically come from the Internet or infected emails. Furthermore, controls were not in place to ensure sensitive data stored in Department photocopiers are erased. This information is stored when employees make copies, FAX, scan, or print documents on these machines. This data must be deleted prior to the photocopiers being replaced or there is a risk that sensitive information could remain on the copiers' hard drives when they leave agency control.

Key Findings

Many Department desktop computers were not receiving monthly operating system security updates. We found that 52 of the 211 desktop computers tested, or 25% of our sample, had not received their Windows updates in over three months or showed large gaps between prior update installations. State security standards require agencies to begin implementing critical security patches within three working days from the date the vendor releases the software patch. Computers without current software security patches represent weaknesses in a computer network that can be exploited by a malicious entity to gain unauthorized access to a computer or computer network. (page 3)

Several database applications from Oracle were missing security updates. Similar to desktop computer operating systems, computer applications such as database software also need to be updated when software vendors issue security patches. These updates had not been installed in over 6 months. These database applications needing security updates included those supporting the Department's offender sentence calculation databases, its data warehouse, its document management database, and its Nevada Offender Tracking Information System (NOTIS). Unpatched database application software increases the risk of unauthorized access to the system's confidential data. (page 4)

Some Department computers did not have current virus protection. Eleven of the 211 computers tested, or 5% of our sample, lacked adequate virus protection. State security standards require virus protection software be installed on each computer to protect from computer viruses that typically come from the Internet or infected emails. The software needs to be periodically updated with new virus definitions. These definitions allow the software to more easily identify and protect from current virus threats. Employees whose computers do become infected will lose productive time while their computers are purged of the infected files. In addition, some malware that infects computers is capable of gaining access to sensitive information that resides on the infected computer or elsewhere on the network. (page 6)

Controls were not in place to ensure sensitive information stored in Department photocopiers is erased. This information is stored when employees make copies, FAX, scan, or print documents on these machines. This data must be deleted prior to the photocopiers being replaced or there is a risk that sensitive information could remain on the copiers' hard drives when they leave agency control. The Department does not currently have a policy or procedure that addresses the data stored on these office photocopiers. Without a policy to educate and guide staff actions, there is increased risk that confidential information will remain on these devices after they leave agency control. (page 7)

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~~

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

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

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

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830
PAUL V. TOWNSEND, *Legislative Auditor* (775) 684-6815
DONALD O. WILLIAMS, *Research Director* (775) 684-6825

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Department of Corrections Information Technology Security. This audit was conducted pursuant to the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This report includes six recommendations to improve information security controls. 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

March 18, 2014
Carson City, Nevada

Department of Corrections Information Technology Security Table of Contents

Introduction

Background

The mission of the Nevada Department of Corrections is to protect the public by confining convicted felons according to the law, while keeping staff and inmates safe. The Department currently manages 18 adult correctional institutions located throughout the State, housing approximately 13,000 inmates. These institutions include seven correctional centers (prisons), nine conservation camps, one restitution center, and one transitional housing center.

The Department's Management Information System (MIS) unit's mission includes keeping the Department's technology infrastructure current, implementing computer technologies to automate the Department's organization, providing proficient IT support staff, and providing its statewide facilities with a network infrastructure.

The MIS unit has a current staff of 25 full-time employees and is organized into an MIS Chief's office and four subordinate sections that include: 1) Application Support, 2) Infrastructure Support, 3) Help Desk, and 4) Telecommunications.

The Department of Corrections' legislatively approved budget for fiscal year 2013 was approximately $300 million and included 2,743 full-time equivalent positions.

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 systems and practices at the Department of Corrections during calendar year 2013. The objective of our audit was to determine if the Department's information security controls were adequate to protect the confidentiality, integrity, and availability of sensitive information and information systems. The scope of this audit did not include certain information system controls related to the Department's Nevada Offender Tracking Information System (NOTIS) which were part of Legislative Audit LA14-02, issued in February 2013.

Software Security Updates Were Not Installed

Software security updates were missing in desktop computers as well as in the Department's mission critical database application software that supports its inmate information system. These security updates are periodically issued by software vendors to correct errors in software code that create security vulnerabilities in their products. Organizations using that software must download and install these security patches to correct problems.

Desktop Computers Were Missing Critical Updates

Many Department desktop computers were not receiving monthly operating system security updates. Microsoft regularly issues operating system software security patches on the second Tuesday of each month, known as "patch Tuesday." Agencies using these Microsoft products must download and install these patches on computers throughout their organization to protect these computers from Internet based threats that try to exploit the unpatched systems.

We found that 52 of the 211 desktop computers tested, or 25% of our sample, had not received Windows updates in over 3 months or showed large gaps between prior update installations. For example, in one institution most desktop computers tested had not had updates installed since September 2010.

Agency staff indicated they were not able to monitor which computers were missing operating system security updates due to the lack of a desktop computer configuration management system. Staff indicated this configuration management system could provide the necessary information.

State security standards require agencies to begin implementing critical security patches within three working days from the date the vendor releases the software patch. Computers without current software security patches represent weaknesses in a

computer network that can be exploited by a malicious entity to gain unauthorized access to a computer or computer network. Without installation of critical software security patches, there is increased risk that known computer vulnerabilities will be exploited.

Database Software Was Missing Updates

Several database applications from Oracle were missing security updates. Similar to desktop computer operating systems, computer applications such as database software also need to be updated when software vendors issue security patches. These updates had not been installed in over 6 months.

These database applications needing security updates included those supporting the Department's offender sentence calculation databases. They also included the data warehouse, document management database, and Nevada Offender Tracking Information System (NOTIS).

The lack of updates had several causes including the retirement of the IT employee who regularly installed those patches. In addition, there were problems with email notifications from Oracle support notifying the IT staff of the availability of Oracle product updates. Furthermore, for its NOTIS system, the Department was using an older, unsupported Oracle product. This was due to the newer Oracle database products being incompatible with the older NOTIS software code. Unpatched database application software increases the risk of unauthorized access to the system's confidential data.

The Department has since indicated it will upgrade to newer NOTIS application software. That upgrade will allow the Department to discontinue use of the older version of the Oracle database software which is no longer supported.

Recommendations

1. Ensure critical updates to desktop computers are monitored for successful installation.
2. Ensure database software is kept current with vendor security update releases.

3. Upgrade to a more current Oracle database product when a compatible version of the NOTIS application is implemented on the Department's network.

Virus Protection Can Be Improved

Some Department computers did not have current virus protection. Eleven of the 211 computers tested, or 5% of our sample, lacked adequate virus protection. State security standards require virus protection software be installed on each computer to protect from computer viruses that typically come from the Internet or infected emails. In addition, the software needs to be periodically updated with new virus definitions. These definitions allow the software to more easily identify and protect against current virus threats.

Agency staff indicated they were not able to monitor which computers were missing current virus protection due to the lack of a desktop computer configuration management system. Staff indicated this configuration management system could provide the necessary information.

Employees whose computers do become infected will lose productive time while their computers are purged of the infected files. In addition, some malware that infects computers is capable of gaining access to sensitive information that resides on the infected computer or elsewhere on the network.

Recommendation

4. Implement a system to ensure all desktop computers have current virus protection.

Photocopiers Were Not Configured to Adequately Secure Information

Controls were not in place to ensure sensitive information stored in Department photocopiers is erased. The Department leases approximately 70 office photocopiers and has additional photocopiers that it owns installed in its facilities throughout the State. Almost all of these photocopiers contain hard drives that store information. This information is stored when employees make copies, FAX, scan, or print documents on these machines. This information is stored inside the photocopiers on internal hard drives, the same storage devices as contained in desktop computers. This data must be deleted prior to the photocopiers being replaced or there is a risk that sensitive information could remain on the copiers' hard drives when they leave agency control.

IT staff have configured some of the photocopiers on the network to overwrite their hard drives each night. However, some Department photocopiers do not have this scheduled overwrite capability and therefore cannot be configured to perform these daily overwrites of the data. In addition, some Department photocopiers with differing overwrite capabilities, such as immediate image overwrite, do not have these options enabled.

Administrative staff throughout the Department were not aware that photocopiers contain hard drives that store processed information. Nor were staff aware of the need to remove the data from the photocopiers before the photocopiers left Department and state control.

State security standards require that photocopiers be configured so data is overwritten immediately after a copy or print job is completed, thereby reducing the risk that confidential information

might remain accidentally stored on these devices. Standards also require that photocopier hard drives be removed from the photocopiers before they leave agency control.

The Department does not currently have a policy or procedure that addresses the data stored on these office photocopiers. Without a policy to educate and guide staff actions, there is increased risk that confidential information will remain on these devices after they leave agency control.

Recommendations

5. Train staff to be aware that photocopiers contain hard drives that store processed information and this information should be erased when a photocopier is replaced.
6. Implement procedures to ensure that photocopiers are configured to not store processed data as indicated in the state security standards.

Appendix A
Audit Methodology

To gain an understanding of the Department of Corrections, we interviewed Department management and staff. We reviewed budget documents, and both state and Department information security policies. We interviewed the Department's information technology staff to gain a broad understanding of the Department's information technology resources and how they are managed and utilized. We discussed how the Department interconnects with its various facilities located throughout the State.

To determine if controls over desktop computer security were adequate, we tested a judgmental sample of 211 of the Department's desktop computers. The sample was based on the location and was selected from 10 of the Department's 18 current statewide locations to ensure they had current virus protection as well as operating system security updates. As the computers were judgmentally selected, the test results cannot be projected to the total population of the Department's computers. For each computer selected we determined if an anti-virus program was installed and that the virus definitions were current. We also conducted wireless network scans at each of the 10 locations in order to determine if any unauthorized wireless networks had been established.

To assess the security of the Department's network servers we tested to ensure those devices were adequately secured in locked rooms and that they had current software security updates installed. We examined the Department's mission critical database application software that supports its NOTIS offender information system to determine if software security updates were being applied to those applications.

We interviewed administrative staff at each of the 10 locations in order to determine how they treated information contained on photocopier hard drives. In addition, we examined a judgmental sample of 11 photocopiers to review their configuration reports to determine if these copiers were configured as recommended in state security standards. The sample was based on the location and was selected from 10 of the Department's 18 current statewide locations. As the photocopiers were judgmentally selected, the test results cannot be projected to the population of the Department's photocopiers. For each photocopier selected, we tested to ensure data was immediately overwritten and hard drives removed before leaving agency control.

Our audit work was conducted from April through September 2013. 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 and 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 Director of the Department of Corrections. On February 26, 2014, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B which begins on page 11.

Contributors to this report included:

Jeff Rauh, CIA, CISA, MBA
Deputy Legislative Auditor

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

Appendix B

Response From the Department of Corrections

Board of State
Prison Commissioners

BRIAN SANDOVAL
Governor
CATHERINE CORTEZ MASTO
Attorney General
ROSS MILLER
Secretary of State

STATE OF NEVADA
DEPARTMENT OF CORRECTIONS

Northern Administration
5500 Snyder Avenue, Carson City, NV 89702
Phone: (775) 887-3285 - Fax: (775) 887-3138

Southern Administration
3955 W. Russell Road, Las Vegas, NV 89118
Phone: (702) 486-9938 - Fax: (702) 486-9961

BRIAN SANDOVAL
Governor

JAMES G. COX
Director

Scott K. Sisco
Deputy Director,
Support Services

March 6, 2014

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

Dear Mr. Townsend:

The Nevada Department of Corrections (NDOC) would like to thank you and your staff for the professionalism and courtesies extended to Department staff in the recent audit of the Department of Corrections, Information Technology Security. NDOC has accepted all six of the recommendations of the audit report. Pursuant to NRS 218G.230 (1) the following provides our written statement/explanation of the audit findings.

Recommendation # 1: Ensure critical updates to desktop computers are monitored for successful installation.

Response: NDOC has upgraded the centralized update deployment system. This system automates the deployment of patches to all desktop computers on the network. Included in this system is the ability to view the status of updates on all desktop computers. Staff have been trained and assigned on duties to monitor the status of the update process, and address issues when a desktop computer is reported as not up to date.

Recommendation # 2: Ensure database software is kept current with vendor security update releases.

Response: Staff has registered with the database vendors to receive notifications when security updates are released. Part of staff's duties is to handle these notifications and periodically check the Vendor's site for updates. Once an update is released they will update all the database software with the security updates.

Recommendation # 3: Upgrade to a more current Oracle database product when a compatible version of the NOTIS application is implemented on the Department's network.

Response: NDOC is working on updating the NOTIS application as provided for in the 2013 Legislative Session. As part of this, the Oracle database will be brought up to the Oracle 11g level. Currently the schedule is to bring the upgraded NOTIS into production in mid-2014 (calendar).

Recommendation # 4: Implement a system to ensure all desktop computers have current virus protection.

Response: NDOC has upgraded our anti-virus deployment software. This new software has the ability to push updates to all desktop computers on the network. Included in this system is the ability to view the status of updates on all desktop computers. Staff have been trained and assigned duties to monitor the status of the update process and address issues when a desktop computer is reported as not up to date.

Recommendation # 5: Train staff to be aware that photocopiers contain hard drives that store processed information and this information should be erased when a photocopier is replaced.

Response: This issue has been discussed with all members of the team. Additionally, Department Policy has been updated to require erasure and/or removal of the hard disk before it leaves NDOC.

Recommendation # 6: Implement procedures to ensure that photocopiers are configured to not store processed data as indicated in the state security standards.

Response: Department Policy has been updated to require erasure and/or removal of any hard disk before any photocopier leaves NDOC. All photocopiers that have the ability to erase data after each use have been configured to do so. Staff has been trained to verify this setting upon installation or service of the photocopiers.

If I can be of any further assistance, please contact me.

Sincerely,

James G. Cox, Director
Nevada Department of Corrections

JGC/sks

Department of Corrections
Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Ensure critical updates to desktop computers are monitored for successful installation.....	X	
2.	Ensure database software is kept current with vendor security update releases.....	X	
3.	Upgrade to a more current Oracle database product when a compatible version of the NOTIS application is implemented on the Department's network.....	X	
4.	Implement a system to ensure all desktop computers have current virus protection.	X	
5.	Train staff to be aware that photocopiers contain hard drives that store processed information and this information should be erased when a photocopier is replaced	X	
6.	Implement procedures to ensure that photocopiers are configured to not store processed data as indicated in the state security standards.....	X	
	TOTALS	6	0