# 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.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

# 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)