Audit Highlights

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

Background

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

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

Purpose of Audit

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

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

Audit Recommendations

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

The Department of Transportation accepted the eight recommendations.

Recommendation Status

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

Information Security

Department of Transportation

Summary

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

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

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

Key Findings

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

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

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

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

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