

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)