Audit Highlights

Highlights of performance audit report on the Nevada Department of Wildlife, Information Security issued on October 18, 2016. Legislative Auditor report # LA16-17.

Background

The mission of the Nevada Department of Wildlife (Department) is to protect, preserve, manage, and restore wildlife and its habitat for the aesthetic, scientific, educational, recreational, and economic benefits to citizens of Nevada and the United States, and to promote the safety of the persons using vessels on the waters of Nevada.

The Department has eight office locations statewide with one in Elko, Ely, Fallon, Henderson, Las Vegas, Winnemucca, and two offices in Reno.

The Department has three information technology employees who provide support for these various statewide locations.

For fiscal year 2016, the Department was authorized 249 full-time employees statewide. In addition, the Department had authorized expenditures of over $61 million during 2015.

Purpose of Audit

The purpose of our audit was to determine if the Department has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems. The audit focused on the systems and practices in place from December 2015, through June of 2016.

Audit Recommendations

This audit report contains four recommendations to improve the security of the Department's information systems.

The Department accepted the four recommendations.

Recommendation Status

The Department's 60-day plan for corrective action is due on January 19, 2017. In addition, the six-month report on the status of audit recommendations is due on July 19, 2017.

Information Security

Nevada Department of Wildlife

Summary

The Department can improve its information security controls in several areas. The Department needs to improve security over laptop computers. The computers of 43 game wardens contain confidential, unencrypted information such as credit card information. In addition, all of the Department's 17 servers lacked virus protection software. Without current virus protection software, servers could become infected with malware such as computer viruses. Furthermore, a faulty antivirus software installation prevented the Department from monitoring the status of virus protection on many computers. Finally, we identified 95 Department staff who had not completed their annual security awareness training. State security standards require all employees to have security awareness training at least annually.

Key Findings

Each of the Department's 43 game wardens in the Law Enforcement Division have a laptop computer containing unencrypted confidential information. This confidential information can contain unencrypted Personal Identifying Information (PII). For example, some case files contain driver's license numbers and credit card or other payment information. State Security Standards require that all sensitive information, including PII, be encrypted. (page 6)

All of the Department's 17 servers lacked virus protection software. State security standards require all computer systems to have current virus protection software installed. Without current virus protection software installed, servers could become infected with malicious software. According to the agency, when they converted to the Enterprise Information Technology Services, Enterprise Symantec Endpoint Protection (SEP) rollout, the rollout included virus protection software licenses for desktop and laptop computers, but not for servers. Therefore, the Department's servers were without virus protection. (page 7)

The Department's Information Technology (IT) support staff could not monitor the status of virus protection of many of the computers on the network. This was caused by faulty installation of software on at least 71 desktop computers. The faulty software installation prevented these computers from communicating with the virus protection management console that is used by IT staff to monitor the virus protection status of computers on its network. The information provided by the management console allows the IT staff to intervene when the virus protection software, or the daily virus definition updates, malfunction. The Department's IT staff were not aware of the failed software installations until our audit identified two computers without virus protection that did not appear on their virus protection management console. During inquiry as to why these two computers did not show up on the management console, the larger virus protection software installation problem was identified. This faulty installation affected at least 71 of the 220 computers on the Department's network. A small number of these 71 computers were missing virus protection software. (page 8)

We identified 95 of 236 current Department staff had not completed their annual security awareness training. State security standards require all state employees to have security awareness refresher training at least annually. State employees receive annual IT security awareness training to ensure they remain aware of current security threats as well as to understand their responsibility to keep state information confidential. Without completing such training, there is a greater risk that employees will not properly protect the information and information systems to which they have access. Department staff indicated that some employees did not heed the email notification to take the training. In addition, they indicated that other employees, who typically work in field locations without internet access, have a more difficult time conducting the web-based training. The Department should consider having its seasonal employees, who frequently use state computers, also take this training. (page 10)

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