

# STATE OF NEVADA

---

## Performance Audit

Nevada Department of Wildlife  
Information Security  
2016



Legislative Auditor  
Carson City, Nevada

---

# 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)

STATE OF NEVADA  
LEGISLATIVE COUNSEL BUREAU

LEGISLATIVE BUILDING  
401 S. CARSON STREET  
CARSON CITY, NEVADA 89701-4747

LEGISLATIVE COMMISSION (775) 684-6800  
MICHAEL ROBERSON, *Senator, Chairman*  
Rick Combs, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821  
PAUL ANDERSON, *Assemblyman, Chairman*  
Cindy Jones, *Fiscal Analyst*  
Mark Krmptic, *Fiscal Analyst*



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

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830  
ROCKY COOPER, *Legislative Auditor* (775) 684-6815  
SUSAN E. SCHOLLEY, *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 Nevada Department of Wildlife, Information 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 four recommendations to improve the security of the Department's information systems. 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,

A handwritten signature in black ink, appearing to read "Rocky Cooper".

Rocky Cooper, CPA  
Legislative Auditor

September 14, 2016  
Carson City, Nevada

# Nevada Department of Wildlife Information Security Table of Contents

Introduction .....	1
Background .....	1
Scope and Objective .....	5
Sensitive Information Needs Stronger Protection .....	6
Servers Were Missing Virus Protection .....	7
Virus Protection System Was Unable To Monitor Many Computers .....	8
Some Staff Did Not Complete Their Annual Security Awareness Training .....	10
Appendices	
A. Audit Methodology .....	11
B. Response From the Nevada Department of Wildlife .....	13

# Introduction

## Background

The mission of the Nevada Department of Wildlife 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 is subdivided into seven divisions with the following functions:

- Conservation Education: The Conservation Education Division works to promote Department programs, services, and recreational opportunities. The Division educates the public about state wildlife and boating rules and regulations, as well as other wildlife, habitat and fishing issues. The Division also strives to involve students, teachers, and the public through hunter, angler, and wildlife education programs. Additionally, the Division has developed a volunteer program to provide the public a hands-on way to get involved in projects such as seed gathering or fish stocking.
- Fisheries: The Fisheries Division works to ensure the health and vitality of Nevada's fish in its network of streams, rivers, lakes, and reservoirs. Hatcheries produce and stock fish. Biologists manage fish and amphibian populations, water quality, and aquatic habitat.
- Game: The Game Division is responsible for management, protection, research, and monitoring of wildlife classified as game mammals, upland and migratory

game birds, and furbearing mammals. The Division has four program areas: avian and terrestrial game species management, game wildlife/depredation control, predator management, and wildlife health and disease monitoring.

- Habitat: The Habitat Division's main objective is to ensure that Nevada wildlife habitats are productive and in good ecological condition. In addition, the Division is responsible for reviewing, assessing, and providing comments on all proposed land and water uses, providing fish and wildlife data to all entities for planning and decision-making purposes. The Habitat Division is also responsible for planning, operating, and maintaining approximately 120,000 acres of state-owned lands administered as Wildlife Management Areas (WMA's). The Division is also responsible for administering the water development, rangeland, and wildfire rehabilitation efforts for the Department. Additionally, duties include regulatory responsibility for Industrial Artificial Pond permitting (primarily the nearly 100 Nevada gold mining operations) statewide.
- Law Enforcement: The Law Enforcement Division is responsible for protecting Nevada's wildlife resources and ensuring the safety of the boating public, which includes enforcing the provisions of the Nevada Revised Statutes and all other regulations that affect wildlife issues. Support activities of this Division include implementing Operation Game Thief and providing warden training, public assistance, and radio communications. In 2000, Nevada's 35 game wardens handled patrol duties over the entire area of the state; approximately 110,000 square miles. Most wardens patrol an area of 3,235 square miles, while a few are responsible for patrol areas of nearly 10,000 square miles.
- Operations: The Operations Division is responsible for the business affairs of the Department which include the management of the customer service programs comprised of licensing, boat titling and registration; application hunts;

special licenses and permits; land agent activities; engineering services; computer and networking services; and statewide building maintenance. The Operations Division is also responsible for the Department's aviation program.

- Wildlife Diversity: The Wildlife Diversity Division compiles data on the abundance and distribution of many of the less well-known wildlife species of Nevada. The Division has taken historical wildlife records, records of scientifically collected specimens, records of commercially collected specimens, and other wildlife related data and created several large databases. These databases are distributed to biologists around the state and shared with other agencies to help everyone make well-informed decisions on the management of natural resources.

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.

Exhibit 1 shows a summary of Department's fiscal year 2015 revenues and expenditures.

<b>Revenues and Expenditures Fiscal Year 2015</b>	<b>Exhibit 1 Amount</b>
<b>Revenues</b>	
State Appropriations	\$ 494,765
Beginning Funds	28,638,529
Fuel Tax	1,216,475
Assessments	465,920
Federal Grants	15,508,493
Licenses & Fees	17,188,385
Other Revenues <sup>1</sup>	7,075,330
Interagency Transfers	18,648,211
Transfer From Other State Agencies	878,312
<b>Total Revenues</b>	<b>\$90,114,420</b>
<b>Expenditures</b>	
Personnel	\$18,048,611
Operating <sup>2</sup>	218,715
Equipment	1,400,816
Program Costs	40,828,409
Information Services	256,052
State Cost Allocations & Assessments	614,270
<b>Total Expenditures</b>	<b>\$61,366,873</b>
<b>Difference</b>	<b>\$28,747,547</b>
Less: Reversion to General Fund	(6,800)
<b>Balance Forward to 2016</b>	<b>\$28,740,747</b>

Source: State accounting system.

<sup>1</sup> Other revenues include sales, fines, cost allocations, gifts/donations, interest, and other miscellaneous revenue.

<sup>2</sup> Operating costs include travel, buildings and grounds, and other operating expenditures.



**Scope and Objective**

The scope of our audit focused on the systems and practices in place from December 2015 through June of 2016.

Our audit objective 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.

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.

# Sensitive Information Needs Stronger Protection

Each of the Department's 43 game wardens in the Law Enforcement Division have a laptop computer containing unencrypted confidential information. This confidential information, including legal case files, can be related to law enforcement activities such as illegal hunting, fishing, trapping, violating boater safety laws, and other activities under the Division's scope of law enforcement authority. The case files 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.

If one of the Law Enforcement Division's laptops were lost or stolen, state law requires that the individuals whose PII has been disclosed to be notified. In addition, the State may be required to notify national credit bureaus of the identity information breach. Furthermore, the legal cases themselves could also become compromised.

The Division had previously discussed encrypting these laptop hard drives. However, they felt there was a substantial risk a laptop user would occasionally forget his disk encryption password and all the data on that laptop's hard drive would no longer be accessible. However, after discussing a laptop encryption methodology that minimizes the risks of forgotten encryption passwords, the Department agreed to encrypt its laptops.

## **Recommendation**

1. Encrypt all Department laptop computers containing sensitive information.

# Servers Were Missing Virus Protection

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. Servers represent a computing resource that is shared by the entire Department. When a server becomes infected with malware, or otherwise compromised, the productivity of the entire Department could be affected and the security of the information on the server could be compromised.

According to the agency, when they converted to the Enterprise Information Technology Services (EITS), 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 other than being positioned behind the State's firewall and being configured to not accept any external network traffic.

During our audit, EITS began making SEP server virus protection software available and Department has installed the software on all its servers.

## **Recommendation**

2. Periodically check all Department servers to ensure they have current virus protection.

# Virus Protection System Was Unable To Monitor Many Computers

The Department's Information Technology (IT) support staff could not monitor the status of virus protection of many of the computers on the Department 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 was 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.

State Security Standards require all computers have current virus protection software installed to reduce the risk of malware infecting state computers.

### **Recommendation**

3. Ensure all Department computers have current virus protection software by periodically comparing the number of computers listed in the virus protection system to the number of staff currently assigned to a location and investigate any discrepancies.

# Some Staff Did Not Complete Their Annual Security Awareness Training

We identified 95 of 236 current Department staff who 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.

## **Recommendation**

4. Periodically reinforce the importance of all Department employees completing their required annual IT security awareness training.

# Appendix A

## Audit Methodology

To gain an understanding of the Nevada Department of Wildlife, we interviewed Department's management and staff. In addition, we reviewed related statutes and regulations. We also reviewed financial information, budgets, legislative committee minutes, and other information describing the Department's activities. Furthermore, we assessed internal controls over the security of computers, computer users, servers, confidential information, and networking.

To determine if controls over desktop computer security were adequate, we examined 153 of the 220 computers on the Department's network in eight different locations across the state. We tested these computers to ensure they had current virus protection and to ensure they were receiving their operating system security patches on a regular basis.

We examined the Department's population of 236 network user accounts to determine if only current employees had access to the computer network. In addition, we determined if all currently assigned Department employees had conducted their annual Information Technology security awareness training.

We examined the security of the server rooms at the eight locations we visited to ensure the equipment contained in them was adequately secured. To assess the security of the Department's 17 servers, we tested to ensure they were protected with virus protection software and that they had appropriate operating system software updates installed timely. We verified that any wireless networks used by the Department were authorized and had proper security controls in place. We reviewed the security of confidential personal data used and stored by the Department to ensure it was adequately protected.

Our audit work was conducted from December 2015 through May 2016. 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, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Nevada Department of Wildlife. On September 1, 2016, 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 13.

Contributors to this report included:

Jeff Rauh, CISA, CIA, MBA  
Deputy Legislative Auditor

Shirlee Eitel-Bingham  
Deputy Legislative Auditor

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



# Appendix B

## Response From the Nevada Department of Wildlife



BRIAN SANDOVAL  
Governor

STATE OF NEVADA  
**DEPARTMENT OF WILDLIFE**  
6980 Sierra Center Parkway, Suite 120  
Reno, Nevada 89511  
Phone (775) 688-1500 • Fax (775) 688-1495

TONY WASLEY  
*Director*  
LIZ O'BRIEN  
*Deputy Director*  
JACK ROBB  
*Deputy Director*

September 12, 2016

Mr. Rocky Cooper, CPA, Legislative Auditor  
State of Nevada Legislative Counsel Bureau  
Legislative Building  
401 S. Carson St.  
Carson City, NV 89701

Subject: **Performance Audit-Information Security 2016**

Dear Mr. Cooper:

The Nevada Department of Wildlife (NDOW) responses to the Performance Audit-Information Security 2016 are provided below:

1. Encrypt all Department laptop computers containing sensitive information.  
The Department accepts the Audit Recommendation.

NDOW has 43 law enforcement laptops containing encrypted confidential legal case information. These legal case files can contain Personally Identifiable Information (PII). For example, some files contain driver's license numbers and/or credit card or other payment information. NDOW Information Technology staff is finalizing our migration path to Windows 10 and will use BitLocker for encryption. As of September 2, 2016, we have 23 laptops deployed running Windows 10 with BitLocker. Staff is confident that this will be a good solution for encrypting the data on these machines.

Staff is unable to install Windows 10 on laptops purchased before 2013 because of hardware compatibility issues with these laptops. Because of these issues with older laptops we are scheduling the BitLocker rollout when employees receive their new scheduled laptop. Staff will be replacing all of the remaining laptops in fiscal year 2017.

Mr. Rocky Cooper, CPA, Legislative Auditor  
September 12, 2016

2. Periodically check all Department servers to ensure they have current virus protection.

The Department accepts the Audit Recommendation.

NDOW has one server remaining out of the 17 servers identified to roll-out to Symantec Endpoint Protection (SEP) virus protection. This remaining server is the Las Vegas server (NDOW-LV) which is scheduled to be replaced by the end of October 2016.

NDOW IT staff is now reviewing the weekly Enterprise Technology Services Division (EITS) SEP report to insure all servers are up to date with the current virus definitions. Staff will continue to monitor all servers weekly to insure SEP is current and working properly.

3. Ensure all Department computers have current virus protection software by periodically comparing the number of computers listed in the virus protection system to the number of staff currently assigned to a location and investigate any discrepancies.

The Department accepts the Audit Recommendation.

NDOW information technology (IT) staff did not have visibility on all agency computers in SEP. Most NDOW computers did have antivirus installed and were up to date. However, after the original install of SEP some of NDOW's computers were not visible in SEP. Most had antivirus software installed and current definition files. All of NDOW computers are now in SEP and staff has visibility on them.

NDOW IT staff is now reviewing the weekly Enterprise Technology Services Division (EITS) SEP report to insure all computers are up to date with the current virus definitions. Staff will continue to monitor all servers weekly to insure SEP is current and working properly.

4. Periodically reinforce the importance of all Department employees completing their required annual IT security awareness training.

The Department accepts the Audit Recommendation.

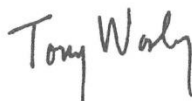
All employees have been sent email notifications that they need to complete this training by November 1, 2016. However some have not completed the training as requested. Along with the email notifications, each new employee received a new hire orientation packet which is similar to an employee handbook. In this booklet it lists the required courses each employee needs to complete. Some employees are in seasonal positions or are in positions that require them to be out in the field without computer or internet access for weeks at a time. This prevents them from completing the course(s) in a timely manner.

Mr. Rocky Cooper, CPA, Legislative Auditor  
September 12, 2016

The Department's plans regarding the training shortfall is to have the supervisors give more direction and delegate the requirements of trainings in a more routine and consistent manner throughout the year.

If you have any questions or need further information, please contact Deputy Director Liz O'Brien at (775) 688-1982.

Sincerely,

A handwritten signature in black ink that reads "Tony Wasley". The signature is written in a cursive, slightly slanted style.

Tony Wasley  
Director

Attachment

cc: Deputy Director Liz O'Brien  
Deputy Director Jack Robb  
Information Technology Professional Pat Wlodarczyk

## Nevada Department of Wildlife's Response to Audit Recommendations

<u>Recommendations</u>	<u>Accepted</u>	<u>Rejected</u>
1. Encrypt all Department laptop computers containing sensitive information.....	<u>    X    </u>	<u>          </u>
2. Periodically check all Department servers to ensure they have current virus protection. ....	<u>    X    </u>	<u>          </u>
3. Ensure all Department computers have current virus protection software by periodically comparing the number of computers listed in the virus protection system to the number of staff currently assigned to a location and investigate any discrepancies. ....	<u>    X    </u>	<u>          </u>
4. Periodically reinforce the importance of all Department employees completing their required annual IT security awareness training. ....	<u>    X    </u>	<u>          </u>
TOTALS	<u>    4    </u>	<u>          </u>