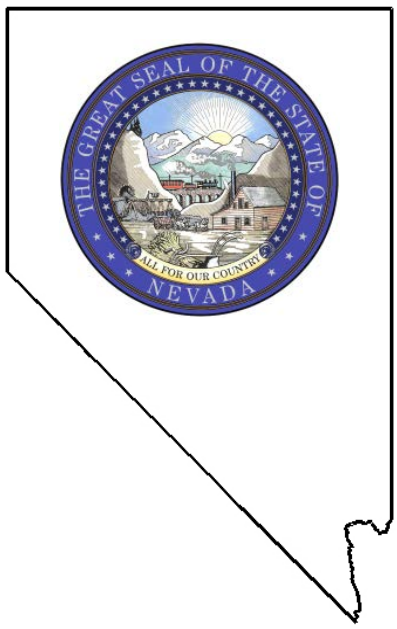
STATE OF NEVADA

Performance Audit – Addendum

Department of Public Safety
Records, Communications and Compliance Division

Information Security – Servers
LA18-12A

Operating System and Database Application Software



Legislative Auditor
Carson City, Nevada

STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747
Fax No.: (775) 684-6600

Legislative Commission
Legislative Building
Carson City, Nevada

This report addendum (LA18-12A) contains supplemental findings, conclusions, and recommendations from our performance audit of the Department of Public Safety's Records, Communications and Compliance Division, Information Security (LA18-12). We issued that report on January 17, 2018. The audit was conducted pursuant to the ongoing program of the Legislative Auditor as authorized by the Legislative Commission, and was made pursuant to provisions of Nevada Revised Statutes 218G.010 and 218G.350.

An addendum to report LA18-12 was necessary because security vulnerabilities existed in certain information systems within the Records, Communications and Compliance Division. Providing details regarding those vulnerabilities, at the time we published the original report, would have unnecessarily exposed those information security weaknesses. Since the Division has performed sufficient corrective actions, we are issuing this addendum as a supplement to our original report. Readers are encouraged to refer to report LA18-12 and this report addendum to gain a complete and comprehensive understanding of the audit's scope and objective, findings, recommendations, and methodology.

This addendum includes four additional recommendations to improve the security of the Division's servers. 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,

Daniel L. Crossman, CPA
Legislative Auditor

May 7, 2020
Carson City, Nevada

Addendum to Audit Report LA18-12

Server Software Lacked Critical Security Updates

Many of the Records, Communications and Compliance Division's (Division) servers had critical security vulnerabilities due to outdated and unsupported software. The Division did not ensure that operating systems and database application software were upgraded to supported versions in a timely manner. As software becomes outdated, the Division can no longer rely on security updates or technical support to keep software current. Knowing key dates in a software asset lifecycle plan ensures an organization makes informed decisions about when to upgrade or make other changes to its software. Without proper software upgrade planning, the Division compromises security, performance, and overall efficiency.

As of August 2016, 19 of the Division's 97 servers were running outdated Windows operating system software with critical security vulnerabilities. Also, seven of the servers were running outdated Oracle database software. There were no current security updates available, as the vendors no longer supported the versions of software installed.

The Division maintains information such as the sex offender registry, criminal history, and point-of-contact firearm information on its systems. Considering the criticality of the information, keeping software current is vital, as this mitigates security risks. The Division could have identified software vulnerabilities in a timely manner through a current software inventory and routine scans, which it did not. Conducting vulnerability scans on a frequent basis identifies vulnerabilities and prioritizes them on each system. The Division had controls in place such as security awareness training, network segmentation, and encrypted communications intended to prevent unauthorized access; however, the controls did not fully mitigate the vulnerabilities.

State security standards require operating systems that reach its end-of-life must be upgraded, application software be current with updates, and vulnerability scans be conducted on existing state systems and networks to identify areas of risk at least annually. Additionally, state standards require security exceptions be placed on file with the Office of Information Security, Division of Enterprise Technology Services (EITS) for justification of noncompliance with security policies and standards. The Division did not file security exceptions for any of its outdated software.

The Division indicated oversight lapsed as an unintentional consequence of the 2013 reorganization through which many Division information technology staff were consolidated under EITS. Three information security officers were retained to provide oversight of the Division's information technology functions. Regardless, it is the Division's responsibility to ensure software is maintained, upgraded, and outlined in a server software asset lifecycle plan. In response to the original audit report, LA18-12, a service-level agreement was completed and signed between the Division and EITS to ensure information technology operations and responsibilities are clarified.

Recommendations

1. Develop and maintain a division-wide server software asset lifecycle plan.
2. Develop policies and procedures to routinely verify servers are receiving operating system and database software critical updates.
3. Develop policies and procedures to ensure vulnerability scanning of servers is conducted at least annually to assist in identifying areas of risk.
4. Coordinate efforts with EITS to ensure operating system and database software are upgraded timely to current supported versions.

Actions Taken by the Agency to Resolve the Security Vulnerabilities

After the outdated software was identified in August 2016, the Division indicated it would require time and significant resources to initiate a project charter encompassing all of the outdated software that needed upgrading. Beginning in December 2017, the Division entered into an end-of-life server software upgrade project with a dedicated EITS project manager, who served as a liaison to the Division and coordinated efforts. This project involved comingled systems between various Department of Public Safety divisions, with varying degrees of integration between servers, databases, and applications. These systems are critical to ensuring the protection of Nevada citizens, visitors, and sworn law enforcement officers.

Over the course of the audit, we conducted monthly meetings to obtain status reports and monitor the progress of system and software upgrades. EITS successfully completed upgrading all of the Division's servers' software to current, vendor-supported versions in March 2020.

Methodology

To assess the logical security controls of all of the Division's 97 servers, we tested to ensure they were protected with current antivirus, operating system, and database application software updates. Based on the results of this test work and identifying outdated software, we conducted monthly meetings with EITS staff, project managers, and Division IT staff and management to follow the end-of-life server software upgrade project's progress. Additionally, we examined the server rooms housing the Division's equipment for physical security including adequate access controls, effective temperature monitoring controls, and after-hours automated notifications.

Our audit work was conducted from June 2016 to March 2020 as we continued to monitor the Division's progress in mitigating the vulnerabilities found early on in the audit cycle. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with Nevada Revised Statutes (NRS) 218G.230, we furnished a copy of our preliminary report addendum to the Records, Communications and Compliance Division. On April 27, 2020, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report addendum. That response begins on page 5.

Statutorily Required Corrective Action and Follow-Up

The four recommendations on page 2 are in addition to the ten issued in the original report (LA18-12) and are subject to the corrective action and follow-up requirements outlined in NRS 218G.250 and 218G.270. The Division's 60-day plan for corrective action on the four recommendations in this addendum is due on December 3, 2020, and the 6-month report on the status of audit recommendations is due on June 3, 2021.

Contributors to this report included:

Shirlee Eitel-Bingham, CISA
Deputy Legislative Auditor

Sarah Gasporra, BBA
Deputy Legislative Auditor

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

Shannon Riedel, CPA
Chief Deputy Legislative Auditor

Response From the Records, Communications and Compliance Division

Steve Sisolak
Governor

Nevada Department of
Public Safety
DEDICATION PRIDE SERVICE

George Togliatti
Director

Sheri Brueggemann
Deputy Director

Mindy McKay
Division Administrator

Records, Communications and Compliance Division
333 West Nye Lane, Suite 100
Carson City, Nevada 89716
Telephone (775) 684-6262 - Fax (775) 687-3289

May 4, 2020

Daniel L. Crossman, CPA
Legislative Auditor
Legislative Counsel Bureau
401 S. Carson Street
Carson City, NV 89701-4747

Dear Mr. Crossman,

This letter constitutes a written statement of explanation to the audit report addendum dated April 22, 2020 attached. Specifically, the addendum (LA18-12A) contains supplemental findings, conclusions, and recommendations from the Legislative Counsel Bureau's performance audit of the Department of Public Safety's Records, Communications and Compliance Division (RCCD), Information Security (LA18-12). The addendum includes four (4) recommendations to improve the security of the division's servers which the division has accepted. Below is a brief status on each recommendation.

Recommendation 1: Develop and maintain a division-wide server software asset lifecycle plan.

Response: RCCD accepts this recommendation.

A plan is being written by the Department's Information Security Officer which should be ready for review by mid-May and implementation shortly thereafter.

Recommendation 2: Develop policies and procedures to routinely verify servers are receiving operating system and database software critical updates.

Response: RCCD accepts this recommendation.

Draft policies and procedures are being developed by the Department's Information Security Officer which should be ready for review by mid-May and implementation shortly thereafter.

Recommendation 3: Develop policies and procedures to ensure vulnerability scanning of servers is conducted at least annually to assist in identifying areas of risk.

Response: RCCD accepts this recommendation.

Draft policies and procedures are being developed by the Department's Information Security Officer which should be ready for review by mid-May and implementation shortly thereafter.

Recommendation 4: Coordinate efforts with EITS to ensure operating system and database software are upgraded timely to current supported versions.

Response: RCCD accepts this recommendation.

The existing Service Level Agreement between EITS and DPS will be amended to include the requirement for EITS to ensure all operating system and database software is upgraded timely to current supported versions.

The division appreciates this opportunity to improve its information security posture. It has been a pleasure working with everyone at LCB during this audit. I appreciate everyone's professionalism, guidance and patience. We look forward to a formal audit closure. Please contact me if you require anything further.

Respectfully,

Mindy McKay, Administrator and CJIS Systems Officer
Records, Communications and Compliance Division

Cc: Shirlee Eitel-Bingham, LCB Deputy Legislative Auditor
Sarah Gasporra, LCB Deputy Legislative Auditor
George Togliatti, DPS Director
Sheri Brueggemann, DPS Deputy Director
Curtis Palmer, DPS Senior Fiscal Officer
Shaun Rahmeyer, DPS Office of Cyber Defense Coordination Administrator
Charlene Boegle, DPS Administrative Services Officer
Tom Dorsey, DPS Information Security Officer

Records, Communications and Compliance Division's Response to Addendum Recommendations

	Recommendations	Accepted	Rejected
1.	Develop and maintain a division-wide server software asset lifecycle plan	X	
2.	Develop policies and procedures to routinely verify servers are receiving operating system and database software critical updates	X	
3.	Develop policies and procedures to ensure vulnerability scanning of servers is conducted at least annually to assist in identifying areas of risk	X	
4.	Coordinate efforts with EITS to ensure operating system and database software are upgraded timely to current supported versions	X	
	TOTALS	4	