Secretary of State
Oregon Audits Division

Oregon Liquor Control Commission

Recommendation Follow-up Report: Cannabis Information Systems Properly Functioning but Monitoring and Security Enhancements are Needed

May 2019
Report 2019-23

Secretary of State Bev Clarno
Audits Division Director Kip Memmott

Secretary of State
Report Highlights

May 2019

Oregon Liquor Control Commission
Recommendation Follow-up Report: Cannabis Information Systems Properly Functioning but Monitoring and Security Enhancements are Needed

Recommendation Follow-Up Results

Since our audit, the Oregon Liquor Control Commission (OLCC) has taken substantial steps to improve the state's recreational marijuana program and the information systems that support it. Management implemented processes to improve marijuana regulation and information system controls, including risk-based and proactive inspections, reconciliation processes, and managing users' access to information technology (IT) systems. The agency is working with the Cannabis Tracking System vendor to improve system functionality and update security requirements.

While OLCC made significant progress in addressing our audit recommendations, ongoing effort is necessary to fully implement or resolve them all. Moreover, opportunities exist for increased maturity of recreational marijuana regulation processes and IT security.

Status of Recommendations

Recommendations agency agreed with	**17**
Recommendations fully implemented since the initial audit	**10**
Recommendations partially implemented	**5**
Recommendations not implemented	**2**
Total recommendations made	**17**

Highlights from the Original Audit

Although OLCC had taken positive steps to establish information systems for recreational marijuana regulation, we identified several weaknesses associated with the new systems for marijuana licensing and tracking. They included data reliability issues and insufficient processes for managing marijuana applications and vendors. In addition, OLCC had not implemented an appropriate agencywide IT security management program. We identified eight IT security issues that significantly increased the risk that OLCC's computer systems could be compromised, resulting in a disruption of OLCC business processes.

Background and Purpose

In 2014, voters approved Measure 91, which legalized the production, sale, and use of recreational marijuana in Oregon. To help regulate and support this new industry, OLCC implemented the Marijuana Licensing System and the Cannabis Tracking System. Our original audit reviewed and evaluated key general computer controls governing OLCC's IT security management program and application controls over the Cannabis Tracking and Marijuana Licensing Systems. The purpose of this follow-up report is to provide a status on the auditee's efforts to implement the audit recommendations.

Introduction

The purpose of this report is to follow up on the recommendations we made to the Oregon Liquor Control Commission (OLCC) as included in audit report 2018-07, "Cannabis Information Systems Properly Functioning but Monitoring and Security Enhancements are Needed."

The Oregon Audits Division conducts follow-up procedures for each of our performance audits. This process helps assess the impact of our audit work, promotes accountability and transparency within state government, and ensures audit recommendations are implemented and related risks mitigated to the greatest extent possible.

We use a standard set of procedures for these engagements that includes gathering evidence and assessing the efforts of the auditee to implement our recommendations; concluding and reporting on those efforts; and employing a rigorous quality assurance process to ensure our conclusions are accurate. We determine implementation status based on an assessment of evidence rather than self-reported information. This follow-up is not an audit, but a status check on the agency's actions.

To ensure the timeliness of this effort, the division asks all auditees to provide a timeframe for implementing the recommendations in our audit reports. We use this timeframe to schedule and execute our follow-up procedures.

Our follow-up procedures evaluate the status of each recommendation and assign it one of the following categories:

- **Implemented/Resolved**: The auditee has fully implemented the recommendation or otherwise taken the appropriate action to resolve the issue identified by the audit.
- **Partially implemented**: The auditee has begun taking action on the recommendation, but has not fully implemented it. In some cases, this simply means the auditee needs more time to fully implement the recommendation. However, it may also mean the auditee believes it has taken sufficient action to address the issue and does not plan to pursue further action on that recommendation.
- **Not implemented**: The auditee has taken no action on the recommendation. This could mean the auditee still plans to implement the recommendation and simply has not yet taken action; it could also mean the auditee has declined to take the action identified by the recommendation and may pursue other action, or the auditee disagreed with the initial recommendation.

The status of each recommendation and full results of our follow-up work are detailed in the following pages.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of OLCC during the course of this follow-up work.

Recommendation Implementation Status

Recommendation #1

Develop and implement standards and protocols for on-site inspections and investigations.	**Implemented/ Resolved**

OLCC implemented standards and protocols for on-site inspections and investigations in process guides. The guides provide the steps inspectors and investigators should take prior to visiting a licensee's location and while on location. They are available for wholesaler, retailer, producer, and processor site inspections. The agency began conducting proactive inspections in April 2018. As of April 2019, OLCC reported they had performed 406 inspections of marijuana producers, 72 inspections of retailers, two of wholesalers, and one of a processor.

Recommendation #2

Evaluate the need and provide for an adequate number of trained OLCC inspectors commensurate with number of licensed marijuana businesses.	**Partially implemented**

The agency requested funding for 12 additional positions in its 19-21 requested budget. However, the agency has not yet determined the total number of inspectors needed to provide adequate oversight to licensed marijuana businesses.

Recommendation #3

Perform risk-based on-site monitoring and inspections to ensure that licensees are reporting accurate information in the Cannabis Tracking System and complying with applicable laws.	**Implemented/ Resolved**

OLCC has developed some processes to assess whether licensees are reporting accurate information in the Cannabis Tracking System and complying with applicable laws. While we consider the recommendation implemented, current processes for identifying high-risk licensees are performed on an ad hoc basis and are not fully documented or standardized. The agency could further decrease risk in this area by developing more defined and repeatable processes to mitigate the risk of inaccurate reporting and noncompliance.

Recommendation #4

Develop and implement policies and procedures for effectively monitoring software as a service vendors to ensure they are meeting security and hosting requirements defined in contracts and service level agreements.	**Partially implemented**

The agency engaged with the Department of Administrative Services (DAS) Enterprise Security Office and Department of Justice to clarify the enterprise expectations regarding security and hosting services provided by third-party software as a service providers. OLCC is working with the state's Cannabis Tracking System vendor to update contract language related to security and hosting requirements.

Recommendation #5

Develop and implement reconciliation processes to ensure that data is appropriately transmitted by the Marijuana Licensing System and received by the Cannabis Tracking System.

Implemented/ Resolved

OLCC implemented an automated reconciliation process that alerts staff when there is a discrepancy between data in the Marijuana Licensing System and the Cannabis Tracking System. Agency staff then work with vendors to correct any identified discrepancies.

Recommendation #6

Establish processes for granting and reviewing access to the Marijuana Licensing System and the Cannabis Tracking System.

Implemented/ Resolved

The agency established processes to ensure that access to both systems is appropriately granted and reviewed. Additionally, OLCC now uses a ticketing system to document and track internal access requests. While the recommendation is implemented, the agency has not yet consistently adhered to the newly established process and could further decrease risk in this area by communicating expectations to management and monitoring compliance with the new procedure.

Recommendation #7

Implement change management processes in line with industry best practices, including measures that ensure test data remains segregated from the production environment.

Not implemented

Agency management chose not to implement this recommendation while they focus on replacing the Marijuana Licensing System. However, without an appropriate change management process that includes the controls to segregate test and production data, the agency will continue to be at risk that test data may be included in the production environment when implementing new systems.

Recommendation #8

Update and test OLCC's information security plan to ensure the plan reflects the agency's current business and IT environment.

Partially implemented

The agency has adopted the DAS Enterprise Security Office’s Statewide Information Security Plan. The Statewide Plan states: “Where shared responsibility exists for system, networks, applications, and information, those specific responsibilities will be articulated in the Agency Addendums section of this plan.” Although the agency shares several responsibilities with the Enterprise Security Office related to its security management program, OLCC has not created the required addenda that reflects the agency’s responsibilities.

Recommendation #9

Establish a process to maintain an up-to-date inventory of authorized hardware and software allowed on OLCCs network.	**Implemented/ Resolved**

The agency implemented multiple tools and processes to maintain an up-to-date inventory of authorized hardware and software. OLCC exceeded the recommendation by also implementing controls to ensure only authorize software is installed and allowed to run on OLCC's network.

Recommendation #10

Develop and implement a configuration management process, including establishing configuration baselines, maintaining an up-to-date repository of configuration items, and monitoring configuration status changes to detect any unauthorized changes.	**Implemented/ Resolved**

The agency has established configuration baselines, and has implemented new tools and processes to manage configurations. This includes automatically updating devices upon reconnecting to the network if they have been working off-site for a time, as well as alerting staff to unauthorized configuration changes and device settings out of compliance with established baselines.

Recommendation #11

Develop and implement a process to scan for vulnerabilities on devices on the network.	**Implemented/ Resolved**

The agency has implemented new tools and processes to scan for network vulnerabilities. Additionally, the agency works with the DAS Enterprise Security Office to monitor and mitigate newly identified vulnerabilities in OLCC's environment. Both the agency director and the Office of the State CIO receive periodic status reports detailing identified vulnerabilities and their mitigation status.

Recommendation #12

Develop and implement an effective antivirus solution on servers and workstations, and monitor to ensure all servers and workstations have an up-to-date antivirus solution.	**Implemented/ Resolved**

The agency has implemented an effective antivirus solution for servers and workstations and has tools in place for continuous monitoring to ensure the software remains up-to-date. Staff are assigned to investigate and remediate issues when a server or workstations is out of compliance or has an error when updating antivirus software.

Recommendation #13

Transition software off obsolete platforms. If that is not possible, ensure unsupported servers are appropriately segregated on the network.	**Partially implemented**

OLCC is in the process of transitioning the agency’s network and server infrastructure to the DAS Enterprise Technology Services data center. The agency has indicated that obsolete platforms will be eliminated when the move is completed.

Recommendation #14

Review physical access procedures to ensure access is appropriate, and require PINs to be periodically changed.	**Implemented/ Resolved**

OLCC disabled PIN access to areas with sensitive IT and infrastructure resources. While this action does not implement the recommendation as written, this does resolve the risk that unauthorized personnel may gain inappropriate physical access to sensitive information technology assets.

Recommendation #15

Develop and implement a process to remediate weaknesses identified in risk assessments and audits, and routinely evaluate and assess the agency’s security posture.	**Partially implemented**

The agency developed ad hoc processes for assigning responsibility and for recording actions taken and implementation status. In addition, some related processes are in place, such as vulnerability scanning (see recommendation no. 11). However, these processes are not documented in a way that would ensure findings from future audits and risk assessments are appropriately addressed.

Recommendation #16

Develop and document an entitywide disaster recovery plan.	**Not implemented**

OLCC has elected to postpone efforts to develop and document a disaster recovery plan until they have completed their transition, currently underway, to the state’s data center operated by the DAS Enterprise Security Office. This is to ensure the plan will reflect their new IT environment.

Recommendation #17

Perform periodic tests of backups to ensure usability.	**Implemented/ Resolved**

The agency updated their backup and restore procedures to include periodic testing of backup media, including tests for restoring operating systems and individual files. Tests of backups are to be performed at least quarterly.

Conclusion

OLCC has implemented new technologies and processes to address the recommendations from the original audit, including those related to vulnerability scanning, asset management, and antivirus solutions. The agency is currently in the process of transitioning its network and infrastructure to the DAS Enterprise Technology Services data center; this transition is expected to provide the agency with additional controls for physical and environmental protection, and maintenance and operation of servers. The agency has elected to postpone disaster recovery efforts until the transition is complete so that disaster recovery planning will reflect the new IT environment. Additionally, the agency has adopted the Statewide Information Security Plan published by the state's Enterprise Security Office, although additional steps are needed to develop addenda that articulate shared responsibilities for systems, networks, applications, and information, where applicable.

The agency continues to take steps to improve the state's recreational marijuana program and the information systems that support it. Management has implemented processes to improve marijuana system controls, including risk-based and proactive inspections, reconciliation processes, and system access management. OLCC is currently engaged with the state's Office of the State Chief Information Officer to pursue a new licensing information system that will replace inefficient and disjointed technology, including the current Marijuana Licensing System. The agency is working with the vendor that hosts and supports their Cannabis Tracking System to improve system functionality and update security requirements.

While the agency has made progress in addressing audit recommendations, ongoing effort will be necessary to address recommendations that have not been fully implemented or resolved. Moreover, management should continue to monitor those recommendations that have been implemented, in order to identify opportunities for increased maturity and continuous improvement.

Follow-up Report Team

Will Garber, CGFM, MPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Matthew Owens, CISA, MBA, Principal Auditor

Jessica Ritter, CPA, CISA, Staff Auditor

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits