State of Oregon

Oregon Liquor Control Commission: Cannabis Information Systems Properly Functioning but Monitoring and Security Enhancements are Needed

February 2018

Secretary of State
Dennis Richardson

Audits Division, Director
Kip Memmott

Report 2018 –07

This page intentionally left blank.

OLCC Cannabis Information Systems are Properly Functioning but Monitoring and Security Enhancements are Needed

Report Highlights

Although the Oregon Liquor Control Commission (OLCC) has taken positive steps to establish information systems for recreational marijuana regulation, we identified several weaknesses associated with OLCC's new IT systems used for marijuana licensing and tracking. They include data reliability issues and insufficient processes for managing marijuana applications and vendors. In addition, OLCC has not implemented an appropriate agency-wide IT security management program. We identified eight IT security issues that significantly increase the risk that OLCC's computer systems could be compromised, resulting in a disruption of OLCC business processes.

Background

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.

Purpose

The purpose of our audit was to review and evaluate key general computer controls governing OLCC's IT security management program, and application controls over the Cannabis Tracking and Marijuana Licensing Systems.

Key Findings

Within the context that legal marijuana is an emergent and unique public policy and the state is understandably still in the process of implementing governance programs, regulations, controls, and resources, we found:

1. Data reliability issues with self-reported data in the Cannabis Tracking System (CTS) and an insufficient number of trained compliance inspectors inhibit OLCC's ability to monitor the recreational marijuana program in Oregon.
2. OLCC should improve processes for ensuring the security and reliability of data in the CTS and the Marijuana Licensing System. In addition, better processes are needed to monitor vendors that host and support these applications.
3. OLCC has not implemented an effective IT security management program for the agency as a whole.
4. OLCC has not formally developed a disaster recovery plan and has not tested backup files to ensure they can be used to restore mission-critical applications and data.

Recommendations

The report includes 17 recommendations to the Oregon Liquor Control Commission focused on addressing the weaknesses in the CTS data reliability, management of software as a service, IT security management, and disaster recovery and backup processes.

The Commission generally agreed with our recommendations. The Commission's response can be found at the end of the report.

Secretary of State, Dennis Richardson
Oregon Audits Division, Kip Memmott, Director

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of his 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 and oversees audits and financial reporting for local governments.

Audit Team

Will Garber, CGFM, MPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Matthew Owens, CISA, MBA, Principal Auditor

Jessica Ritter, CPA, Staff Auditor

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

website: sos.oregon.gov/audits

phone: 503-986-2255

mail: Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, Oregon 97310

We sincerely appreciate the courtesies and cooperation extended by officials and employees of the Oregon Liquor Control Commission during the course of this audit.

OLCC Cannabis Information Systems are Properly Functioning but Monitoring and Security Enhancements are Needed

Oregon Liquor Control Commission provides oversight for the recreational marijuana program

"In 2014, voters approved Measure 91, which legalized the production, sale, and use of recreational marijuana in Oregon."

The Oregon Liquor Control Commission (OLCC) Board of Commissioners oversees Oregon's recreational marijuana program.[1] The Board of Commissioners consists of seven citizen commissioners who set policy for OLCC. They meet monthly to make decisions regarding liquor licenses, rules, contested case hearings, appointments of liquor store agents, and issues related to regulating recreational marijuana.

The Governor appoints commissioners to four-year terms, subject to Senate confirmation. Commissioners must represent each of the congressional districts, eastern Oregon, western Oregon, and the food and beverage industry. Commissioners appoint the agency's executive director, who oversees the agency's employees and day-to-day operations.

Along with liquor regulation responsibilities, the commission is tasked with ensuring the newly formed recreational marijuana program aligns with the existing OLCC structure. OLCC's recreational marijuana program and public safety program make recreational marijuana available to consumers 21 years of age and over, and medical marijuana to medical cardholders 18 years and older. OLCC achieves this through the licensing and regulation of independent marijuana growers, processers, and retailers. The program also tracks the growing, transporting, processing, and selling of OLCC-regulated recreational and medical marijuana products throughout Oregon.

Marijuana Licensing System and Cannabis Tracking System support the regulation of recreational marijuana

In 2014, voters approved Measure 91, which legalized the production, sale, and use of recreational marijuana in Oregon. House Bill 3400, signed into law during the 2015 legislative session, clarified regulatory oversight of Oregon's marijuana programs by granting OLCC the necessary duties, functions, and powers. The regulatory oversight includes licensing, investigative, and rule-making authority for the production and sale of both recreational and medical grade marijuana.

[1] ORS 475B.025(1)

State statute requires applicants for OLCC-regulated marijuana business licenses or renewals to submit their application to OLCC.[2] The Commission has the duty and authority to approve or deny applications to produce, process, and sell recreational and medical grade marijuana.[3] Licensees are required to renew licenses annually.[4] OLCC has the authority to refuse to license an applicant for a number of reasons, including if the Commission has reasonable ground to believe that the applicant "is not of good repute and moral character."[5]

The state law for legalized marijuana requires that recreational marijuana be tracked from "seed to sale" using a tracking system. Specifically, the system must be able to capture data showing the entire "chain of custody" of a marijuana plant from when it was still a seed through to the final retail sale to consumers. Additionally, the system must be able to track specific plant characteristics such as weight, moisture loss, and potency.

Citing a lack of skilled technology project management staff and expertise, and not having the capacity to build and support a fully functional seed-to-sale system, OLCC determined that a Software as a Service[6] (SaaS) solution would best support the technological needs of the recreational marijuana program.

OLCC management had to make a decision on whether to pursue a seed-to-sale traceability system that would also meet licensing requirements, or procure a licensing solution separate from the seed-to-sale system. Due to time constraints imposed by Measure 91, specifically requiring OLCC to begin accepting marijuana license applications on or before January 4, 2016, OLCC chose to procure a separate, easier to develop, licensing solution. The agency contracted with external vendors to develop, host, and support the Marijuana Licensing System and Cannabis Tracking System.

Marijuana Licensing System

In March 2015, OLCC signed a contract with NIC-USA, a national company that provides official government websites, online services, and secure payment processing solutions. This vendor was readily available as a provider of services to OLCC through a master agreement with the Department of Administrative Services. NIC-USA developed a system that provides a statewide, web-based solution for Oregon citizens to apply for licenses to become recreational marijuana producers, processors, and retailers.

---

[2] ORS 475B.040
[3] ORS 475B.060
[4] ORS 475B.070, 475B.090, 475B.110
[5] ORS 475B.045
[6] Software as a Service: A licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.

OLCC staff use the licensing system to review and track applicant data in order to make license approval determinations. The system also includes an interface that sends licensee approval status data to the Cannabis Tracking System. NIC-USA completed the project on time and OLCC began accepting license applications in January 2016.

Cannabis Tracking System

In March 2015, Oregon sought a Software as a Service (SaaS) solution for recreational marijuana traceability. The state awarded the contract to Franwell, Inc., which had already developed a cannabis tracking application in use in Colorado, called Metrc. Franwell developers, in cooperation with OLCC, customized Metrc to meet Oregon's requirements. This customized application, referred to as the Cannabis Tracking System (CTS), was implemented in April 2016.

To help ensure compliance with recreational marijuana laws in Oregon, the CTS tracks the transfer of marijuana items between licensed growers, processors, and retailers through the final sale of marijuana products. System functionality includes:

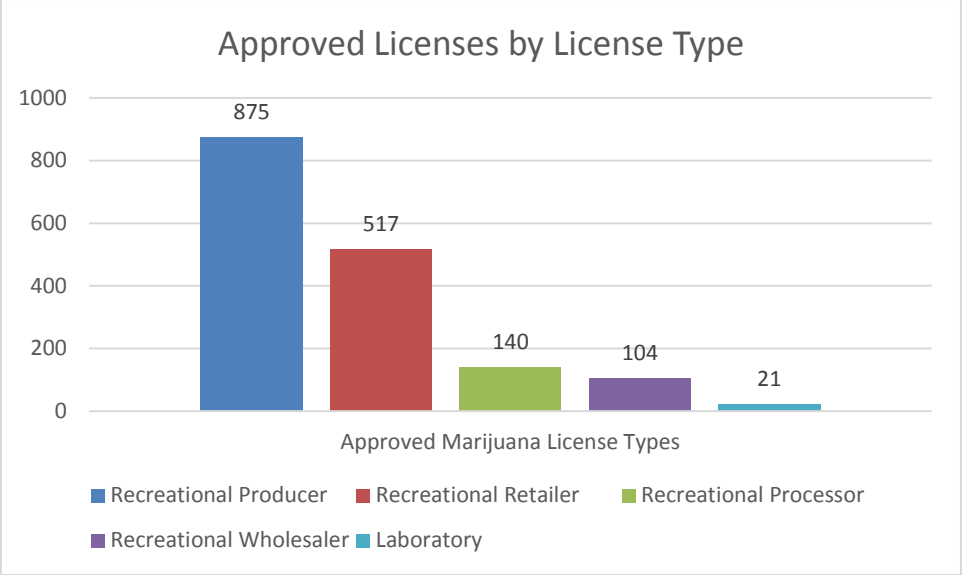
- a secure web-based interface for data entry, display, and reporting by marijuana licensees;
- a central data management system capable of storing inventory data, retail sales transaction data, and data for all licenses from seed to sale;
- a secure user interface for OLCC user and system administration, and for displaying licensee sales and inventory information; and
- reports, data analytics, and alerts to identify potential compliance issues and marijuana market trends.

Number of marijuana license applicants significantly higher than initially estimated

In 2015, OLCC estimated that there would initially be approximately 800 to 1,300 marijuana license applicants, based on an analysis of Washington and Colorado trends. Instead, as of December 2017, OLCC had received over 3,100 license applications and had approved over 1,600. Of those, over 50% are for producer licenses to grow marijuana and 31% are for retailer licenses to sell marijuana products (see chart below.) The number of approved applications is expected to reach approximately 2,000 by 2019.

The recreational marijuana program has generated over $480 million in sales through November 2017. The Department of Revenue has collected approximately $115.5 million in state tax revenue since retail sales began in January 2016.

Approved Marijuana License Types



Based on data provided by OLCC

OLCC's IT Department manages department information systems and data

The agency's Information Technology (IT) division consists of a Network Administration team and a Systems Administration and Software Development team. The Network Administration team is responsible for developing and supporting the data communications network. The Systems Administration and Software Development team is responsible for web application design and development, database administration, software development, and business needs analysis.

The agency communicated the need for a Chief Information Officer position in the 2017 legislative session; however, the agency did not receive funding for the position. Without a Chief Information Officer, both teams report to the agency's IT Director who, in turn, reports to the OLCC Deputy Director. During the course of our audit, the IT Director submitted his resignation, effective the end of 2017. Subsequent to our audit work, OLCC filled the IT Director position, and is again seeking funding for the CIO position during the 2018 legislative session.

Due to the outsourcing arrangement of the marijuana licensing and tracking systems, OLCC's network environment does not affect either system. However, the department is responsible for working with, and monitoring application service providers to ensure they are meeting all functional, security, hosting, and performance requirements as detailed in their respective contracts.

Objective, Scope and Methodology

The purpose of our audit was to review and evaluate key general computer controls governing OLCC's information technology security management program, and application controls over the Cannabis Tracking System and Marijuana Licensing System.

Objective

Our specific audit objectives were to determine whether management has implemented:

- a security management program with supporting policies and procedures to ensure that computer resources are protected against known vulnerabilities and physical threats; and
- sufficient computer controls over the Cannabis Tracking System and Marijuana Licensing System to support the regulation of the recreational marijuana programs according to current law.

Scope

The scope of our audit included processes and procedures governing OLCC's security management program that were in effect during calendar years 2016 and 2017. Additionally, our scope included processes and procedures that were in effect during calendar year 2016 through 2017 for collecting and recording marijuana license applicant information, marijuana inventory data, and sales data.

Methodology

To fulfill our audit objectives we conducted interviews with department personnel, observed department operations, and examined available system documentation. We also evaluated or tested:

- policies and procedures governing security management;
- policies and procedures over contingency planning, disaster recovery, and system and data backups;
- vendor management practices;
- processes used to provide access to marijuana applications; and
- the recreational marijuana compliance framework.

To identify generally accepted control objectives and practices for information systems, we used the IT Governance Institute's publication "Control Objectives for Information and Related Technologies," the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual," and Oregon Statewide Information Security Standards.

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 and reported provides a reasonable basis to achieve our audit objectives.

Audit Results: OLCC Cannabis Information Systems are Properly Functioning but Monitoring and Security Enhancements are Needed

The Oregon Liquor Control Commission (OLCC) has taken many positive steps that support regulation of the recreational marijuana industry. However, within the context that legal marijuana is an emergent and unique public policy and the state is understandably still in the process of implementing governance programs, regulations, controls, and resources, OLCC needs to continue enhancing processes, safeguards, and information necessary for the regulation of the recreational marijuana program in Oregon.

We identified several weaknesses associated with OLCC's new IT systems used for marijuana licensing and tracking. They include data integrity and maturity issues, and insufficient processes for managing marijuana computer programs and vendors. Until these issues are resolved, the agency may not be able to detect noncompliance or illegal activity occurring in the recreational marijuana program.

Additionally, we found that OLCC management has not implemented an appropriate security management program for all agency IT systems. OLCC does not have sufficient policies, procedures, and plans in place to ensure that computer resources are protected against known vulnerabilities and physical threats. Although this does not affect the externally hosted marijuana applications, other programs and administrative systems at OLCC may be at risk.

Immature regulatory processes and poor data quality increase risk that compliance violations may go undetected

After Oregon voters legalized recreational marijuana in 2014, the Legislature tasked OLCC with regulating this emerging and unique industry. OLCC had little time to develop processes and procedures, and implement new information systems to support and regulate this industry in time for the mandated January 2016 launch date. Additionally, significant statutory changes were made in the 2015, 2016, and 2017 legislative sessions, which required substantial modifications to software and additional changes to processes and procedures.

Marijuana businesses are required to track a number of items in the CTS, including daily sales activity, inventory transfers, lab test results, inventory adjustments, and marijuana waste. OLCC has developed some initial processes to identify when businesses fail to report activity in the CTS. These include alerts for the following:

- failure to report daily sales;
- failure to report marijuana harvests within 45 days of harvest date;

- marijuana sales that are inconsistent with reported inventory; and
- marijuana sales that are inconsistent with market pricing.

The department also developed some on-demand reports that help identify potential compliance violations such as marijuana plants that have been in the ground for an unusually long length of time, and individual consumer purchases exceeding legal limits.

However, due to the legally required rapid implementation of the recreational program, OLCC has not been able to implement robust compliance monitoring and enforcement controls and processes for the recreational marijuana program.

We identified five issues that increase the risk that OLCC may not detect potential compliance violations or illegal activity. These include relying on self-reported data from marijuana businesses, inconsistent weight measurement systems, allowing untracked marijuana inventory within the first 90 days of operations, poor or insufficient data quality in the CTS, and an insufficient number of trained inspectors needed for on-site investigations.

Self-reported marijuana tracking increases risk of inaccurate data

Licensed marijuana businesses input their own product inventory and sales data into the CTS. Although this is self-reported information, OLCC needs to ensure that the data is complete, accurate, and valid.

Oregon Administrative Rules require all licensed marijuana businesses that grow, process, or sell usable marijuana to report sales and inventory data on a daily basis using the CTS. While there are application programming interface[7] protocols that allow third-party point of sale (POS) devices to communicate directly with the CTS, thus ensuring more accurate reporting, OLCC does not require the licensees to use them. This was primarily due to a lack of available POS devices at the initiation of the program.

Currently, businesses may choose to enter data directly into the CTS, either manually or using spreadsheets. This approach could allow them to submit inaccurate sales figures and inventory amounts. We observed one retailer demonstrate this risk by exporting a spreadsheet file of sales transactions from their POS device to a computer, and then altering the data. Although the retailer did not upload the altered file into the CTS, this demonstrated that there are no controls in place to prevent retailers from uploading altered data to the system.

[7] Application Programming Interface: A set of programming rules that allows multiple software systems to communicate with one another.

Inconsistent measurement systems increase data tracking complexity

There is no standard unit of measurement for marijuana weight in the CTS. Weight can be reported using either the metric system (kilograms or grams), or the U.S. Imperial system (pounds or ounces). Additionally, marijuana growers can change units with every new harvest, and retailers can change units as desired.

Generally accepted computer control practices indicate that when defining the type of information or data collected by a system, data owners should implement procedures to ensure the integrity and consistency of all information stored in electronic form.

OLCC requires the use of specific scales for measuring product weight that are certified by the Oregon Department of Agriculture. However, without additional guidance on when and how to convert from one unit of measurement to another, these types of conversions could add an additional layer of confusion and uncertainty to the data, thereby, increasing the complexity of data analytics OLCC must perform for compliance monitoring. Moreover, it elevates the risk that CTS users could manipulate inventory data and falsely attribute any discrepancies to rounding errors.

For example, one pound of marijuana is equivalent to 453.592 grams. If a retailer receives 2.75 pounds of marijuana, but enters it in grams, they could enter it as 1247.378 grams (2.75 x 453.592 = 1247.378) or 1270.08 grams (2.8 x 453.6 = 1270.08). This constitutes a difference of 22.7 grams just due to rounding errors. Depending on the quality of the cannabis, 23 grams could have a retail market value ranging from $115 to $345.

Licensees can create marijuana inventory without a tracking history

The requirements for the CTS include tracking usable marijuana from seed to sale. The premise behind this is that OLCC would be able to monitor daily sales, and in conjunction with tracked marijuana characteristics (weight, lab results, etc.), analyze the data for patterns that may indicate noncompliant or illegal activity.

However, when recreational marijuana became legal, Oregon Administrative Rule 845-025-2060 allowed newly licensed producers to acquire usable marijuana from any source and add it to their inventory within the first 90 days of licensure. This rule was put in place primarily to allow the transfer of existing medical marijuana plants into the recreational marijuana market. OLCC refers to this as the “immaculate conception” rule, which is set to expire after July 1, 2018. The marijuana added to inventory under this rule does not have any history associated with it in the CTS.

To accommodate this rule, the CTS includes functionality to create usable marijuana “packages” without tracking history. After 90 days, a licensee would have no legitimate business need to utilize this feature. However, we

found there are no system controls that would prevent a user from taking advantage of this feature after the initial 90-day period.

The lack of system controls increases the risk that marijuana retailers could sell illegally sourced or untested marijuana products. While OLCC has the ability to generate the CTS reports showing when "immaculate conception" has occurred, they have not established processes to review these reports on a consistent basis.

While we did not perform a full review of all "immaculate conception" transactions, in reviewing prior OLCC investigations, auditors noted a single marijuana processor used this feature 47 times from February through May of 2017. Of those transactions, 22 occurred outside the established 90-day window.

Data quality issues impair OLCC's ability to monitor marijuana industry

Currently, owing to the new and emergent nature of legal marijuana policy, there is a lack of established standards or baselines for recreational marijuana data analytics and compliance monitoring. OLCC intends to develop these benchmarks, but data quality issues have thus far hindered this strategic goal.

OLCC reports that known data quality issues in the CTS make the information less than completely reliable. Furthermore, due to the newness of the industry, the system lacks a sufficient number of quality data points to develop and establish robust industry trends and baselines. This inherent issue can only be resolved over time, when OLCC collects enough data to develop quality points and trend analyses.

Examples of poor data quality include instances where different marijuana strains, grown under varying conditions, were inappropriately included in the same "package" in the system. Due to the varying characteristics of the marijuana plants included, there is too much variance in the data to be usable. If the plants were all of the same strain, grown under the same conditions, OLCC would be able to establish more accurate trends and baselines.

Another example includes an instance where a retailer inadvertently uploaded marijuana product code numbers to the CTS instead of the dollar amount for that day's sales total. Although this error was corrected within 24 hours, it caused sales data to be off by almost $300 million until corrected.

Until appropriate benchmarks are established, OLCC may not have the ability to identify more subtle, hard-to-detect compliance issues, or illegal activity, which inhibits the agency's effective monitoring of the recreational marijuana industry in Oregon.

OLCC lacks protocols and trained staff to perform on-site inspections

To compensate for data quality issues, periodic on-site inspections could help ensure marijuana businesses are complying with state law and are reporting inventory and sales accurately. However, OLCC has not yet developed the standards and protocols needed to perform on-site inspections. Additionally, OLCC does not have a sufficient number of trained staff to investigate all potential violations.

To identify most potential compliance issues, OLCC relies on tips from the public, or other reactive measures such as following up on unreported daily sales. OLCC plans on-site inspections of marijuana businesses in the future, but has not yet finished developing the standards or protocols needed to ensure consistency across investigations.

Furthermore, OLCC lacks a sufficient number of trained staff to perform the inspections. When our audit began, OLCC only had 11 Regulatory Specialists responsible for performing inspections. Management determined additional inspectors were needed to handle the anticipated workload. In 2017, OLCC received authorization to hire additional Regulatory Specialists, and currently has 20 positions, two of which are vacant.

Even with the additional staff, OLCC may not be able to ensure an appropriate amount of scrutiny for marijuana businesses. Both Alaska and Nevada have approximately one inspector for every 18 recreational marijuana licenses. Currently, Oregon only has one inspector position for every 83 recreational marijuana licenses.

Until investigation standards and protocols are developed, and a sufficient number of staff are trained, OLCC will not be able to perform needed on-site inspections with sufficient guidance and scrutiny to ensure marijuana businesses are complying with state law.

Again, emphasis needs to be placed on the newness of marijuana policy in the state and the challenges of establishing a sound governance structure and properly staffing and training personnel in a relatively short period of time.

Better practices needed for managing marijuana computer programs and application vendors

In order to capture licensee applicant information and track marijuana sales, OLCC chose to use a Software as a Service (SaaS) model for both the Marijuana Licensing System and the Cannabis Tracking System. OLCC contracted with NIC-USA to implement the Marijuana Licensing System and with Franwell, Inc. for the Cannabis Tracking System.

In choosing a SaaS model for these two applications, OLCC assumed certain risks and responsibilities for ensuring the respective SaaS providers are

meeting their contractual obligations and that the applications are secure and working as intended.

We found that OLCC management did not perform adequate due diligence to ensure their marijuana application vendors are meeting their contractual requirements for providing SaaS computer programs and security requirements for hosting OLCC data. In particular, we found that OLCC lacks processes to monitor their marijuana SaaS providers and needs better procedures for reconciling data between their two marijuana systems, a more robust change management process to ensure data integrity, and better procedures for ensuring that access for state employees to the systems remains appropriate.

OLCC lacks processes to monitor some third-party service providers

OLCC management has not performed due diligence to ensure its marijuana application vendors are meeting their contractual obligations for hosting and security requirements.

The CTS and its data are hosted and maintained by the application developer Franwell. The contract with this developer states that IT security controls for this application and its data must meet the minimum information security standards published by the Center for Internet Security.[8]

Industry best practices indicate that prior to receiving IT services from a third-party service provider and prior to granting access to data, an organization should confirm the service provider can meet or exceed its minimum security standards. We found OLCC has not taken any steps to validate that Franwell is in compliance with these standards, nor has OLCC requested an independent IT security assessment or performed other measures to ensure this service provider has adequate security controls in place.

We contacted the vendor and asked if an independent assessment of their IT security has been performed. A Franwell representative stated they have never had an independent assessment performed. Furthermore, when we asked for a Service Level Agreement monitoring report that would show whether they were meeting their contractual requirements for hosting, they were unable to provide an accurate report.

Without independent verification, OLCC does not have assurance that data hosted by Franwell is adequately protected against unauthorized use, disclosure, or modification. This is particularly significant because the data in the Cannabis Tracking System is used by OLCC to help regulate Oregon's recreational marijuana industry.

---

[8] The Center for Internet Security provides global standards and best practices for securing IT systems and data against cyber-attacks.

Interface reconciliation processes non-existent

OLCC has not implemented reconciliation processes or procedures to validate that the CTS appropriately receives data sent by the Marijuana Licensing System.

OLCC uses the Marijuana Licensing System to record applicant data and to track decisions regarding the status of the application or the licensee. When an application is approved and made active, or when an active licensee status changes, those changes need to be communicated to the CTS. To accomplish this, an interface was set up between the licensing system and the tracking system.

Controls surrounding interface processing should reasonably ensure that data is transferred from the source system to the target system completely, accurately, and timely. OLCC relies on their two marijuana application vendors to work together to ensure the interface is working appropriately. The systems send an alert to all three parties when an error occurs. The parties then work together to troubleshoot and correct the issue.

While this approach is largely effective, we found that license status (active, revoked, or expired) information in the two systems can still be out-of-sync and must periodically be reconciled.

We identified one expired license in the licensing system that was still designated as active. Although a licensee with an expired license would normally be locked out of the tracking system, this error could allow the licensee to continue operations in the tracking system with an expired license.

Additionally, we identified three active licenses that did not transfer to the tracking system, which could allow these licensees to temporarily operate with a valid license while not having to track or report sales.

Test data in Marijuana Licensing System production environment

OLCC does not have appropriate change management processes in place to ensure that data in the Marijuana Licensing System is complete, accurate, and valid.

Data in a production environment should be complete, accurate, and valid and test data[9] should remain isolated in a test environment. We identified ten OLCC employees listed in the Marijuana Licensing System production environment as having a financial interest in marijuana businesses. After further review, we determined these names were relics of system testing, and were never removed at the completion of testing.

[9] Test data: A set of data created for testing new or revised applications. While test data appears similar to actual production data, it does not represent real transactions.

Errors such as these increase the risk that management may make licensing and other program decisions based on unreliable data in the Marijuana Licensing System.

User account management processes lacking

User account management processes governing access to both the Marijuana Licensing System and the CTS are not sufficient to ensure that users only have access to systems and system functionality needed to perform their duties.

Logical access to computer application should be restricted according to each user's individual need to view, add, or alter information. In order to maintain this principle of "least privilege," organizations should have formal processes for timely granting, suspending, and closing user accounts. Management should also periodically review and confirm users' access rights to ensure they remain appropriate.

We found OLCC has immature processes in place to grant and review logical access to these systems. Additionally, the systems do not have robust account management features that allow for easy review of user access. Auditors requested user access lists for both the Marijuana Licensing System and the CTS, but OLCC was unable to provide one for either system without significant effort.

For the licensing system, individual users and their access permissions would have to be manually pulled individually in order to generate a list. This method is labor intensive and unreliable.

For the tracking system, there is a table in the database that contains the user access data, but OLCC indicated the developer was unwilling to provide that data to outside entities, including OLCC, because the table also contains confidential login credentials for the users.

If OLCC does not periodically review access, it increases the risk that users retain inappropriate access. While the majority of the information in the systems is not sensitive, OLCC uses it for compliance purposes and should protect it against unauthorized use, disclosure, or modification.

Currently, there are 72 internal state users of the CTS. While we could not review access, system reports show that eight of these users have never logged in, which indicates they do not need access to the system.

OLCC lacks an appropriate IT security management program

In addition to reviewing the marijuana licensing and tracking systems, we also reviewed OLCC's processes for ensuring all of its IT systems and data are secure. The agency has implemented important protection measures and tools for security across the agency, such as firewalls and intrusion detection and prevention network devices. However, we identified

significant weaknesses related to OLCC's IT security management practices. They include the following:

- OLCC lacks an up-to-date security plan;
- information technology assets are not sufficiently tracked;
- OLCC has not set server or network device baselines, and does not have a process to monitor for unauthorized changes or devices;
- management has not developed processes to identify IT security vulnerabilities;
- antivirus solutions are not effectively managed;
- servers and workstations are running on unsupported platforms;
- physical access controls should be improved; and
- long-standing information security issues remain unresolved.

Information technology security plan is insufficient

OLCC's security plan is out of date and does not accurately reflect the agency's current business or technology environment.

Agency management should have a documented security plan to ensure state computing assets are properly protected. Effective security plans are a roadmap for maintaining security infrastructure and defining the necessary resources to accomplish critical objectives. Security plans should detail security roles and responsibilities, and should be supported and enforced by related security policies, procedures, and technical controls.

OLCC last updated its security plan in 2008. Since then, the agency has undergone numerous changes in both its IT infrastructure environment and its major applications. Additionally, OLCC's overall mission expanded to include regulating the recreational marijuana program in Oregon.

OLCC's security plan does not provide sufficient guidance for agency personnel to adequately protect OLCC's information assets. This significantly increases the risk that an IT security event could occur that would adversely affect OLCC's ability to fulfill its mission.

Information technology assets not sufficiently tracked

OLCC does not sufficiently document and track authorized hardware and software allowed on their network.

Managed control of IT assets plays a critical role in network security. A fundamental first step in protecting these assets is maintaining a comprehensive list of authorized hardware and software.

OLCC's management does not maintain a documented inventory of the agency's IT assets, including a comprehensive inventory of hardware and software authorized to be on their network.

Without a process for identifying all IT assets, the agency cannot develop and implement appropriate measures needed for protecting their assets from unauthorized use, modification, disclosure, or theft.

OLCC does not adequately manage device configurations

The agency does not have an effective process in place to determine if network devices are configured appropriately, nor has the agency established configuration baselines for servers, workstations, and network devices.

Security standards indicate that entities should establish a centralized repository to document baseline configurations for operating systems and network devices such as routers, firewalls, and switches. In addition, entities should monitor operating systems and network devices to detect unauthorized changes or devices.

We found OLCC has not established baseline configurations for Windows servers, firewalls, and other network devices. Furthermore, the agency does not have a process to detect unauthorized changes to system parameters or detect when an unauthorized device accesses its network.

Without robust device configuration management and monitoring, OLCC staff are less likely to detect unauthorized changes to critical security parameters. Unauthorized changes to these configurations could leave affected devices vulnerable to internal or external attack or compromise.

OLCC lacks comprehensive vulnerability assessments

OLCC does not have adequate processes in place to scan for vulnerabilities on network servers, workstations, and applications.

To provide adequate security, organizations should have processes to evaluate security controls periodically. These processes should include evaluations to identify technical vulnerabilities and potential security weaknesses, and effectively resolve them in a timely manner.

We determined OLCC does not have ongoing processes to scan for vulnerabilities on network servers and applications. The department also has not developed systematic procedures to correct or mitigate identified vulnerabilities.

Without these processes, the OLCC cannot adequately plan for and protect itself against internal or external security threats, thus increasing the likelihood that computer systems and data could be compromised due to a known vulnerability.

Antivirus software not appropriately managed

OLCC does not appropriately manage servers and workstations to ensure they are adequately protected from viruses and other malware.

Network servers running Microsoft Windows operating systems should have mechanisms in place to protect systems from malicious software such as viruses and Trojan horses. Statewide Information Security Standards require that all workstations and Windows-based servers have appropriate antivirus/anti-malware protection installed. Furthermore, Linux servers should have malware protection in place to prevent the propagation of viruses and other malware on the network.

We found OLCC IT management has not established an effective solution to ensure that its servers and workstations are protected from malicious software. We identified numerous servers and workstations that either lacked an effective antivirus software solution, or had one that was significantly out-of-date.

While OLCC purchased a tool to check for out-of-date antivirus software on its workstations, we found staff responsible for ensuring antivirus software is current did not resolve reported problems in a timely manner. Absence of an effective antivirus or anti-malware solution significantly increases the risk that OLCC systems and its data could be compromised.

Servers and workstations are operating on unsupported platforms

OLCC does not have processes in place to ensure its servers and workstations have operating systems that are supported by their respective vendors.

Security standards indicate organizations should have strategies in place for ensuring operating system software is appropriately updated to reduce the risk that known weaknesses could be used to compromise computer systems and its data.

As vendors become aware of security vulnerabilities in their software products, they typically issue updates or patches to correct or mitigate the vulnerabilities. However, vendors generally discontinue support for a particular operating system version or application after a period of time.

We identified multiple obsolete Windows and Linux servers running on OLCC's network. Additionally, we identified five workstations running an unsupported version of Microsoft Windows.

OLCC management indicated they have several "mission critical" applications installed on obsolete servers that cannot run on more modern operating systems. Additionally, management was unsure as to why workstations were still running on outdated operating systems, as they believed they were all previously updated to a supported version of Windows.

Management stated they have put Linux server updates on hold because they are currently working to transition to an enterprise license for their Linux servers, at which time they will transfer all Linux machines to the newer supported version.

Relying on unsupported operating systems significantly increases the risk that OLCC's computer systems could be compromised and may result in a disruption of business processes that support alcohol sales to Oregonians.

Physical access controls should be improved

More robust procedures are needed to ensure that physical access to critical OLCC IT resources are appropriately secured.

Best practices for physical security state that sensitive information technology and infrastructure resources should be adequately secured using appropriate access control devices such as keys, employee badge readers, or key pads. Additionally, management should periodically review badge access to secure areas, and require PINs to be changed on a set interval.

OLCC management has provided adequate controls to limit physical access to their main building, including check-in and check-out procedures, required badge access, and keypads on secure doors. However, we determined that controls over physical access to sensitive information technology and infrastructure resources should be more robust. For example, OLCC does not have processes to ensure PINs are appropriately secured or that they are changed on a periodic basis.

Without appropriate processes governing physical security, there is an increased risk unauthorized personnel may gain physical access to critical IT infrastructure and compromise key business processes.

Long-standing information security issues remain unresolved

The agency has a history of taking limited and ineffective action to remediate IT security vulnerabilities.

Specifically, in the last five years OLCC has had two independent external risk assessments and one internal audit performed. These reports identified numerous weaknesses in OLCC's IT governance, policies, procedures, and plans. Most of these weaknesses have not been addressed. They include:

- outdated or unpatched operating systems and applications;
- lack of internal vulnerability assessments and/or penetration testing;
- poor antivirus management;
- outdated IT Security Plan; and
- insufficient or outdated policies and procedures related to IT security.

These long-standing issues significantly increase the risk that OLCC's network, systems, and data could be compromised. While multiple individuals have responsibility for the IT systems and processes associated

with these weaknesses, we found that OLCC lacks clear leadership and direction for its IT department.

OLCC recognized that this was an issue and in 2017 requested a Chief Information Officer position as part of its budget request to the state legislature. The request was denied.

OLCC should develop a disaster recovery plan and improve backup media testing

OLCC management has taken steps to ensure operations continue in the event of a disruption or disaster, but more action is needed to ensure systems can be restored in the event of a disaster.

Disaster recovery planning insufficient

Disaster recovery planning is a resource-intensive task that organizations generally defer to work on projects with more immediate or certain payback. However, long delays in restoring critical computer systems could severely affect OLCC's ability to carry out their mission.

OLCC management has taken several steps to help ensure operations continue in the event of a disruption or disaster. They include:

- backing up critical applications and data;
- implementing a disaster recovery warm site[10];
- documenting business restoration priorities; and
- documenting an Emergency and Business Continuity Communication Plan.

While these steps are important, OLCC has not developed a comprehensive disaster recovery plan that includes the technical details necessary to timely restore operations. Without such a plan, the department cannot ensure it can timely restore operations and risks significant disruption to the agency's ability to perform its mission.

More steps needed to ensure backup media reliability

OLCC has not tested backup files to ensure they can be used to restore mission-critical applications and data.

The department has processes in place to ensure that the system data are backed up. However, OLCC does not periodically test these backups to confirm the system and data could be restored in the event of a major disruption or outage.

We evaluated the department's process for backing up key applications and data, including backup frequency, notifications of backup success or failure,

[10] Disaster Recovery Warm Site: A warm site is a disaster recovery option where the needed hardware and connectivity are already established but require backup tapes to restore operations.

and whether or not backups are tested on a periodic basis. OLCC has documented procedures in place that require testing server and data backups on at least a semiannual basis. However, we found this did not occur in practice.

We concluded that the department is backing up the system and its data using specialized backup software. However, without testing, management has no assurance that the system and its data could be timely restored in the event of a disruption.

Recommendations:

To address the risk that recreational marijuana compliance violations may go undetected, we recommend OLCC management:

- Develop and implement standards and protocols for on-site inspections and investigations.
- Evaluate the need and provide for an adequate number of trained OLCC inspectors commensurate with number of licensed marijuana businesses.
- Perform risk-based on-site monitoring and inspections to ensure that licensees are reporting accurate information in the CTS and complying with applicable laws.

To address weaknesses related to marijuana vendor and application management we recommend OLCC:

- 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.
- Develop and implement reconciliation processes to ensure that data is appropriately transmitted by the Marijuana Licensing System and received by the Cannabis Tracking System.
- Establish processes for granting and reviewing access to the Marijuana Licensing System and the Cannabis Tracking System.
- Implement change management processes in line with industry best practices, including measures that ensure test data remains segregated from the production environment.

To address weaknesses related to OLCC IT Security Management Program we recommend OLCC management:

- Update and test OLCC's information security plan to ensure the plan reflects the agency's current business and IT environment.
- Establish a process to maintain an up-to-date inventory of authorized hardware and software allowed on OLCCs network.
- 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.
- Develop and implement a process to scan for vulnerabilities on devices on the network.
- 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.

- Transition software off obsolete platforms. If that is not possible, ensure unsupported servers are appropriately segregated on the network.
- Review physical access procedures to ensure access is appropriate, and require PINs to be periodically changed.
- Develop and implement a process to remediate weaknesses identified in risk assessments and audits, and routinely evaluate and assess the agency's security posture.

To address weaknesses related to disaster recovery planning and backup media testing, we recommend OLCC management:

- Develop and document an entity-wide disaster recovery plan.
- Perform periodic tests of backups to ensure usability.

Oregon
Kate Brown, Governor

Liquor Control Commission
9079 SE McLoughlin Blvd
Portland, OR 97222-7355
(503) 872-5000
(800) 452-6522

January 26, 2018

Kip Memmott, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 500
Salem, OR 97310

Dear Mr. Memmott,

This letter provides a written response to the Audit Division's final draft audit report titled "Oregon Liquor Control Commission: Cannabis Information Systems Properly Functioning but Monitoring and Security Enhancements are Needed."

The Oregon Liquor Control Commission (OLCC) appreciates the professional work of the Oregon Secretary of State's Office Audits Division (SOS Audit Division) and generally agrees with the recommendations.

The technology recommendations of the SOS Audit Division fall into two distinct categories: 1) Security and Functional Recommendations Concerning the Marijuana Licensing System (MLS) and Cannabis Tracking System (CTS); and, 2) Overall IT Security and Disaster Recovery Recommendations.

The OLCC will highlight the order of its most important technology priorities related to audit recommendations through a general response. The response will provide the necessary public safety context as it relates to the audit recommendations about the marijuana program. Last, the agency will detail actions specific to the marijuana program IT recommendations and then those related to overall IT security and disaster recovery.

General Response: Urgent Operational and IT Security Action Items

The agency is actively following up on all aspects of the audit and will be seeking budget limitation authority to move forward on the technology issues listed below during the 2018 Legislative Session. *These priorities for the OLCC are connected to the agency's immediate security improvement and urgent operational needs.*

1. **Evolving IT Management Expertise and Capacity**: The OLCC lacks the capacity for high-level IT planning and solutions implementation and needs to build internal expertise by hiring a Chief Information Officer (CIO). Execution of IT security remedies is but one important example underscoring the need for increased management oversight and expertise. Generally, the OLCC has antiquated IT systems throughout its operations and the need to modernize and create an overarching architecture integrating industry standard platforms for doing business has been

management's consistent priority since the agency's strategic plan which was created in 2015. The OLCC is managing four major IT projects; all started within the last two-and-half years. The OLCC recently hired a new IT program manager to continue daily operations. The OLCC continues to pursue legislative approval for a new position to hire a CIO to provide strategic leadership and address system-wide IT needs. This key position is related to specific findings of the SOS Audit recommendations concerning overall security management and to recommendations to improve oversight for managing marijuana program vendors. *Completion: 2nd quarter 2018.*

2. **Replacing Old Unsupported Servers and Switches**: The agency's antiquated servers and the lack of technical support of old switches by the manufacturer is a mission-critical issue. Like many businesses, the OLCC was waiting for product improvement solutions from the manufacturer that have not materialized; specifically the manufacturer has not upgraded switching capabilities or provided for the ability to integrate third-party solutions. The agency is requesting limitation from the 2018 Legislative Session to replace server and switching technology. This action specifically responds to the SOS Audit Division finding and recommendations that, "Servers and workstations are operating on unsupported platforms." The OLCC will seek $400,000 in limitation to address this issue. *Completion: 3rd quarter 2018.*

3. **Proving Near-Term Redundancy for Disaster Recovery**: The OLCC intends to take immediate steps to establish a backup hot site for critical computer systems and has secured approval from Oregon's Chief Information Officer's Office to install fiber optic line connecting two OLCC warehouses that are within a half-mile of each other. This will establish near-term redundancy within the 2018 calendar year. The OLCC can achieve this objective if limitation is approved for new switches and servers. This project works in tandem with the server and switch replacement because it is dependent on the efficient redeployment and reuse of old servers (Item 2. above). Over the long-term, the fiber optic connection will not only serve the hot site, it will add value by extending enhanced interoperability between warehouses. The multiple benefits of this immediate action will enable OLCC to evaluate future options for geographically distributed redundancy. This is an immediate and urgent issue because weather and electrical events threatened operations of the liquor warehouse on multiple occasions last year. Because the OLCC ships out liquor daily with a retail value of $2.2 million, recovery and redundancy of computer systems is critically important for continuity of operations. The SOS audit specifically identifies taking the step of establishing a warm-site. *Completion: 3rd quarter 2018.*

4. **Expanding IT Capabilities for Marijuana Program Management: Near Term Work and Making Choices about Vendor Contracting**: The OLCC is concerned about future provider services for licensing and for absorbing tracking responsibility for medical grow sites, processors, and dispensaries in the Cannabis Tracking System. The agency believes its Software as a Service (SaaS) providers have produced timely and quality services to date. Vendors have been flexible in working with the agency to establish and reset development priorities. The OLCC must now determine how to evolve licensing system capabilities and define the options it has for future systems

development. The agency believes this requires building additional internal capacity and expertise to plan, negotiate and provide oversight for the deployment of more robust IT systems. Additionally, the agency must establish contractual requirements and work expectations with its vendor to extend capabilities to track medical registrants in the Cannabis Tracking System (CTS) by June 31, 2018. This body of IT work directly addresses audit findings and recommendations, and it provides a focus for immediately improving system security issues and oversight; it is specifically related to the audit recommendations to improve vendor management. The ability of OLCC to do this will be aided by the approval to hire a CIO (Item 1. above). *Completion: 2nd quarter 2018.*

The OLCC must immediately manage the following four areas of urgent concern and the audit reinforces the need for timely action. To achieve success in these areas, OLCC must secure budget limitation authority and meet many required administrative approvals for purchasing and technology system development.

Response: Security and Functional Recommendations Concerning the Marijuana Licensing System (MLS) and Cannabis Tracking System (CTS)

The OLCC generally agrees with all recommendations and is complimentary of the SOS auditors for their input to a program for what overall, has been a successful launch of the recreational (medical) cannabis industry in Oregon.

Marijuana Regulation is a start-up business for the state: The regulation of marijuana is essentially a new business start-up and the OLCC has been as entrepreneurial as possible to deal with the unique challenges of standing up this regulatory enterprise. OLCC staff has had to focus on solving multiple issues in time to meet critical statutory deadlines.

Since voter approval in 2014 of Ballot Measure 91, three sessions of the legislature produced comprehensive legislative changes with substantial policy and system details. The rapid implementation of marijuana IT systems — within an ever changing legal environment — has been challenging. Consequently, the OLCC and its vendors focused on the delivery of required changes in programing to meet the fundamental requirements of the law, and regulations codified in newly adopted statutes. While the OLCC never missed a major operational deadline, the process led to rapid acceptance of completed development work and deferral of important analytical software development. Now that a developed legal framework and additional changes by Oregon lawmakers are expected to be less encompassing, the OLCC can revisit security issues raised by the audit, as well as other operational issues with its system vendors.

Marijuana IT system costs are financed through fees licensing the industry and do not utilize State General Funds in their development or operation. At this time, it appears the financial structure in place is sustainable and the OLCC will be able to refine and redevelop systems based on the knowledge and experience gained during the initial program implementation, along with the recommendations of this audit.

The Marijuana Licensing System (MLS) and the Cannabis Tracking System (CTS) are delivering results: In this unique area of endeavor, without blueprints or a playbook, the current condition of OLCC's IT systems related to marijuana can be characterized as, "state-of-the-art imperfection." The audit confirms several shortcomings of the systems, all of which require fixing, and all of which will help to perfect the quality of the program and IT security. *While the audit has identified several important issues, those issues do not suggest that the functioning of the IT systems compromise OLCC's ability to provide for public safety oversight of the marijuana industry through its use.* The audit does make recommendations that would improve the IT systems' effectiveness.

Many of the issues identified in the audit were well known to OLCC, however the work accomplished by vendors and the OLCC has created a strong knowledge base, a solid framework to build upon with IT systems that provide a greater degree of accountability and licensee oversight. Because of the major commitment of staff time, these IT systems have served the state well and at a moderate expense.

The marijuana license system has been utilized to license about 2,000 marijuana business that are forecasted to generate, by the end of the current biennium, a total of about $210 million dollars in tax revenue to be used for state and county services. Annual retail marijuana sales now exceed $500 million dollars.

The Cannabis Tracking System (CTS) has identified thousands of discrepancies, small and large, that have led to investigations, administrative charges, and warnings or sanctions.

Licensees that fail to accurately record data do so at the jeopardy of losing their licenses and other sanctions: The SOS audit makes several findings about data quality within the CTS that are accurate but require contextual explanations. CTS is essentially an accounting ledger where all licensees must account for daily sales and activity. A ledger in and of itself does not guarantee that businesses are accurately reporting data nor that they understand the laws and rules governing their regulated industry. However, a ledger does create a paper trail for later enforcement action, so even "bad" data in CTS is meaningful data.

To clarify, *the dependency, burden, and interest of data accuracy falls on the licensees whose product on hand must match, upon inspection, their self-reporting into the CTS. The reporting of inaccurate data can lead to the loss of license and sanctions that include fines and business closures.* The simple correction of minor mistakes is also a frequent remedy of unintentional inaccuracies. Nevertheless, the OLCC will work to reduce the ability of licensees to make errors by inputting incorrect data. Data quality and overall regulatory compliance will improve as the system is populated with data, additional training is provided for licensees and staff, and overall user experience catches up with the deployment of system features. As the marijuana program stabilizes, this system will vastly improve as a regulatory tool. It is already producing good results today.

To determine data quality and the accuracy of reporting in the system, field investigations and/or forensic auditing of records in the data tracking system must take place. This type of analysis helps to understand the relative accuracy or inaccuracy of data reported and provides proof of compliance and violations. The process of accountability is powered by people: inspectors, fiscal analysts, and data analysts who monitor transactions and carry out field inspections.

The possibility of inspection is the deterrent to willful and systemic data manipulation and inaccuracies, ensuring that the systemic recording of data must match transactions and inventories is in itself important. However, the technical focus of an audit is meaningful as well, the system should not allow users to manipulate data in ways that it is not intended to be reported. Developing more extensive user training and limiting opportunities for the misuse of core features, including creating "startup inventory" entries long after initial licensure will improve data quality.

The audit points to several data reporting compliance issues related to timely entry of data. The OLCC will be systematically issuing fines based on violations that can be proven by data recorded in the CTS system or the absence of data by failing to record it, such as not meeting a requirement to account for a marijuana crop's moisture loss within 45 days of a harvest. Further build out of CTS will provide staff the ability to be routinely alerted to this type of violation, and potentially trigger a licensee user alarm. The OLCC is exploring how modifying the IT system and requirements under the Administrative Procedures Act (APA), that protect due process, can be integrated to auto-generate citations based on compliance failures to properly and timely record data. Similar to a "speeding ticket," with this type of sanction the accumulation of too many tickets would result in the loss of license. In the meantime, the OLCC is manually monitoring data for timely entry and analyzing it for potential action against violators.

Also described in this audit are important but less urgent issues. The audit identified that some data entry measurement and rounding errors resulting from measurement conversion issues could lead to systemic misreporting of marijuana quantities. Specifically, the audit is critical that the system allows both imperial (ounces) and metric (grams) measurements. While an important issue, today the OLCC is focused on efforts to stop diversion of large amounts of marijuana through overall regulatory efforts. Because the method of measurement is also an issue within the marijuana supply chain of commerce, the OLCC is confident that measurement conventions and uniformity can be achieved.

The CTS is one part of a three-part strategy for strong oversight and enforcement: CTS is proving to be a solid tool for triggering enforcement actions and providing proof of violations. To date, OLCC has only been able to focus on the most serious violations. As the functionality of the data tracking system is enhanced, and OLCC adds trained staff, the overall performance will improve. Recommendations of the audit will contribute to strengthening the system.

The OLCC is putting in place a robust regulatory regime to ensure public safety. *Citizens and policy makers need to know that as important as the issues identified in this audit*

are, the OLCC is not dependent on the CTS system alone to identify licensees that are attempting to use the state system as a cover for diversion. The CTS system is one fundamental tool for successful enforcement and compliance. Readers of the audit should not have the impression that the CTS system is defective or is the sole method for detecting compliance issues, rather the audit recommendations focus on improving the overall effectiveness of the system which the audit acknowledges is *properly functioning*. The OLCC appreciates this audit insight and for acknowledging the potential need for staff to carry out monitoring and compliance inspections to ensure operational efficiency.

Robust compliance and enforcement is being established. The effectiveness of the OLCC enforcement regime depends upon the CTS, field inspections, forensic financial and data audits, reported observations by the public or employees about licensee activity, and continuous coordination with law enforcement. Additionally, security measures required by regulation for on-site gates, locks, safes, alarms, and fencing also help to prevent diversion. Lastly, camera coverage of grow sites, processing activity, and of the entryways and exits of all facilities on the licensed premises are additional tools for licensee accountability. The CTS system supports all of this enforcement activity and is one leg of the three-legged stool comprised of CTS tracking, premises inspections, and premise security regulations.

Committed to improve data accuracy and establish enforcement routines: The start-up business the OLCC now operates to regulate cannabis in Oregon is still evolving. In December 2017, the OLCC conducted its first minor decoy operations to test if businesses were making retail marijuana sales to anyone under the age of 21 (age 18 with a medical card). It took a while to develop the protocols and to find the time to deploy an inspection staff, with competing priorities, to do these operations in every region of the state. In the coming year or two, this compliance work will become routine. The same is true for training and protocols for field inspections and CTS data analysis. This audit was insightful in its observation on the need for training.

The recreational marijuana program is still growing with more than 1,200 new applications moving through our licensing approval process. Applicant interest in licensing continues to exceed expectations, cannabis supply is robust, and low consumer market prices are directly challenging illegal market sales in Oregon. As well, the recreational system's growth in sales to people who hold medical cards shows the regulated system can play an important role in providing reliable access to medical marijuana products.

In 2016, the OLCC's focus moved from meeting demand for licenses to enforcement of regulations. Security of the IT systems for licensing and tracking cannabis is vital to this work. OLCC is committed to make IT system improvements identified by the audit as rapidly as possible.

Response: Overall IT Security and Disaster Recovery Recommendations

The shortcomings of OLCC's overall IT security is not particularly surprising as OLCC continues to rely on legacy systems and generally has not modernized its agency-wide

systems at the same pace as the rest of state government. Over the years, the focus of IT staff has been to maintain fragile IT systems that operate vital warehouse inventory, orders, and financial processes. It was only a year ago, the agency retired the last of its COBOL systems.

In addition to marijuana IT systems, the OLCC is in process of deploying a Software as a Service (SaaS) alcohol licensing system and a SaaS system to improve the efficiency of privilege tax collections and auditing for beer and wine tax collections. The scoping, design and implementation of these projects have spanned the past two budget cycles. The agency has embraced the need to utilize industry standard IT across the entirety of the OLCC enterprise.

The IT security auditor's findings reflect a symptom of a general lack of management proficiency and capacity to maintain a focus on state requirements and practices. Executive staff have made it clear that they do not have the necessary expertise to manage the many specialized facets of IT that are critical to agency operations. Over the past two years, the agency and the executive team have pursued strategies to increase capacity, relieve staff of additional work by contracting for services, and providing the business case for securing approval for the position of a high-level CIO to oversee a rapidly growing portfolio of IT concerns.

The OLCC has a talented IT staff. The agency has hired a new IT division director and is positioned to get approval for a Chief Information Officer by the Legislature in 2018. In our response to the audit report, you will see that the staff has capably and quickly responded to many of the issues identified in the audit. With increased management, expertise, and direction, agency leadership expects this staff to excel.

The OLCC deeply appreciates the work of the audit team to clearly identify weaknesses in our security management program and to make specific recommendations for disaster recovery. The agency does not believe this is a difficult objective to meet. What the audit highlights is the fact that plans, inventories and procedures are not well documented. This is of concern to the agency, and the OLCC will work to ensure that complete plans and documentation for IT security and disaster recovery are created, used, and regularly updated.

The OLCC will be asking the Legislature to provide limitation for the agency to address two concerns highlighted by the report: $400,000 to replace unsupported servers and switches; and, position authority for a CIO ($197,000).

The following are OLCC's responses to the specific SOS audit recommendations concerning Overall IT security planning.

Detailed response to specific SOS Audit Division recommendations.

RECOMMENDATION 1
Develop and implement standards and protocols for on-site inspections and investigations.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	Aug. 1, 2018 & Ongoing	Shannon Hoffeditz, Director of Compliance, Tel. 503-872-5212

Narrative for Recommendation 1

The OLCC is working to update the Public Safety Division Compliance manual to include standards and protocols for marijuana inspections, and follow up on compliance issues. The Compliance Program wants to be proactive by developing a "feet on the street" approach so inspectors are inspecting businesses on a regular randomized basis. A different set of inspection standards will be established for the different types of licenses. In addition to the proactive inspections, the Compliance Division also conducts minor decoy operations, follows up on complaints generated from a variety of sources that includes but not limited to: citizen complaints, industry complaints, detected by Regulatory Specialists or referred by law enforcement. This process, however, will be ongoing as new rules and regulations are developed, the marijuana industry continues to evolve, and resources provided to the agency are adjusted.

RECOMMENDATION 2

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

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	Aug. 1, 2018 & Ongoing	Shannon Hoffeditz, Director of Compliance, Tel. 503-872-5212

Narrative for Recommendation 2

The OLCC will continually evaluate the adequacy of enforcement resources dedicated to marijuana. The OLCC has twenty-three regulatory specialist assigned to marijuana enforcement for 1,700 issued licenses. Currently the number of license applications is growing and OLCC expects to issue more than 2,000 license by the end of the 2018. The addition of new enforcement resources will require OLCC to go through the legislative budget process. OLCC is currently developing its budget request for the 2019-2021 biennium which will be submitted in July 2018. An evaluation of the need for additional inspectors will be in the agency's requested budget submission.

RECOMMENDATION 3

Perform risk-based on-site monitoring and inspections to ensure that licensees are reporting accurate information in the CTS and complying with applicable laws.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	Aug. 1, 2018 & Ongoing	Shannon Hoffeditz, Director of Compliance, Tel. 503-872-5212

Narrative for Recommendation 3
The OLCC is currently monitoring information in the Cannabis Tracking System, conducting follow up and issuing notices of warning and violations. There are currently some staff who are better versed in how to monitor the tracking system. The Regulatory Specialists are scheduled to be trained on the tracking system so they can adequately conduct inspections and follow up on tracking violations. The legislature provided additional resources to OLCC during the last legislative session for monitoring and compliance and those resources are currently being deployed. Risk based criteria will be developed and documented in the compliance manual.

RECOMMENDATION 4
Develop and implement policies and procedures for effectively monitoring software of service vendors to ensure they are meeting security and hosting requirements defined in contracts and service level agreements.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	Aug. 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 4
The OLCC IT Director will consult with the Department of Administrative Services Office of the State Chief Information Officer and other agencies to formalize a process for monitoring software service vendors to ensure that they are meeting hosting requirements defined in the contracts and service level agreement.

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.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation

Agree	Aug. 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 5

The data transfer process from the Marijuana Licensing System to the Cannabis Tracking System is undergoing review, and processes and reports will be developed as necessary to enable reconciliation of key data (e.g. licenses by status type) in the two systems by Marijuana program and/or Finance department personnel. The OLCC IT Director will develop and document a process once the review is completed.

RECOMMENDATION 6 Establish processes for granting and reviewing access to the Marijuana Licensing System and the Cannabis Tracking System.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Dec. 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 6

The OLCC IT Director will develop a process for granting access to the Marijuana Licensing System (MLS) and to the Cannabis Tracking System (CTS). This process will require review and possible amendments to OLCC Policy PP 845-155-004 (Employee Access to Information Assets) and be included in revision to the agency information security plan under recommendation 8.

RECOMMENDATION 7 Implement change management processes in line with industry best practices, including measures that ensure test data remains segregated from the production environment.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Feb 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 7
Policies and processes relating to third-party systems development and change management will be formalized by the OLCC IT Director, and will address test and production environment segregation and related issues. OLCC will work with the vendor to delete or segregate test data in the current system.

RECOMMENDATION 8 Update and test OLCC's information security plan to ensure the plan reflects the agency's current business and IT environment.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Aug 1, 2018	Bill Schuette, Economist/CAE/ASO 503-872-5023

Narrative for Recommendation 8
OLCC's information security plan will be updated to include the addition of the new marijuana licensing and tracking systems. OLCC will test the updated plan in this year's Business Continuity exercise.

RECOMMENDATION 9 Establish a process to maintain an up-to-date inventory of authorized hardware and software allowed on OLCCs network.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	June 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 9
The OLCC IT Director will formally document the software approved for use on the agency network. All hardware is currently authorized for use, but an inventory of IT hardware will be developed for use in monitoring obsolescence. OLCC will utilize MDM (mobile device management) and other client applications to keep an up-to-date inventory of authorized hardware and software allowed on the OLCC network. OLCC will also implement SOPHOS (https://www.sophos.com/en-us.aspx) and utilize its application control feature to block certain legitimate applications from running on work computers.

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Aug 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 10

The OLCC IT Director will 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. OLCC is in the process of updating and creating server and computer configuration baselines. OLCC currently has baseline configurations for all client laptops, desktops, and servers. OLCC will utilize SOPHOS (https://www.sophos.com/en-us.aspx) to help with monitoring configuration changes and to detect any unauthorized changes.

RECOMMENDATION 11 Develop and implement a process to scan for vulnerabilities on devices on the network.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Aug 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 11

The OLCC IT Director will develop, implement, and document a process to scan for vulnerabilities on devices on the network. The current plan is to implement Sophos Device Control which allows an administrator to manage the use of storage devices, network interfaces and media devices connected to all managed endpoints.

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.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	Aug 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 12

In consultation with DAS CIO, the OLCC IT Director will develop processes and obtain software as necessary to monitor device vulnerability on the OLCC network. OLCC is in the process of procuring Sophos. Sophos Endpoint Protection integrates a range of innovative technologies to secure Windows, Mac and Linux systems against malware and advanced threats such as targeted attacks.

RECOMMENDATION 13

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

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	Feb. 1, 2019	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 13

OLCC will work on a strategic plan to either procure, build or replace the older platforms. Replacement of obsolete platforms will require resources that will have to be procured through the budget process. OLCC will develop the request in the 2019-21 budget as a policy option package but implementation will not likely occur until next biennium. Segregation of unsupported servers will also require a strategic plan and resources. OLCC will develop a plan and costs for segregating servers and make a determination for the best course of action. Segregation of servers, given sufficient resources is expected to take six to twelve months to complete.

RECOMMENDATION 14

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

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation

Agree	June 1, 2018	Bill Schuette Economist/CAE/ASO 503-872-5023

Narrative for Recommendation 14
The keypad (PIN) functions for physical access to the OLCC headquarters will be disabled, and entry will only be permitted with an OLCC issued badge swiped at the access point.

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Aug. 1, 2018	Bill Schuette Economist/CAE/ASO 503-872-5023

Narrative for Recommendation 15
Weaknesses identified in risk assessments and audit findings will be tracked by the Chief Audit Executive (CAE) and brought to the agency's internal audit committee for report and review. The agency's security plan and posture will be reviewed annually by the agency security officer, administrative services manager and the information technology manager.

RECOMMENDATION 16 Develop and document an entity-wide disaster recovery plan.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Aug. 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 16
The OLCC IT Director will develop a formal disaster recovery plan for IT from existing documentation which will be incorporated to the agency's Emergency Plan (PP 845-155-009) and Business Continuity Plan (PP 845-155-008).

RECOMMENDATION 17 Perform periodic tests of backups to ensure usability.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	Aug. 1, 2018	Kai Nakashima, Acting IT Director* 503-872-5056

*Note that the contact point will change when OLCC's new IT Director is hired in February 2018

Narrative for Recommendation 17
The OLCC IT Director will create a backup and restore strategy, as well as testing backup and restore schedule. OLCC will verify the entire backup and restore process for disaster recovery purposes.

Conclusion:

The OLCC would like to thank the SOS Audit Division for its professional assessment of the OLCC Marijuana IT systems and of the agency's overall IT security measures. The recommendations are essential to program improvement and acknowledged by this thorough response. The recommendations are important to our future operations and the OLCC has offered detail plans and responses to identified issues.

We are taking immediate action to obtain the necessary approvals to help us remedy issues as rapidly as possible. As resource stretched as the agency is with the high profile implementation of the marijuana program and improving overall IT management, we look forward to a complete marijuana program performance audit in 2018.

Our agency's primary contact on the audit is Bill Schuette, OLCC Economist and Chief Audit Executive. He can be contacted at bill.schuette@oregon.gov , phone: 503-872-5023.

Sincerely,

Steve Marks
Executive Director
Oregon Liquor Control Commission