Secretary of State
Oregon Audits Division

Department of Administrative Services
Office of the State Chief Information Officer

Progress Has Been Made to Address Security Weaknesses at the State Data Center, but Improvements Are Still Needed

November 2018
2018-34

Secretary of State Dennis Richardson
Audits Division Director Kip Memmott

Secretary of State
Audit Highlights

November 2018

Department of Administrative Services, Office of the State Chief Information Officer

Progress Has Been Made to Address Security Weaknesses at the State Data Center, but Improvements Are Still Needed

Report Highlights

Security at the Enterprise Technology Services State Data Center (data center) has improved due to organizational and staffing changes and the increased role of the Enterprise Security Office. Several longstanding security challenges have been addressed, yet more work remains to further refine and improve security capabilities and to address other areas where roles are not sufficiently defined. The operating environment for the data center remains stable and appropriately controlled. Disaster recovery capabilities have improved, although prioritization of recovery order needs to occur to ensure that the most critical state systems can be restored timely in the event of a major disaster.

Background

The data center is comprised of an extensive inventory of computer operating system platforms and networks. It provides centralized computer services such as networking, email, backup, and server services for more than 100 state agencies, boards, and commissions. Since the creation of the data center in 2006, numerous prior audits have identified significant security weaknesses. Starting in 2015, organizational changes moved overall responsibility for the data center to the Office of the State Chief Information Officer (OSCIO) and expanded the staffing and role of the Enterprise Security Office.

Purpose

Because of the critical services the data center provides, we audit it every two to three years. This audit followed up on the status of prior audit findings and evaluated the current security framework and stability of the operating environment.

Key Findings

1. The OSCIO has made significant progress in improving security at the data center through security planning and staffing, vulnerability assessments, security event monitoring, and anti-malware and patching processes. Further progress is needed to refine these processes and better track vulnerability remediation.
2. Some security areas require improvement, including privileged access, asset and configuration management, and security incident response. Work is underway to improve Windows privileged access.
3. Day-to-day computing remains stable and disaster recovery capabilities have improved. While additional disaster recovery capabilities are being built, data center customers need to prioritize which systems should be recovered first in the event of disaster.

Recommendations

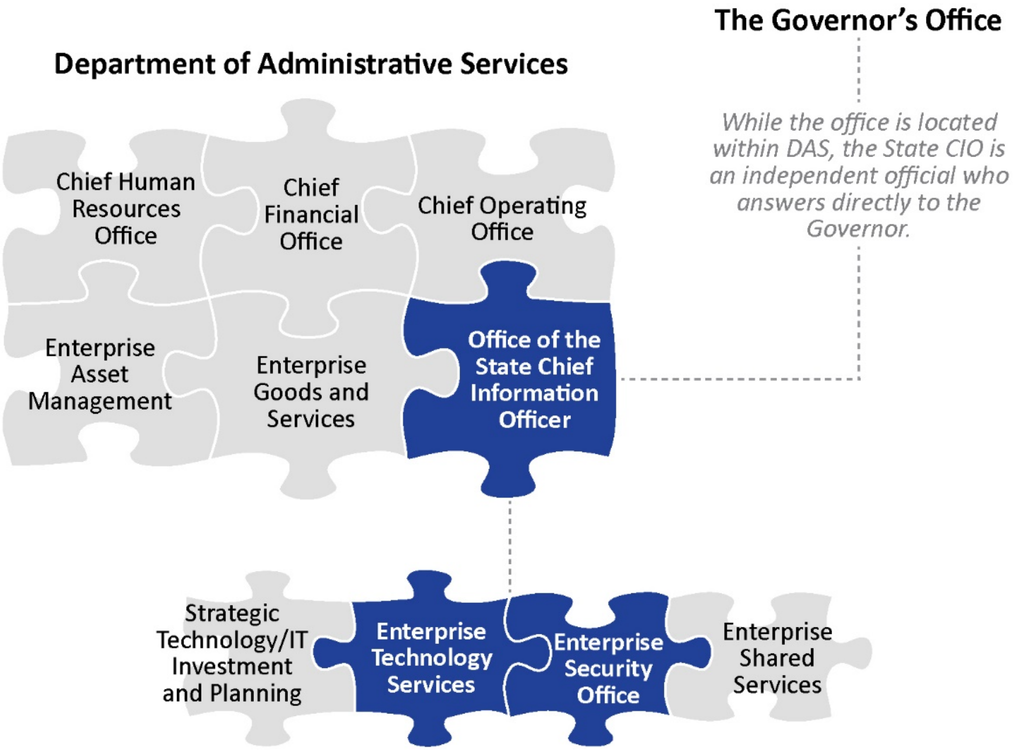
We recommend improvements in defining roles and responsibilities, refining vulnerability scanning and security event monitoring, monitoring privileged access, and disaster recovery prioritization.

The OSCIO agreed with all of our recommendations. The agency's response can be found at the end of the report.

Introduction

The Office of the State Chief Information Officer (OSCIO), which is organizationally a component unit of the Department of Administrative Services (DAS), is responsible for providing centralized computer services for state agencies through its Enterprise Technology Services State Data Center (data center). The data center is comprised of a complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure. More than 100 state agencies, boards, and commissions use the data center for various services, including networking, email, backup, mainframe, and server services. Agencies also use data center resources to operate hundreds of computer applications, including mission-critical systems that often contain citizens' confidential information, such as personal income tax returns, social security numbers, driver's license information, and confidential medical records.

The Enterprise Security Office, a division of the OSCIO, brings together elements of enterprise security — including governance, policy, procedure, and operations — under a single accountable organization. Resources within the Enterprise Security Office provide day-to-day enterprise security operations in the data center and a Security Operations Center for providing real-time security monitoring and response across the state.


The Governor's Office
Department of Administrative Services
While the office is located within DAS, the State CIO is an independent official who answers directly to the Governor.
Chief Human Resources Office
Chief Financial Office
Chief Operating Office
Enterprise Asset Management
Enterprise Goods and Services
Office of the State Chief Information Officer
Strategic Technology/IT Investment and Planning
Enterprise Technology Services
Enterprise Security Office
Enterprise Shared Services

Significant reorganization to the OSCIO changed the governance structure of the data center

Starting in 2015, significant changes have occurred that affect the organization and roles and responsibilities within the data center and state information technology governance and security as a whole. These changes included modifying the role of the State Chief Information Officer (CIO) and transferring security positions to the Enterprise Security Office.

House Bill 3099 changed the role of the State CIO and modified operational responsibility of the data center

Prior to 2015, the DAS director retained substantial authority over state information technology (IT) operations and policy, and the State CIO reported to the DAS director. Under this structure, the State CIO lacked independence and possessed only nominal authority over statewide IT policy. The State CIO had no authority over IT service delivery within the data center. Consequently, there was a notable disconnect between statewide IT security policy, which was driven by the Enterprise Security Office, and service delivery, which was provided by the data center.

In March 2015, the Governor reorganized leadership over statewide IT policy and operations, temporarily assigning operational responsibility for the data center to the State CIO. The temporary reassignment and delegation of joint authority over statewide IT policy and operations was made permanent upon the passage of House Bill 3099 in August 2015. The bill designated the State CIO as an independent official, directly responsible to the Governor as the primary advisor on statewide IT policy and operations.

This change also meant the data center and the Enterprise Security Office were both brought under the umbrella of the OSCIO. The role of the Enterprise Security Office expanded to include not only policy, but also operational responsibilities. Because of this, data center personnel assigned to security-related tasks transferred to the Enterprise Security Office. As a result of this change, Enterprise Security Office staffing increased from five to 26 positions by January 2016.

Senate Bill 90 transferred additional security resources to the Enterprise Security Office

In September 2016, the Governor signed Executive Order 16-13, which outlined a process to unify IT security functions for the majority of state agencies in order to protect and secure information entrusted to the State of Oregon.[1] The order directed executive state agencies to consolidate security functions and staffing into the OSCIO and to work with the newly consolidated group to develop and implement security plans, rules, policies, and standards adopted by the State CIO.

This order was made permanent by the passage of Senate Bill 90 in June 2017.[2] This change transferred 30 positions from state agencies and created five additional positions within the Enterprise Security Office. All transitioning agency personnel were operationally moved to the Enterprise Security Office by January 2018, though some individuals lent time back to their original agencies until July 2018. As of July 2018, the Enterprise Security Office had 56 positions, although not all of these were filled.

Multiple prior audits found little progress was made on security issues

The data center provides critical computing and networking resources to nearly all state agencies. As such, it has been the subject of frequent audits. We audited plans for the data center just prior to its completion in 2006 and have returned periodically to reevaluate controls. During these audits, we identified numerous security weaknesses that went unresolved for years. Until 2015, our audits identified security weaknesses at the data center with little actual movement to improve.

[1] Executive Order 16-13, "Unifying Cyber Security in Oregon"
[2] Senate Bill 90, "Transfers information technology security functions of certain state agencies in executive branch to State Chief Information Officer."

Historically, minimal action taken to address security weaknesses identified by audits

In September 2006, we issued an audit report that found project plans to create the data center were incomplete in part because they did not sufficiently address how critical security and disaster recovery services would be provided.[3]

In July 2008, after agencies moved computing infrastructure into the data center, we repeated our previous concerns regarding data center security in another audit report.[4] In that report, we communicated that the data center had not yet provided a secure computing environment for its clients. That conclusion was based on the detailed findings and recommendations we provided to data center management in an accompanying confidential audit report.

Our March 2010 audit found the data center had not resolved most of the security weaknesses reported in the previous audit.[5] We provided details in an accompanying confidential audit report. Because of the duration of these weaknesses, we expanded the audit work to determine why they were not resolved. We issued an additional report concluding that the governance structure was not effective for managing security at the data center.

In January 2012, we issued a confidential management letter in conjunction with our public management letter indicating that management had made little meaningful progress in resolving the security issues identified in prior audits.[6]

Governance changes began to make a positive difference in 2015

During an audit conducted and issued in 2015, we identified that actions had been taken to resolve longstanding security weaknesses.[7] This was based in part on the governance decisions that moved overall responsibility for the data center to the OSCIO.

During the current audit, we found the OSCIO has made significant progress in addressing these longstanding security weaknesses. Further progress is still needed to refine procedures and better define some roles and responsibilities.

[3] Report 2006-33, "Department of Administrative Services: Computing and Networking Infrastructure Consolidation Risk Assessment."

[4] Report 2008-21, "Department of Administrative Services: State Data Center Review."

[5] Report 2010-15, "State Data Center: Faster Progress Needed on Security Issues."

[6] Public Management Letter 107-2012-03-01

[7] Report 2015-20, "State Data Center: First steps to address longstanding security risks, much more to do."

Objective, Scope, and Methodology

Objective

Our audit objectives were to:

- Determine if the OSCIO provides an adequate security framework to protect agency and enterprise applications and data housed at or processed through the Enterprise Technology Services State Data Center.
- Determine if the data center provides a controlled and stable operating environment for agency and enterprise applications.

Scope

We focused our efforts on determining the status of prior audit findings and assessing controls in place during 2018. Our audit also included reviewing the status of critical areas not formally reported in our prior audit, but that were relevant to the security environment for systems operating at the data center.

Methodology

To address our audit objectives, we:

- reviewed policies and procedures;
- observed physical controls;
- reviewed various project, disaster recovery, and security plans;
- reviewed network drawings and inventory records;
- observed vulnerability scan results and dashboards;
- observed security information and event management rules and dashboards;
- analyzed volume data from security information and event management logs;
- compared computer inventory data to centralized patch management and anti-malware monitoring system records;
- observed central patch management and anti-malware dashboards; and
- interviewed Enterprise Security Office and data center staff regarding data center and security operations.

We determined the data used for patch management and anti-malware testing was sufficiently reliable by conducting interviews with knowledgeable officials, reviewing available documentation, and comparing each data source to the other data sources. We also followed up on potential negative test results with data center staff to validate the results.

To identify generally accepted control objectives and practices for information systems, we used ISACA's "COBIT" publications, the State of Oregon's "Statewide Information Security Standards" from March 2017, the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002 Second edition 2013-10-01 "Information Technology — Security Techniques — Code of practice for information security controls," the National Institute of Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and the Center for Internet Security publication "CIS Controls" Version 7.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

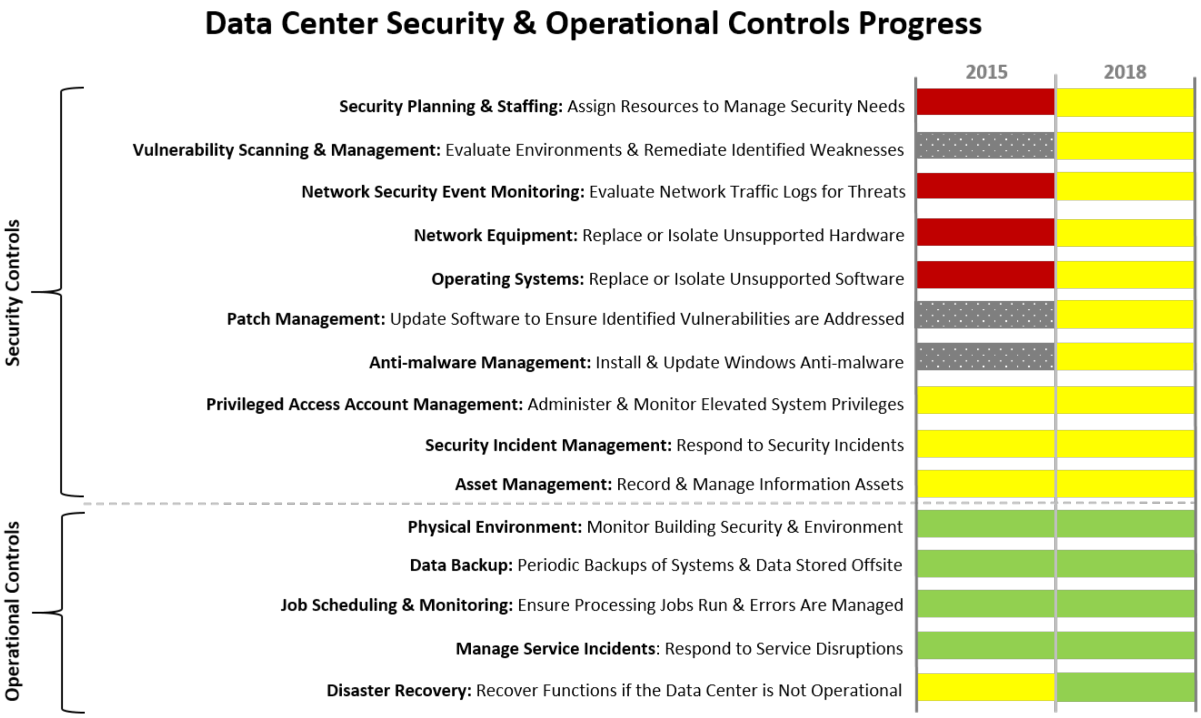
We sincerely appreciate the courtesies and cooperation extended by officials and employees of DAS and the OSCIO during the course of this audit.

Audit Results

The OSCIO has made significant progress to correct longstanding security weaknesses at the data center. We observed notable improvement in security planning and staffing, security event monitoring, vulnerability assessments, replacement of obsolete network devices and operating systems, anti-malware and patching processes, and disaster recovery. Other areas, such as asset management, security incident management, and privileged access management, only had modest improvement, but we considered the original risk in these areas to be lower than in the areas where the significant improvements were made. Further progress is still needed to refine these processes.

The following table illustrates our overall evaluation of risk associated with key audit areas between the 2015 audit and the current audit. During this audit, we compared prior findings to our current findings and assigned a risk level to illustrate the OSCIO's progress in each area identified in Figure 1.

Figure 1: The OSCIO has made progress in a number of areas since 2015



Data Center Security & Operational Controls Progress

		2015	2018
Security Controls	**Security Planning & Staffing:** Assign Resources to Manage Security Needs	🟥	🟨
	Vulnerability Scanning & Management: Evaluate Environments & Remediate Identified Weaknesses	▨	🟨
	Network Security Event Monitoring: Evaluate Network Traffic Logs for Threats	🟥	🟨
	Network Equipment: Replace or Isolate Unsupported Hardware	🟥	🟨
	Operating Systems: Replace or Isolate Unsupported Software	🟥	🟨
	Patch Management: Update Software to Ensure Identified Vulnerabilities are Addressed	▨	🟨
	Anti-malware Management: Install & Update Windows Anti-malware	▨	🟨
	Privileged Access Account Management: Administer & Monitor Elevated System Privileges	🟨	🟨
	Security Incident Management: Respond to Security Incidents	🟨	🟨
	Asset Management: Record & Manage Information Assets	🟨	🟨
Operational Controls	**Physical Environment:** Monitor Building Security & Environment	🟩	🟩
	Data Backup: Periodic Backups of Systems & Data Stored Offsite	🟩	🟩
	Job Scheduling & Monitoring: Ensure Processing Jobs Run & Errors Are Managed	🟩	🟩
	Manage Service Incidents: Respond to Service Disruptions	🟩	🟩
	Disaster Recovery: Recover Functions if the Data Center is Not Operational	🟨	🟩

Legend:

🟥 = **High Risk** (No one assigned, no processes in place, and/or many negative results from testing)

🟨 = **Medium Risk** (People assigned, processes in place but could be improved, and/or few negative results from testing)

🟩 = **Low Risk** (Although additional improvements still possible, people assigned, processes in place and functioning, and/or no significant negative results from testing)

▨ = **NA** (Not publicly reported during prior audit, rating is not applicable)

Source: Oregon Audits Division analysis of risk levels

Significant progress has been made to address critical security issues, but further work is still needed

Organizational and staffing changes, along with the increased role of the Enterprise Security Office, has improved the security environment at the data center. Through the efforts of the

Enterprise Security Office and the data center, the OSCIO has addressed several longstanding security weaknesses identified in prior audits through completed or ongoing projects and through assignment of staff to provide ongoing monitoring and support for the resulting implementations. Work is still needed to continue to expand capacity and to better define some roles and responsibilities.

Security planning has improved, but needs additional clarification of roles and responsibilities

Our 2015 audit report recommended developing a comprehensive security plan to address security weaknesses. The Enterprise Security Office recently released an updated security plan that the data center adopted. However, the plans lack details regarding how security measures will be enforced or accomplished under the state's shared security model.

Organizations should maintain an information security plan that describes how information security risk is to be managed and aligned with the enterprise strategy and information architecture. These plans should identify roles and responsibilities and provide enough detail to ensure that security functions are appropriately managed.

As part of their overall planning efforts, the Enterprise Security Office finalized a statewide security plan on August 1, 2018, to replace the existing plan last modified in 2009. The OSCIO requires Oregon executive branch agencies to adopt and comply with the plan, with any deviations or amendments articulated in an agency memorandum or addendum, respectively. The plan provides a good summary of best practice security controls and assigns agencies the responsibility of implementation. As such, agency plans need more detail regarding how they will implement and enforce controls in their environment, whether they articulate these in the plan addendum or whether they reference agency policies, procedures, or standards.

Although the data center is not a separate agency, it adopted the security plan along with a two-page addendum listing minimal changes and clarifications. The data center is in a unique position in the state in that it hosts the majority of the state's critical information systems, but it does not own those systems and does not have responsibility for the policies governing agency employees or agency systems and their use. However, because data center personnel provide services for agency-owned systems, some roles and responsibilities identified in the plan and addendum need more detail to identify how responsibilities are to be divided among the data center and the agencies whose systems it hosts.

Without a clear division of roles and responsibilities, some critical requirements may not be met because each entity may believe the other is performing the related tasks. For instance, the plan states: "Privileged user activity must be monitored, and specific behaviors alerted, for example, when a privileged user attempts to increase privileges, when a privileged user attempts to modify logs, and when a privileged user attempts to create another account, or assign privileges." [8] The plan and data center addendum do not provide additional detail to indicate how alerts will be configured or monitored or who should perform those duties. Identifying the responsible entity is especially relevant because both agency and data center personnel have privileged access to agency systems.

[8] Privileged users are those with privileged access, which refers to the ability of a user to take actions that may affect computing systems, network communications, or the accounts, files, data, or processes of other users. Privileged access implies greater access than the average end user.

Security staffing has improved, although some roles should be better clarified

Prior audits found security initiatives were not always properly staffed and therefore were never fully implemented. We recommended clearly defining and assigning data center security roles and providing sufficient human resources to carry out critical security functions. During the current audit, we identified improvement in the assignment of resources. Even so, there are some areas where responsibilities should be better clarified or assigned.

Since the prior audit, Enterprise Security Office staffing has increased. Data center staff performing security functions, such as reviewing potential security incident alerts or modifying firewall rules, moved to the Enterprise Security Office, along with those responsibilities. In addition, Senate Bill 90 transferred security positions from agencies to the Enterprise Security Office. During these transitions, the Enterprise Security Office prioritized training security personnel and continued to develop and modify their organization to plan for how these individuals would be assigned and used.

Based on our evaluation of staffing at both the Enterprise Security Office and the data center as it related to critical areas of security, we concluded the OSCIO has appropriately allocated critical information security responsibilities in most, but not all, areas as it pertains to operations at the data center.

Specifically, it has appropriately assigned personnel to:

- monitor and respond to potential security incidents and events through monitoring of the security information and event monitoring system feed;
- conduct regular vulnerability scans;
- process and grant requests for privileged access to systems on a centralized basis;
- provide central patch management to Windows servers and other platforms based on defined change management processes, including having exception processes for systems not following the normal procedures; and
- provide central anti-malware management for Windows servers, including an exception process for systems not following the normal procedures.

In other areas, roles are less clear or have not been sufficiently assigned. For example, roles should be better clarified for security incident response and for review and monitoring of privileged access membership and activities. In addition, overall information security responsibilities at the data center are not clearly defined. Per discussions with data center and Enterprise Security Office management, overall information security responsibility for the data center ultimately resides with the State Chief Information Security Officer, but this is not defined in the data center plan addendum.

Without clear identification and assignment of roles, intended activities to secure the environment may not occur or be properly managed.

Vulnerability scans occur regularly at the data center, but tracking could improve

Although not publicly reported, the prior audit found that while some initial work had begun, vulnerability scans were not being conducted. The current audit found significant improvement in this area as the data center currently conducts scans of most of its environments. However, coverage is incomplete, and the results are not completely tracked over time to ensure all critical vulnerabilities are being addressed timely.

When security researchers or vendors identify new vulnerabilities in software, they report them to the community at large so that these vulnerabilities may be fixed. Attackers may also receive this information and develop exploit code to launch against targets of interest. Because of this, organizations should periodically scan their environments to identify any vulnerabilities that should be remediated through system software patches or other remediation strategies.

Over the last several years, the Enterprise Security Office installed vulnerability scanners on agency networks. Currently, the data center runs monthly scans on its Windows servers and quarterly scans on its network devices, unless federal requirements require more frequent scans. It has not yet implemented regular scanning on all computing platforms.

Vulnerability scanning
The Enterprise Security Office has provided a vulnerability discovery tool for agencies to identify missing patches, unsupported software, and common system misconfigurations. State agencies are required to conduct vulnerability scans on their environments.

In addition, while data center personnel report they remediate weaknesses identified in these scans, there is little documentation available to demonstrate this remediation is occurring timely. Review of various monthly reports provided by the Enterprise Security Office to the data center shows a downward trend of critical vulnerabilities, but the number of devices scanned can fluctuate over time due to errors and it is difficult to identify consistent patterns. Further, we noted some vulnerabilities appear on multiple reports and date back months. The number of devices tied to such issues has tended to decrease over time, but the data center does not directly tie remediation plans back to identified vulnerabilities, so there is less assurance that all critical vulnerabilities are being addressed. Data center staff stated that some vulnerabilities identified represented false positives, and that they discuss each one, but do not document or track them.

In part, tracking does not take place because data center personnel had not identified a need or a method to track specific vulnerabilities. They indicated that the scanning tool itself does not retain history, only the current scan results. While this is helpful for showing the real time state of system vulnerabilities, it does not provide a method to track whether all vulnerabilities are being remediated timely.

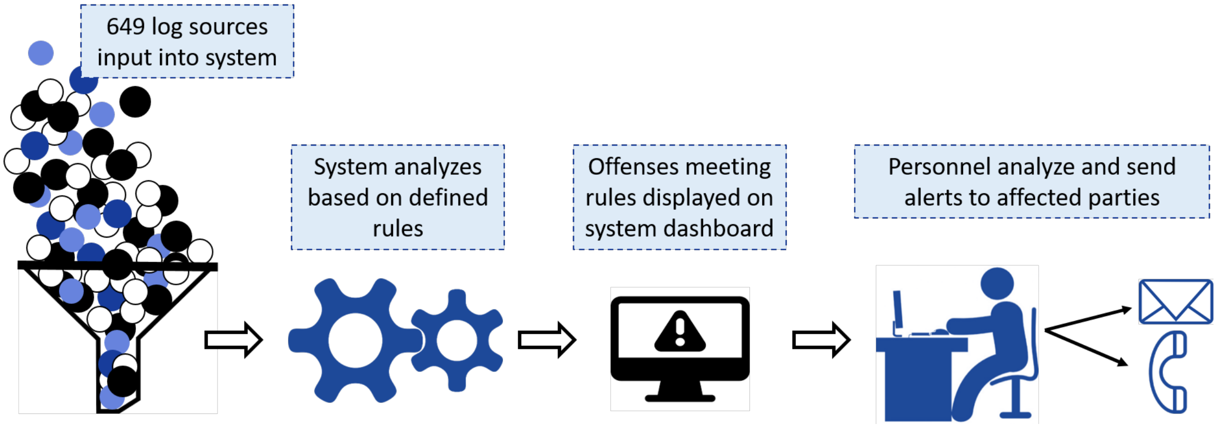
Without tracking of identified vulnerabilities and documentation of associated remediation strategies, there is less assurance that critical vulnerabilities will be addressed timely. While some vulnerabilities carry little risk, others can make state systems more susceptible to outside attacks.

Security information and event monitoring system is implemented, but not all capabilities are in place and results are not measured

Prior audits identified that various hardware and software had been purchased to monitor logs of activities on the state's network, but systems were never fully implemented or appropriately staffed. Since the 2015 audit, the Enterprise Security Office made significant progress by implementing a monitoring system and assigning staff to monitor the traffic to identify whether alerts should be generated for potentially affected agencies. Although this represents a major improvement to the security stance of the state, more work is needed to add capabilities and to measure and report results to demonstrate and improve its effectiveness.

One method for detecting potential attacks on an organization is to deploy and monitor a system for log correlation and analysis. This type of system obtains log data from networking or computing devices and analyzes the traffic to detect possible threats. A category of tools that provides this analysis is a security information and event monitoring system, also known as a SIEM system.

Figure 2: The security information and event monitoring system analyzes logs and provides information for personnel to send alerts regarding suspicious traffic


649 log sources input into system
System analyzes based on defined rules
Offenses meeting rules displayed on system dashboard
Personnel analyze and send alerts to affected parties

Since the data center purchased a security information and event monitoring system in 2015, significant work has been done to implement it for use on the state's network. Enterprise Security Office staff now operate and monitor the system, which was receiving information from 649 log sources as of May 2018, including the main firewalls and other network devices. Over one three-hour period, the product received and analyzed over 26 million log entries. The system applies rules to these log entries to identify patterns that could signal a possible threat or attack, with a focus on comparing information from one log to information from another log, which is known as log correlation. When the system identifies a possible threat or attack, it displays the offense information on-screen to staff monitoring the traffic. Staff investigate the offenses and determine whether they should alert other entities, such as an agency that experienced the suspicious network traffic. Enterprise Security Office staff estimated that the system presents approximately 75 offenses per day, resulting in one or two alerts per day.

Staff could not provide actual numbers for the number of offenses and alerts received from the system because they are not adequately tracking activities associated with monitoring and reporting potential problems. In addition, analysts change rules periodically to eliminate or reduce false positives and improve the system's pattern recognition abilities. However, there are no formal processes followed to ensure only needed changes are made or that changes are effective. Enterprise Security Office staff indicated processes and standard operating procedures will be developed as they continue with efforts to build the Security Operations Center in the Enterprise Security Office.

The current implementation of the security information and event monitoring system does not include all available log sources, partially due to capacity constraints. To address this, the Enterprise Security Office has identified a need for an additional logging aggregation system to receive network management data from different systems and forward it to the security information and event monitoring system for further analysis.

Without a complete log aggregation and correlation solution, the Enterprise Security Office may not be sufficiently identifying and monitoring risky network traffic. Without tracking results generated by the existing product, the Enterprise Security Office will be unable to demonstrate whether the system effectively identifies potential problems and track which of these potential problems represent actionable alerts. Such tracking would likely help improve development of further rules to more accurately identify which traffic problems are more likely to represent problems and increase the efficiency of the system analysis.

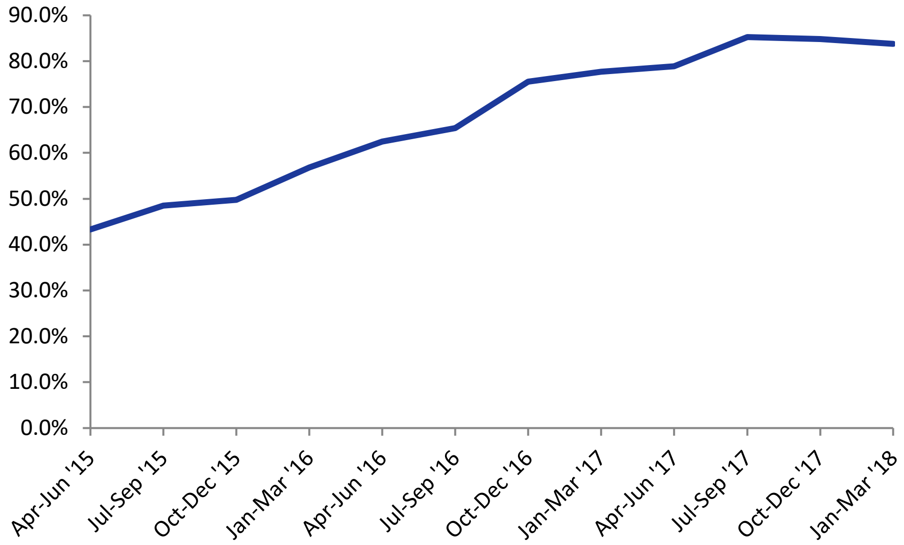
Progress has been made to eliminate out-of-support networking equipment, but work remains to continue lifecycle management

Prior audits identified that efforts to replace networking equipment no longer supported by the vendor were underway, but that those efforts were not complete. During the current audit, we identified that many of these replacements had been completed. However, these lifecycle replacements have been handled on a project-by-project basis without the development of an ongoing lifecycle management program funded to ensure critical equipment continues to be replaced timely.

To ensure ongoing technical support is available, network hardware needs to be replaced when it is no longer supported by its vendor. In addition, unsupported equipment will not be covered under support contracts if it breaks.

Data center management requested and received funds in 2014 to replace hardware and other computing equipment. At the time, the project was expected to continue well through 2016. Currently, the data center and the Enterprise Security Office reports they have replaced over 2,400 networking devices, with plans underway to replace an additional 232 pieces of equipment. These efforts have improved the average age of equipment from our prior audits. Between June 2015 and March 2018, the data center reported the percentage of its assets that were less than five years old, which includes both server and networking equipment, improved from 43% of its assets to almost 84%. The data center's current target for this statistic is 80% of assets. As part of lifecycle planning, the data center identified an additional 770 networking devices that should be replaced during the current biennium. Data center management indicated these devices will be replaced as part of funded operational work by the end of the biennium.

Figure 3: The percentage of data center server and network assets less than five years old has increased



Source: Enterprise Technology Services Key Performance Measure Scorecard

Lifecycle replacement will continue to be an ongoing need for the data center and the Enterprise Security Office. Data center managers indicated the data center has never been sufficiently funded for ongoing lifecycle replacement or for growth in general. As a result, they have needed to address replacement efforts through individual projects instead of having ongoing budgetary support to allow for these activities. While this is a viable option for replacing equipment, it increases the risk that the data center and the Enterprise Security Office will not receive approval or funding for future replacement efforts, and that equipment will not be replaced timely. This could lead to security risks through unsupported networking equipment and increased risk of hardware failure that disrupts state services.

Progress has been made to eliminate out-of-support operating systems, but work remains to continue lifecycle management and develop isolation solutions

Prior audits identified that the data center housed multiple systems with unsupported operating systems. Unsupported operating systems do not receive vendor updates to patch critical security weaknesses. During the current audit, we noted the data center has made progress eliminating out-of-support operating systems but some unsupported operating systems remain on the state's network.

Security standards indicate organizations should have strategies for ensuring operating system software is appropriately updated to reduce the risk that known weaknesses could be used to compromise computer systems. When operating systems are no longer supported by vendors, they do not issue security patches, meaning any new identified vulnerabilities will not be fixed using vendor patches. Such systems provide a risk to the entire environment in which they reside.

Operating system age has improved
The number of Windows and Linux servers has increased by about 80% since 2015, and the number of obsolete operating systems in use has decreased by over 60%.

During the prior audit, we noted that about 175 Windows and Linux servers were out of support, out of approximately 2,000 servers. Most of those unsupported versions were Linux servers, as none of the Linux servers were being supported centrally by data center staff. For the current audit, we identified approximately 3,600 Linux and Windows servers, with fewer than 70 unsupported operating systems, most of which were also Linux.

In contrast to the prior audit, nearly half of the current inventory of Linux servers are now managed by data center administrators using centralized management software that allows them to apply patches, grant access to privileged users, and actively maintain the configuration of the servers. All of the Linux servers being centrally managed by data center administrators have up-to-date operating systems. The remaining servers are minimally supported on a "best effort" basis, and in some cases data center personnel have no ability to access the servers, meaning the agency or entity that built the server would be solely responsible for maintaining it. More than half of these servers have older operating systems no longer supported by their vendors.

For the Windows environment, the data center worked with its customers to transition their servers from the unsupported operating system version identified during the prior audit, and none currently remain. Since the last audit, another version of Windows has moved out of support, and five servers hosted at the data center have not yet been upgraded to a newer version. For these servers, the data center receives "critical" security updates and legacy modernization consulting services under a custom support agreement with Microsoft costing over $1 million for the next year. Under the agreement, "important" security updates are optional and could be applied for an additional fee. Agencies using these servers pay the cost of the agreement and any additional fees. The decision to upgrade operating systems to supported versions is the agency's responsibility. The data center periodically presents lifecycle planning status information to agencies to inform them of the planned supported path for various system platforms to assist agencies in their planning efforts.

Using obsolete operating systems increases the risk that computer programs and data residing on them could be compromised. This risk may extend beyond these servers, potentially allowing intruders access to other computer systems attached to them. The risks posed by obsolete operating systems could be reduced by isolating the affected servers on a network not connected to other systems. However, while data center and Enterprise Security Office managers have generally discussed isolation strategies, they have not taken steps to build such an environment.

Windows patching and anti-malware management is automated and monitored for most servers, but some gaps remain

Statewide security standards require all servers running Microsoft Windows operating systems to have anti-malware software installed to protect systems from malicious software.[9] In addition, organizations should apply vendor supplied patches to operating systems to correct identified software vulnerabilities. Failure to scan systems periodically for malware or to ensure software patches are applied timely increases the risk that systems could be breached.

Since our last audit, the data center replaced the software product used to facilitate automated patching, and has implemented an exception process to document servers not following normal patch or anti-malware processes. We compared the list of deployed servers in the inventory tracking tool to servers being covered by centralized patching and anti-malware software to identify whether the software and supporting processes and procedures were functioning as intended.

We found that 99% of deployed servers were being managed through the automated patching software, or were being managed manually but represented known exceptions, although not all exceptions had been formally documented. The remaining 1% of servers were not being managed under the central patching solution, but data center staff reported they have now corrected these.

99% of deployed Windows servers were appropriately managed using central patching and anti-malware management software, or represented known exceptions to central management.

Of the servers patched through the automated software, dashboards showed that 99% were up-to-date with critical patches. Data center staff follow up on missing patches to ensure missing patches are applied as needed.

In addition to automated operating system patching, the data center uses centrally managed anti-malware software installed on servers. We found 99% of servers were centrally managed or were known exceptions, although not always documented as such on exception forms. At the time of our review, 1% were not being managed by the central solution but data center staff indicated they have now corrected these servers. Data center staff also monitor anti-malware dashboards showing whether servers are reporting security risk detections.

These results illustrate that data center staff monitor almost all Windows servers to ensure patching and anti-malware coverage, although some minor gaps remain. The gaps were due to oversights in documenting exceptions for internally managed servers and a lack of formal review to identify servers not currently being covered by the automated solutions.

Monitoring and managing users with special access is inadequate

Our 2015 audit noted weaknesses in the assignment of special access and monitoring of activities of privileged users. Our current audit found that data center managers developed, but have not yet implemented, new processes to periodically review who has privileged access.

[9] Anti-malware is a type of software program designed to prevent, detect, and remove malicious software on information technology systems.

In addition, there are still very few procedures in place to monitor the actions of privileged users. A project is underway to improve these weaknesses in the Windows environment.

Data center personnel responsible for maintaining systems and networks need comprehensive access to perform their job functions. This special access is generally referred to as privileged access and allows such users to view or alter everything on a system, including system data. Best practices for security indicate that all privileged users should be authorized and their actions closely monitored.

The data center has developed processes and procedures for granting privileged access to its various operating platforms. These procedures cover both data center and customer agency staff. If followed, these procedures are sufficient to ensure that privileged users have had their access requested by authorized parties and to document when privileged access was granted or removed.

In addition, the data center developed procedures requiring periodic review of assignment of privileged access, but data center personnel reported they do not receive the information necessary to perform the reviews. Another procedure compares membership of Windows privileged access groups with membership from the day before, but this procedure does not identify users added and removed during a single day and does not identify the creation of new groups providing privileged access.

Some authentication information is being sent to the security information and event monitoring system for analysis, and some actions generate emails to administrators regarding activity, such as failed logins. However, other actions — such as creating a new group that has privileged access, reviewing whether data has been modified, or modifying system configuration settings — are logged but only reviewed when personnel are investigating a problem. Management indicated that a current project to improve privileged access assignment and management for the Windows environment will also provide improved alerting for actions taken by data center privileged users. However, the project is not expected to be completed until 2019.

We examined privileged access records and found three users who no longer work at the data center who had been assigned some level of privileged access. These users retained access because procedures to remove it had not been fully followed by managers and no review was performed to identify that the access of these individuals had not been removed when expected. Without periodic review of privileged user assignments or actions, there is higher risk that privileged access users could make unauthorized changes to systems and data without being detected.

Information security incident response procedures need updates to reflect current operations

The prior audit also noted that potential information security incidents were not sufficiently tracked. The data center has since developed an information security incident response plan, but elements of it have not been implemented. Roles and responsibilities for data center and Enterprise Security Office personnel have not been sufficiently defined for security incident response. In addition, the Enterprise Security Office has not documented standard operating procedures for managing information security incidents.

Security standards indicate that responsibilities and procedures should be in place to handle information security incidents once they have been identified and reported to management. Best practices also indicate that organizations should develop standard operating procedures to guide incident responders on different types of potential information security incidents, such as a significant malware attack as opposed to a loss of personally identifiable information.

After the last audit was completed, the Enterprise Security Office and the data center both published information security incident response plans. These plans provide high-level guidance regarding how information security incidents are identified, how severity levels are assigned, and how they are reported and managed. Both plans also reference the State Incident Response Team, which is led by Enterprise Security Office personnel but can also include different members for each incident, depending on the agency involved and the type of incident.

We found the plans were not fully implemented. For example, the data center security management plan indicates potential information security incidents will be tracked on a "sightings log" by the Enterprise Security Office, but this type of log does not exist. The Enterprise Security Office only tracks declared information security incidents, not potential incidents that, taken together, could indicate a larger pattern. This is also true for potential incidents identified through the security information and event monitoring system, which are only formally tracked if Enterprise Security Office staff recorded them as alerts.

We noted uncertainty regarding roles and responsibilities that would be filled by data center and Enterprise Security Office personnel in the event of an information security incident. The plans contain definitions of roles and responsibilities, although they emphasize flexibility based on the type and severity of the incident.[10] Plans indicate that data center personnel will inform the Enterprise Security Office of a potential information security incident, and if it is identified as an actual information security incident, the Enterprise Security Office takes the lead and provides any further documentation. If it is determined to be a service incident rather than a reportable information security incident, the data center resolves it using their existing service incident management procedures.[11] This leaves room for uncertainty regarding roles between the two entities, in particular in relation to lower-level information security incidents that do not involve activating the Security Incident Response Team, and as it pertains to documenting steps and actions taken.

In addition, the plans are not supported by detailed documented procedures to guide responders. The Enterprise Security Office indicated they have staff who have experience managing information security incidents, and that these types of incidents require flexibility. Due to this, and due to the significant growth in the Enterprise Security Office and continued reorganizations, supporting procedures have not yet been developed. We also noted that at least 14 of the Enterprise Security Office staff previously worked at the data center. This provides an additional blending of previous roles and responsibilities. However, while flexibility and experienced staff are critical, procedures should be defined so that the loss of key individuals from an organization would not result in significant reduction in its ability to respond.

Lack of agreed-upon roles and responsibilities and lack of detailed standard operating procedures increases the risk that information security incidents will not be managed efficiently or effectively. Data center and Enterprise Security Office staff are less likely to notice patterns of ongoing or persistent attacks without a process for tracking or evaluating them.

[10] A "service incident" is defined as an event which is not part of the standard operation of a service and which causes, or may cause an interruption to, or a reduction in the quality of, that service. An "information security incident" is defined as a single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets, and agency, or third party and requires non-routing preventative or corrective action. An "information security event" is defined as an observable, measurable occurrence involving an information asset that is a deviation from normal operations.

[11] To be reportable, the incident or event must involve information security, be unwanted or unexpected, show harm, intent to harm, or significant threat of harm, and require non-routine action for response. For example, a loss of network connectivity could be due to hardware failure or due to a denial of service attack. The former case would be managed as a service incident, while the latter should be handled as an information security incident.

Asset and configuration management is manual and subject to errors

The prior audit noted that a complete inventory of system configurations had not been adequately maintained and monitored. During this audit, we noted that asset and configuration item inventories continue to be maintained manually, which makes them more subject to errors.

In order to properly secure and manage their environment, organizations need to understand what devices are on their network and maintain updated inventories of these devices and how they relate to one another. Ideally, asset inventories should be automated and tied to several data sources.

The data center maintains an inventory of computers and network devices through manual data entry into an open source software tool. While the data center has processes to ensure new devices and servers are documented using this tool, the manual nature means it is more subject to errors. For example, we found that operating systems recorded in the inventory were not always up-to-date. There is also a higher risk that devices or servers could be added to the environment that were not recorded. Incorrect or incomplete records could result in incorrect billing for data center services to customers, since information from the inventory system is used as part of the billing process.

Day-to-day computing remained stable and disaster recovery improved

We also evaluated the data center's ability to meet the day-to-day needs of state agencies relying on its services. Specifically, data center management and staff continued to:

- monitor and control the physical environment to limit physical access and protect computing resources from environmental hazards, such as excessive heat and humidity;
- provide routine back-ups for agency computer programs;
- monitor computer processing to ensure production problems are identified and resolved; and
- manage service incidents using detailed defined procedures.

Disaster recovery planning and documentation has improved, but restoration prioritization is still needed

The prior audit noted significant progress in disaster recovery capabilities at the data center, but noted these efforts remained incomplete and testing did not occur on all system platforms. Since that time, the data center has made additional progress and performed disaster recovery tests of all platforms, restored isolated environments for two agencies, and plans to invite customers to participate in future annual tests. However, it does not currently have sufficient capacity and infrastructure to restore all agency applications and data. In addition, priorities among agencies have not been established to ensure that the state's most critical applications are recovered first.

Restoring data center operations after a disaster or serious disruption requires significant advance planning, coordination, and testing. In addition, data backups stored off-site should be protected against loss or inappropriate disclosure.

In 2012, as part of the data center's disaster recovery strategy, it entered into an inter-governmental contract with the state of Montana, allowing replication of its computing environment and data off-site at the Helena Montana State Data Center. This provided the data center with needed infrastructure for disaster planning, coordination, and testing, and a secure location for storage of redundant data backup files. Data center staff reported the physical security of the facility is audited regularly by the Internal Revenue Service, and that they and other agencies have visited the facility and observed physical security measures in operation.

Since the prior audit, the data center has made additional strides in maturing its disaster recovery processes. All major system platforms now have some infrastructure replicated in Montana. In October 2017, the data center held a functional test that assumed the loss of both internet access and the data center building. This test involved all major system platforms and included restoring network connectivity along with selected applications and data for the tested systems. The data center partnered with two agencies during this test and successfully created an isolated environment for each in Montana. Data center staff is currently planning the next test, scheduled for October 2018, and plans to conduct tests going forward at least annually.

A data center disaster recovery planning document noted that additional work is needed to add capacity and upgrade networking equipment in Montana. In addition, data center personnel indicated current capacity does not support the complete restoration of all applications on all system platforms. For example, the Windows environment in Montana currently supports approximately half of the servers operating at the data center. Because of these restrictions, data center customers need to work together to prioritize the applications and services to be restored so that the most critical applications are recovered first. This prioritization has not yet occurred and is outside the scope of the data center's responsibilities. It will require a coordinated effort with their customers.

Recommendations

To further improve the security framework for the data center, we recommend OSCIO management:

1. Clarify the information security roles of data center personnel pertaining to security requirements defined in the information security plan and overall responsibility for security at the data center.

2. Improve tracking of remediation efforts to mitigate critical vulnerabilities detected by scans.

3. Improve implementation and capabilities of the security information and event monitoring system by:
    a. developing metrics to measure and track volume and content of logs and associated offenses generated by the system;
    b. developing procedures to modify system rules; and
    c. continuing to build capacity to manage additional log sources for input and analysis in the system.

4. Request funding from the Legislature to implement networking and security equipment lifecycle replacement as an ongoing program as opposed to individual projects.

5. Develop and implement solutions to isolate operating system environments that are not fully supported by vendors.

6. Periodically reconcile installation of anti-malware and patch management agents on Windows servers with applicable servers in its inventory to ensure full coverage.

7. Enforce existing procedures requiring periodic review of privileged access membership.

8. Develop additional alerts to monitor actions taken by privileged access users, as required by the statewide security plan and standards.

9. Further define procedures for security incident response, including:
    a. better defining roles and responsibilities for security incident response between the Enterprise Security Office and the data center;
    b. ensuring that potential security incidents are tracked to enable additional analysis; and
    c. developing standard operating procedures for responding to different types of security incidents.

10. Identify and implement an automated solution for asset inventory and configuration management.

11. Work with state agencies dependent upon the data center for disaster recovery and ensure priorities for recovery are identified.

Oregon
Kate Brown, Governor

Department of Administrative Services
Chief Information Office
155 Cottage St NE, 4th Floor
Salem, OR 97301
PHONE: 503-378-3175
FAX: 503-378-3795

22 October 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 Audits Division's final draft audit report titled **"Department of Administrative Services, Office of the State Chief Information Security Officer: Progress has been made to address security weaknesses at the State Data Center, but improvements are still needed."**

Centralized Security Responsibility of the Data Center Yields Significant Progress

Prior to 2015, audits of the state data center (SDC), operated by Enterprise Technology Services (ETS), consistently found numerous and unresolved security weaknesses. For years, little progress was made in addressing the findings and recommendations identified by the Secretary of State.

In 2015, by executive order of Governor Kate Brown and later confirmed in statute, the State Chief Information Officer (CIO) has been responsible for operation and security of ETS and the SDC. With this change, the CIO directed the State Chief Information Security Officer (CISO) and the Enterprise Security Office (ESO) to drive security improvements at the SDC and provide any security services necessary to ensure the SDC operated in a secure manner. Security remediation efforts were initiated immediately, some of which were noted in the SDC Audit by the Secretary of State in 2015.

The majority of Oregon's state agencies now have unified IT security functions. This is designed to provide consistent protection and security for information entrusted to the State of Oregon. Strong CIO leadership coupled organizational focus on security by ETS and the increased role of the ESO have ushered in solid and measurable improvements to security at the SDC.

The CIO, SDC Administrator and CISO have reviewed these audit results and generally agree with the findings and recommendations.

Response to Audit Results

Significant progress has been made to address critical security issues, but further work is still needed.

We are in agreement with the findings and the recommendations made by the Secretary of State auditors. The findings confirm our significant progress and the recommendations are well-aligned to the plans already in place to further mature the security of the State Data Center. Most of these recommendations are already in progress, although some require budget approval in the coming legislative session or completion of long-term projects before they can be fully addressed.

Below is a detailed response to each recommendation in the audit.

RECOMMENDATION 1

Clarify the information security roles of data center personnel pertaining to security requirements defined in the information security plan and overall responsibility for security at the data center.

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 2019	David McMorries 503-373-0210

Narrative for Recommendation 1

The first stage in addressing security concerns at the SDC was establishing critical security capabilities that were missing, which the findings of this audit confirm have been addressed. The next stage is to mature those services from ad-hoc to fully documented and tested capabilities, including clear documentation of roles & responsibilities. The ESO will work in partnership with ETS to drive to this next level of maturity across security relevant operations through the end of the 2017-19 biennium.

RECOMMENDATION 2

Improve tracking of remediation efforts to mitigate critical vulnerabilities detected by scans.

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	October 2019	Shawn Wagoner 503-373-2142

Narrative for Recommendation 2
Vulnerability remediation is taking place consistently at the SDC, as reflected in the audit findings. The SDC is currently managing vulnerabilities to a level which exceeds current state standards and has consistently maintained that level in monthly regular scan results. Processes to improve vulnerability management coordination between the SDC and agencies are under development and will be supported by the OSCIO Information Technology Service Management (ITSM) project. The ITSM project will deliver a modernized ticketing and workflow management platform the improved processes can take full advantage of.

A policy option package has been submitted in the 2019-21 legislative session to permanently staff this lack of capacity to ensure dedicated focus to security vulnerabilities in SDC managed systems is put in place. This resource will establish a system for tracking vulnerabilities to closure, leveraging the SDC's implementation of the OSCIO ITSM platform that will replace the existing SDC ticket tracking system.

RECOMMENDATION 3

Improve implementation and capabilities of the security information and event monitoring system by:

a. Developing metrics to measure and track volume and content of logs and associated offenses generated by the system;
b. Developing procedures to modify system rules; and
c. Continuing to build capacity to manage additional log sources for input and analysis in the 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	October 2019	Mark Johnston 503-947-0488

Narrative for Recommendation 3

The Enterprise Security Office (ESO) Security Operations Center (SOC) currently manages the security information and event management (SIEM) system that supports the state data center. The SOC is still early in its development, so detailed metrics and documented procedures are still being developed. Metrics will be established that will include the log information (type, contents, volume, etc.), as well as the related alerts and incidents generated from these logs. SOC development activities include the completion and documentation of formal operating procedures including, but not limited to, change management for SIEM rules. Specific requirements and controls around rule changes and/or changes to SIEM configuration will be documented in the coming months.

Both short and long-term plans for the enterprise SIEM include expansion to handle both the physical requirements for the growing number and sizes of logs, as well as the processing capability to perform the necessary analysis to generate alerts. A policy option package to fund additional needed log capacity to serve SDC needs has been submitted for consideration in the 2019 legislative session.

RECOMMENDATION 4

Request funding from the Legislature to implement networking and security equipment life cycle replacement as an ongoing program as opposed to individual projects.

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	2019 Legislative Session	Shawn Wagoner 503-373-2142

Narrative for Recommendation 4

Funding has been requested in a policy option package in the 2019 legislative session to provide ongoing operating budget to sustain lifecycle replacement costs for security equipment - specifically, funding for firewall lifecycle. As new security solutions are implemented, funding requests will include budget provisions for on-going support of the entire lifecycle of the assets from concept to replacement. Discussions have been initiated to consider moving these resources to a lease model to ensure they are regularly refreshed automatically, rather than requiring periodic capital investment, which often includes delays in replacing older infrastructure.

RECOMMENDATION 5

Develop and implement solutions to isolate operating system environments that are not fully supported by vendors.

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
Partially Agree	June 2020	Shawn Wagoner 503-373-2142

Narrative for Recommendation 5

Management partially agrees with this recommendation, as hosted agencies drive this need. A more complete solution would involve a change in policy, such as the introduction of an Authority to Operate process, or other governance that would require compliance at the risk of application isolation from the Oregon Government Enterprise. In the absence of this kind of control, ESO standards prohibit the use of obsolete or non-vendor supported operating. Due to agency resourcing shortfalls, exceptions are sometimes granted to temporarily support business needs. ESO will formalize the exception process over the coming months. In addition to tracking of exceptions, a technical scheme for isolating systems that remain outside of state standards is necessary to protect the rest of the enterprise.

RECOMMENDATION 6

Periodically reconcile installation of anti-malware and patch management agents on Windows servers with applicable servers in its inventory to ensure full coverage.

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 2020	Shawn Wagoner 503-373-2142

Narrative for Recommendation 6

Efforts are already underway in ESO to develop two enterprise solutions to accommodate this recommendation. The first will be focused on establishing a solution or solutions that accurately account for inventory in an automated manner, both for software and hardware. This will allow for confirmation of existence of appropriate anti-malware software and patch management agents on each client in the environment.

The second solution will focus on configuration management, which will inform when a system is configured in an insecure, non-compliant manner. This solution will help ensure anti-malware and patch management agents are properly configured to do what was intended.

ESO will be deploying these solutions during the 2019-21 biennium when the necessary budget will be available. ETS/SDC will be the first target for both solutions once they are identified and procured.

RECOMMENDATION 7

Enforce existing procedures requiring periodic review of privileged access membership.

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 2020	Shawn Wagoner 503-373-2142

Narrative for Recommendation 7

ESO has worked with ETS and agency partners to drive forward a multi-year project to upgrade the controls around the isolation, tracking and use of privileged access credentials within ETS. Agreeing on a solution has included partnership with IT and security teams across all agencies with systems currently managed at ETS. ESO and ETS have already contracted a vendor and started implementation of the new privileged access system that should be ready for use starting in 2019.

ESO will assist ETS in the development, documentation and testing of a periodic privileged access audit procedure as soon as the move to a new privileged access management system is complete. The conversion to this new system will take quite a while as each agency domain will need to be integrated individually. Substantial progress should be observable in the latter half of 2019.

RECOMMENDATION 8

Develop additional alerts to monitor actions taken by privileged access users, as required by the statewide security plan and standards.

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	October 2019	Mark Johnston 503-947-0488

Narrative for Recommendation 8

The Enterprise Security Office (ESO) Security Operations Center (SOC) is currently in the process of developing use cases that will enable alerting for actions taken by privileged users as required by the Statewide Information Security Plan. This includes alerting on specific behavior such as privilege escalation attempts, log modification and non-standard creation of user accounts and privilege assignment. Once these alerts are developed and ETS endpoint systems are integrated into the SOC, this finding will be fully addressed.

RECOMMENDATION 9

Further define procedures for security incident response, including:

a. Better defining roles and responsibilities for security incident response between the Enterprise Security Office and the data center;
b. Ensuring that potential security incidents are tracked to enable additional analysis; and
c. Developing standard operating procedures for responding to different types of security incidents.

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 2019	Mark Johnston 503-947-0488

Narrative for Recommendation 9

As called out in the Statewide Information Security Plan (dated August 1, 2018), the Enterprise Security Office (ESO) is to develop, coordinate and maintain the State Incident Response capability. The ESO is currently in the process of clearly defining roles and responsibilities for security incident response as part of efforts to update the Statewide Security Incident Response policy (107-004-120) and related procedures. This body of work will enable better role definition and responsibilities in this area between the ESO and the data center.

As part of the SOC development mentioned in recommendations #1 and #8, the SOC will be formalizing the tracking and analysis of security incidents, as well as the standard operating procedures for responding to different types of security incidents. Incidents detected in the SOC are already being documented and tracked in a SOC ticketing system (this was implemented after the audit was completed). Written procedures for tracking and closing tickets in this system are still being developed, with an expected completion date of June 30, 2019. These procedures must be applicable to agency incidents as well as SDC incidents, therefore more time will be required to complete the documentation.

RECOMMENDATION 10

Identify and implement an automated solution for asset inventory and configuration management.

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 2020	Shawn Wagoner 503-373-2142

Narrative for Recommendation 10

Efforts are already underway in ESO to develop two enterprise solutions to accommodate this recommendation. The first will be focused on establishing a solution or solutions that accurately account for inventory in an automated manner, both for software and hardware. The second solution will focus on configuration management, which will inform when a configuration changes in a non-compliant way. ESO will be deploying these solutions during the 2019-21 biennium when the necessary budget will be available.

ETS/SDC will be the first target for both solutions once they are identified and procured.

RECOMMENDATION 11

Work with state agencies dependent upon the data center for disaster recovery and ensure priorities for recovery are identified.

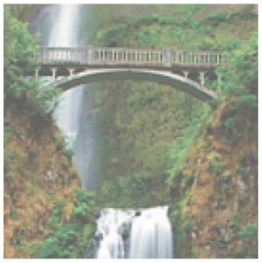
Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	June 2019	Janet Orton 503-373-0841

Narrative for Recommendation 11
ETS is currently in the process of gathering this information. Further work will then be needed to identify interdependencies and interfaces across platforms to fully understand the requirements and complexity of system recovery. Completion of this recommendation will require partnership between ETS and customer agencies.

Please contact Stefan Richards at 503-378-8295 for any questions.

Sincerely,

Terrence Woods
Interim State Chief Information Officer



Audit Team

William Garber, CGFM, MPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Erika Ungern, CISA, CISSP, Principal Auditor

Sheila Faulkner, Staff Auditor

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 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