Secretary of State
Oregon Audits Division

Department of Revenue

Cybersecurity Controls Assessment

January 2019
2019-03

Secretary of State Dennis Richardson
Audits Division Director Kip Memmott

This page intentionally left blank

Secretary of State
Assessment Highlights

January 2019

Department of Revenue
Cybersecurity Controls Assessment

Report Highlights

This audit was conducted to assess critical security controls and the Department of Revenue's (DOR) information technology (IT) security management program. We concluded the agency should update its security management program to reflect recent statewide changes to IT security governance structures, as well as correct weaknesses in inventory management, vulnerability management, control of administrative accounts, configuration change management, and audit logging processes.

Background

DOR handles sensitive information, including taxpayer personal information and tax data. The agency, in collaboration with the Enterprise Security Office at the Office of the State Chief Information Officer (OSCIO), is responsible for implementing a security management program to ensure the confidentiality, availability, and integrity of the information with which it is entrusted.

Purpose

The purpose of this audit was to determine whether DOR has implemented an appropriate IT security management program and the basic cybersecurity controls necessary to ensure cyber defense readiness.

Key Findings

1. DOR has implemented a security management program, but associated plans and procedures have not been updated to reflect current staffing levels and reorganization of statewide security by the OSCIO.

2. DOR lacks specific policies and fully automated controls for many elements of the basic security controls identified by the Center for Internet Security. These basic controls should be implemented in every organization to reduce the risk that attackers could compromise systems and data.

Recommendations

We recommend DOR improve its security management program and remedy weaknesses we identified in the basic controls defined by the Center for Internet Security.

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

Introduction

Cybersecurity is a growing concern for both the private and public sector. In order to protect against growing threats, information technology (IT) security management professionals need to apply robust controls at various levels of infrastructure to protect their networks, servers, and user workstations. State agencies utilize a variety of frameworks and standards with varying levels of detail to guide these efforts.

In the spring of 2018, the Audits Division developed a repeatable audit program to evaluate cybersecurity risks and provide a high-level view of an agency's current state. For criteria, we chose to use the Center for Internet Security's CIS Controls™, version 7, a prioritized list of 20 high-priority defensive actions that provide a starting point for enterprises to improve cyber defense.[1] The controls are divided into three categories: basic, foundational, and organizational. This assessment covers the first six basic controls, which are defined as key controls that should be implemented in every organization for essential cyber defense readiness.

In the following pages, we present our assessment results as graphs depicting whether a particular control is not implemented, partially implemented, or fully implemented. This provides agency management, the Legislature, and those with responsibility for cybersecurity in the state with a snapshot of areas with higher risk that may need additional controls applied. It also provides the Audits Division with valuable information about an entity that we can use in our audit planning process so we can focus limited audit resources where the risks are highest.

The assessment does not consider an individual agency's risk appetite, so while these controls are considered basic by many security practitioners, agency management may choose not to fully implement a control to the highest level if they believe the cost of doing so outweighs the risk. In addition, we generally considered compensating controls that might mitigate risks, but we did not perform a detailed assessment of potential compensating controls for each sub-control.

State agencies and the Office of the State Chief Information Officer share responsibility for cybersecurity in Oregon government

In September 2016, the Governor signed Executive Order 16-13, unifying IT security functions for the majority of state agencies in order to protect and secure information entrusted to the State of Oregon.[2] The order directed executive state agencies to consolidate security functions and staffing into the Office of the State Chief Information Officer (OSCIO), which is part of the Department of Administrative Services. In addition, the order instructed agencies to work with the newly consolidated group to develop and implement security plans, rules, policies, and standards adopted by the State Chief Information Officer. The order was made permanent by the passage of Senate Bill 90 in June 2017, resulting in the permanent transfer of 30 security-related positions from state agencies to the OSCIO.[3]

The OSCIO maintains policy and performs statewide IT oversight functions. The Enterprise Security Office (ESO), a division of the OSCIO, brings together elements of enterprise security, including governance, policy, procedure, and operations under a single accountable organization. Agencies retain responsibility for many organization level security controls and

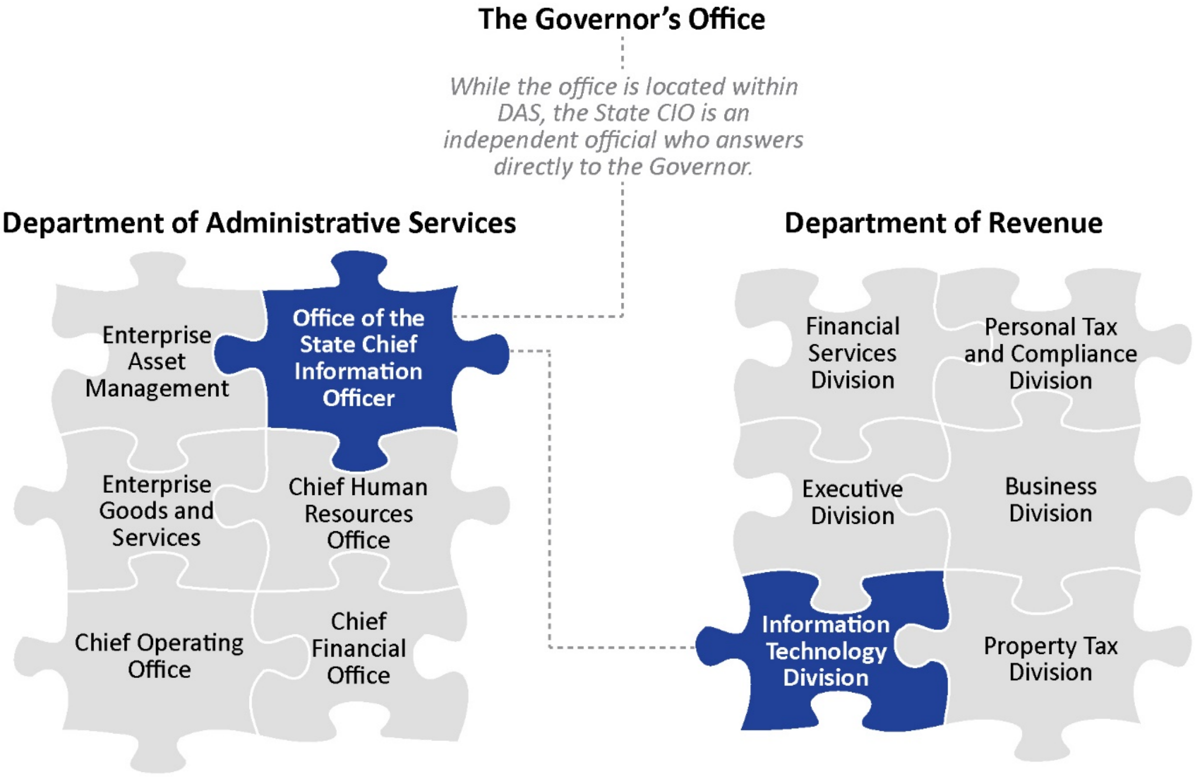
[1] Center for Internet Security CIS Controls

[2] Executive Order 16-13, "Unifying Cyber Security in Oregon"

[3] Senate Bill 90, "Transfers information technology security functions of certain state agencies in executive branch to State Chief Information Officer."

work collaboratively with the ESO to ensure the confidentiality, availability, and integrity of their sensitive business information.

The Department of Revenue (DOR) serves millions of Oregonians each year by collecting taxes and fees that fund the majority of public agencies in the state. Total revenue collected by the agency for the 2017-19 biennium is projected at $20.7 billion. Ninety percent of this revenue is transferred to the General Fund. DOR's legislatively adopted budget for 2017-19 is $313 million and includes 933 full time equivalent staff.


The Governor's Office
While the office is located within DAS, the State CIO is an independent official who answers directly to the Governor.
Department of Administrative Services
Enterprise Asset Management
Office of the State Chief Information Officer
Enterprise Goods and Services
Chief Human Resources Office
Chief Operating Office
Chief Financial Office
Department of Revenue
Financial Services Division
Personal Tax and Compliance Division
Executive Division
Business Division
Information Technology Division
Property Tax Division

Objective, Scope, and Methodology

Objective

The objective of this work was to determine the extent to which DOR has implemented an appropriate IT security management program as well as selected controls from the Center for Internet Security's CIS Controls™, version 7. These controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices to help protect systems and networks from the most common attacks.[4]

Scope

The scope of this work included a review of security management and the first six of the 20 CIS Controls™ in place at DOR during 2018. Cybersecurity experts generally agree that these six basic controls should be implemented by all organizations for cyber defense readiness.

Methodology

We interviewed agency staff, reviewed documentation, and performed limited control testing to assess whether management has established policies and implemented controls to stop cyberattacks that may target the agency.

In addition to the CIS Controls™, we used the Federal Information System Controls Audit Manual as IT security management criteria.

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

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

[4] Defense-in-depth refers to the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives.

Assessment Results

Our review identified specific areas where DOR could improve security controls. In particular, DOR has not updated its security plan to better reflect its current resources and define roles and responsibilities between DOR and the OSCIO. DOR also lacks specific policy statements and fully implemented automated controls for many specific sub-controls included in this review. Together, these weaknesses increase the risk that attackers could compromise DOR systems and data.

DOR security management program

At DOR, the security management program is a collaborative effort with the ESO, which is part of the OSCIO. DOR is responsible for the development, documentation, and implementation of a security management program for its specific environment, while the ESO is responsible for enterprise information security strategy and strategic planning.

DOR developed an information security plan, last updated in February 2016, which addressed such foundational activities as defining security roles and responsibilities, conducting annual risk assessments, and developing security policies. The agency also had internal and external risk assessments performed within the past year that address security-related topics. Based on the plan and associated policies, we found DOR has implemented an appropriate security management program.

However, several changes have occurred since the plan was last updated that are not reflected in DOR's plan and procedures. The reorganization due to Senate Bill 90 transferred some responsibilities and 30 positions from state agencies to the OSCIO. This included three positions from DOR.

The loss of these positions, including DOR's Chief Information Security Officer, is not reflected in the agency's security plan. The plan also indicated that DOR was in the process of acquiring a security information and event monitoring system, which has not occurred and is not currently being pursued. In addition, the ESO published a statewide security plan in August 2018 that agencies were required to adopt, with the addition of an agency-specific memorandum or addendum to provide additional information; these elements have not yet been completed by DOR.

Overall, there is significant uncertainty at DOR regarding how elements of its security management program are to be addressed in the current statewide security environment. The transfer of the three security positions left DOR with only one half-time security employee plus another position currently assigned to perform security-related tasks. DOR plans to work with the ESO to address identified gaps.

Security management is the foundation to security control and structure in an organization. Entities should have policies, plans, and procedures that describe the management program and cover all major systems, facilities, and applications. Detailed roles and responsibilities should be clearly defined.

Agencies should:

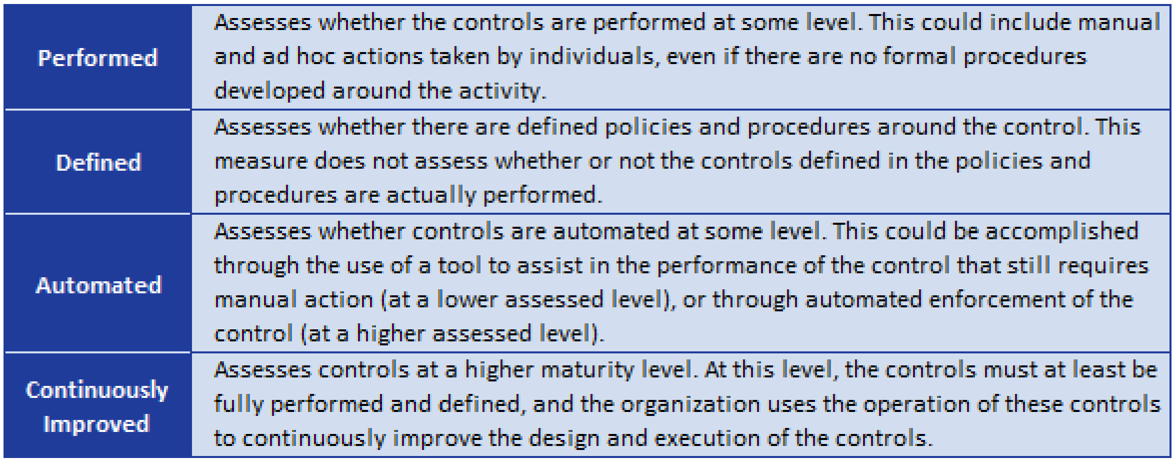
- periodically assess and validate risks;
- document and implement security control policies and procedures;
- implement and monitor effective security awareness trainings;
- remediate information security weaknesses; and
- ensure external third parties are adequately secured.

Without a well-designed program, security controls are likely inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls are at risk of being inconsistently applied, leaving the agency vulnerable to attacks.

CIS Controls assessment

For this assessment, we evaluated the implementation level of the agency's cybersecurity control environment against the top six CIS Controls™ and their associated sub-controls. We evaluated each sub-control against four levels of implementation to provide an assessment of the agency's overall cybersecurity implementation.

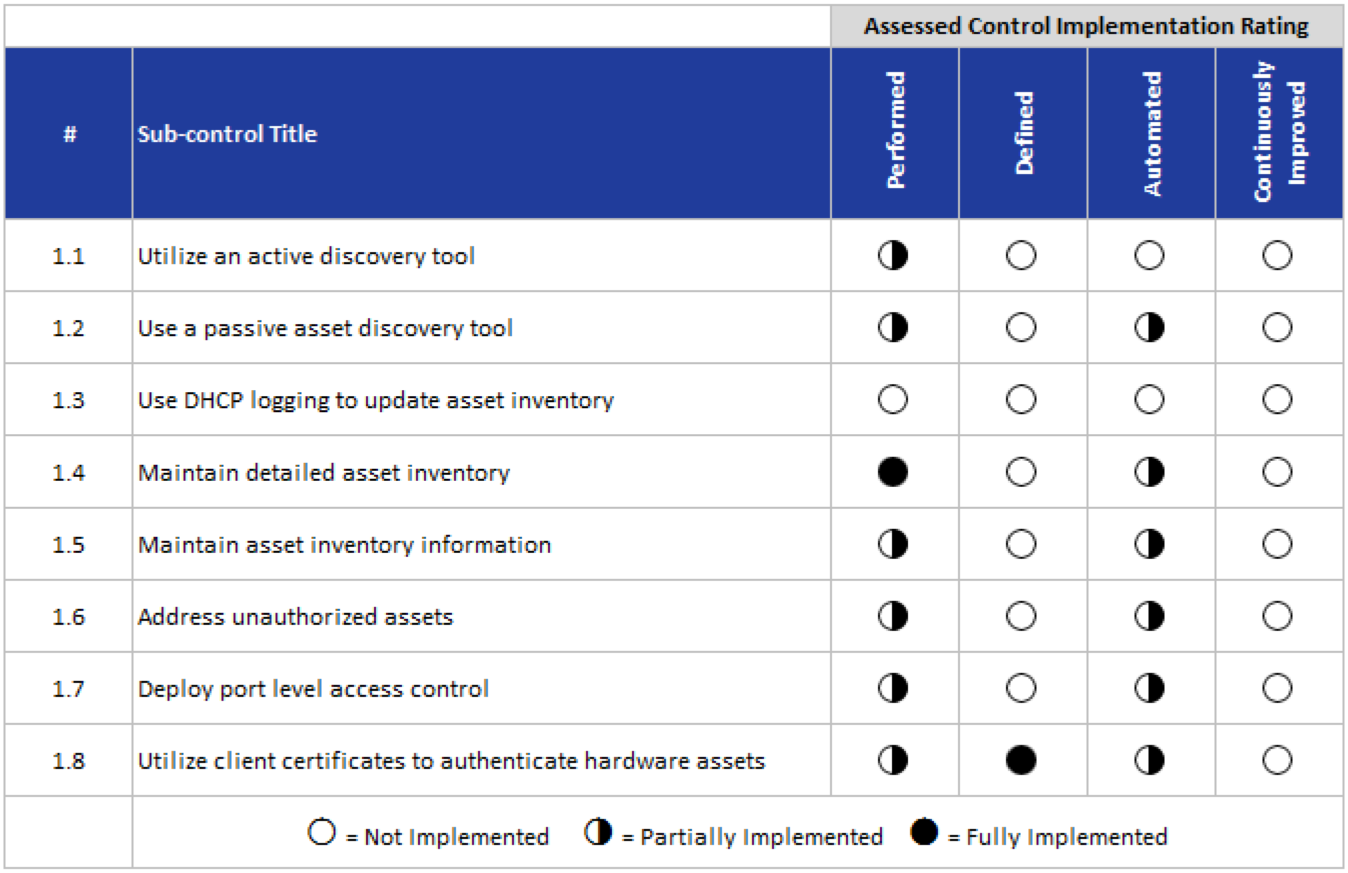
Figure 1: Control implementation levels



Performed	Assesses whether the controls are performed at some level. This could include manual and ad hoc actions taken by individuals, even if there are no formal procedures developed around the activity.
Defined	Assesses whether there are defined policies and procedures around the control. This measure does not assess whether or not the controls defined in the policies and procedures are actually performed.
Automated	Assesses whether controls are automated at some level. This could be accomplished through the use of a tool to assist in the performance of the control that still requires manual action (at a lower assessed level), or through automated enforcement of the control (at a higher assessed level).
Continuously Improved	Assesses controls at a higher maturity level. At this level, the controls must at least be fully performed and defined, and the organization uses the operation of these controls to continuously improve the design and execution of the controls.

Some implementation categories will not apply to select sub-controls due to their intended function. For example, implementing sub-controls 3.4 and 3.5 requires automation. Therefore, the first level of implementation is not relevant.

CIS Control™ 1: Inventory of Authorized and Unauthorized Devices



		Assessed Control Implementation Rating			
#	Sub-control Title	Performed	Defined	Automated	Continuously Improved
1.1	Utilize an active discovery tool	◐	○	○	○
1.2	Use a passive asset discovery tool	◐	○	◐	○
1.3	Use DHCP logging to update asset inventory	○	○	○	○
1.4	Maintain detailed asset inventory	●	○	◐	○
1.5	Maintain asset inventory information	◐	○	◐	○
1.6	Address unauthorized assets	◐	○	◐	○
1.7	Deploy port level access control	◐	○	◐	○
1.8	Utilize client certificates to authenticate hardware assets	◐	●	◐	○
	○ = Not Implemented ◐ = Partially Implemented ● = Fully Implemented				

We evaluated DOR's processes to identify network devices, maintain an updated inventory of hardware devices, and control devices that can connect to the network. We found that DOR generally lacks formal policies in this area. The agency maintains inventories of devices and has tools available that can identify devices on its network; however, most of the inventories are manually maintained, and DOR does not use available tools to automatically identify other network devices not on its inventory list. The agency also has controls to ensure only authorized devices may connect to its wireless environment, but those restrictions are not implemented on its wired environment.

Any new device introduced to an agency's network may introduce vulnerabilities. Ensuring only authorized devices have access to information on the agency's network allows IT professionals to identify and remediate vulnerabilities by implementing proper security controls. However, without a clear understanding of which devices are on the network, the agency cannot ensure that proper controls are in place for those devices. Additionally, without an up-to-date inventory of authorized hardware, the agency may not identify unauthorized devices, which limits the agency's ability to prevent or detect unauthorized access to the network.

CIS Control™ 2: Inventory of Authorized and Unauthorized Software

		Assessed Control Implementation Rating			
#	Sub-control Title	Performed	Defined	Automated	Continuously Improved
2.1	Maintain inventory of authorized software	◑	◑	○	○
2.2	Ensure software is supported by vendor	◑	◑	○	○
2.3	Utilize software inventory tools	◑	○	◑	○
2.4	Track software inventory information	◑	◑	◑	○
2.5	Integrate software and hardware asset inventories	◑	○	◑	○
2.6	Address unapproved software	◑	◑	○	○
2.7	Utilize application whitelisting	○	○	○	○
2.8	Implement application whitelisting of libraries	○	○	○	○
2.9	Implement application whitelisting of scripts	○	○	○	○
2.10	Physically or logically segregate high risk applications	◑	○	○	○
	○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented				

We evaluated DOR's processes to document approved software, determine high-risk software, and identify software on its systems. We found that DOR generally lacks formal policies in this area. The agency has implemented a tool that automatically develops an inventory of software on Windows workstations, but this does not identify whether the software is authorized. DOR restricts the ability to install software on its workstations and servers to authorized privileged users, which helps reduce the risk in this area. However, controls should be improved by implementing software whitelisting, improving automation of inventory, and monitoring software installations on all systems.[5]

An organization should maintain an inventory of software installed on its computer systems similar to the inventory of its hardware assets. Without a complete, accurate, and up-to-date list of the software that is authorized to be on an agency's systems, it cannot ensure effective controls are in place to protect software on the agency's information systems.

In addition to not being able to effectively safeguard authorized software, without an inventory of system software, an agency may be unable to identify unauthorized software on its information systems, such as malicious software or software with known vulnerabilities.

[5] Software whitelisting is the practice of identifying a list of approved software to be installed on computer systems and restricting access installation to only approved software. Whitelisting reduces the risk of malicious software such as computer viruses or ransomware.

Attackers can exploit systems with malicious or vulnerable software to gain unauthorized access to the agency's data or disrupt operations.

CIS Control™ 3: Continuous Vulnerability Assessment and Remediation

		Assessed Control Implementation Rating			
#	Sub-control Title	Performed	Defined	Automated	Continuously Improved
3.1	Run automated vulnerability scanning tools	●	●	●	○
3.2	Perform authenticated vulnerability scanning	●	●	●	○
3.3	Protect dedicated assessment accounts	●	●	●	○
3.4	Deploy automated operating system patch management tools	▨	●	◑	○
3.5	Deploy automated software patch management tools	▨	●	◑	○
3.6	Compare back-to-back vulnerability scans	◑	○	○	○
3.7	Utilize a risk-rating process	◑	◑	○	○
	○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented ▨ = Not Applicable				

We evaluated DOR's processes for patching systems to prevent vulnerabilities and for identifying and remediating vulnerabilities that are detected. Vulnerability management is a joint effort between DOR and the ESO. We found DOR generally has policies in place for vulnerability management. DOR has also partially implemented automated controls for most of the related sub-controls. For example, DOR regularly scans each device on its network for vulnerabilities. It has a process to prioritize the remediation of identified critical vulnerabilities, but does not formally track individual vulnerabilities over time to ensure all identified vulnerabilities are remediated. The agency automatically patches most of its systems, but some are patched manually.

Organizations should be continuously engaged in identifying, remediating, and minimizing security vulnerabilities to ensure their assets are safeguarded. Attackers commonly exploit IT systems that have not been patched with security updates or have other known vulnerabilities. By scanning the network for those known vulnerabilities, an agency can identify and prioritize software patching and other remediation activities to ensure these known risks are controlled. Attackers may exploit known vulnerabilities to compromise the confidentiality, integrity, or availability of agency data. Agency management should ensure processes are in place to keep informed of available patches, test those patches for compatibility on the agency's systems, document the basis for the decision to implement patches or not, and implement appropriate changes in a timely manner.

CIS Control™ 4: Controlled Use of Administrative Privileges

		Assessed Control Implementation Rating			
#	Sub-control Title	Performed	Defined	Automated	Continuously Improved
4.1	Maintain inventory of administrative accounts	◑	◑	◑	○
4.2	Change default passwords	◑	○	◑	○
4.3	Ensure the use of dedicated administrative accounts	◑	○	◑	○
4.4	Use unique passwords	◑	○	◑	○
4.5	Use multifactor authentication for all administrative access	◑	○	◑	○
4.6	Use dedicated workstations for all administrative tasks	○	○	○	○
4.7	Limit access to scripting tools	●	○	●	○
4.8	Log and alert on changes to administrative group membership	◑	○	◑	○
4.9	Log and alert on unsuccessful administrative account login	◑	○	◑	○
	○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented				

We evaluated DOR's processes to grant and monitor privileged access, to log and monitor login activity, and to establish robust authentication procedures.[6] We found DOR generally lacked formal policies for this area, though it has general policies that indicate access should be granted on the basis of "least privilege."[7] DOR has partially implemented automated procedures for controlling the use of administrative privileges. For example, work requiring administrative access is conducted over encrypted channels and server administration is performed using dedicated administrative accounts. Controls could be improved by developing more detailed policies and procedures for privileged accounts, improving alerting of changes to administrative account assignments, expanding multifactor authentication for administrative tasks, and ensuring privileged users use dedicated machines and accounts for all administrative tasks.

Management should ensure that only authorized users are able to perform administrative functions on the agency's information systems. While some users may have authorization to read, edit, or delete data based on their job duties, certain users have access to advanced functions such as system control, monitoring, or administrative functions. Actions performed under these administrative accounts may have critical effects on the agency's systems.

[6] Privileged access refers to the ability of some users 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.

[7] Least privilege is the principle that a security system should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Therefore, use of accounts with these privileges should be effectively controlled by management, which should implement controls to segregate, manage, and monitor use of these accounts.

CIS Control™ 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

		Assessed Control Implementation Rating			
#	Sub-control Title	Performed	Defined	Automated	Continuously Improved
5.1	Establish secure configurations	◑	●	◑	○
5.2	Maintain secure images	◑	●	◑	○
5.3	Securely store master images	◑	○	◑	○
5.4	Deploy system configuration management tools	◑	○	◑	○
5.5	Implement automated configuration monitoring systems	▨	●	◑	○
	○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented ▨ = Not Applicable				

We evaluated DOR's processes to document and safeguard baseline configurations, deploy secure configurations, and monitor configurations on its network. We found that DOR has some formal policies related to this control, and has partially implemented automated controls for all of the sub-controls. For example, DOR deploys secure configurations to most of its workstations using a centralized process. However, other systems require manual installation of required software. Several configuration settings are controlled through central automated rules, but there is no formal review to ensure those rules are not modified inappropriately. Overall, configuration settings are not monitored to ensure they have not changed.

Organizations should have processes in place to ensure hardware and software are securely configured. Default configurations may not align with business or security needs and may leave the agency's systems vulnerable to attack. The agency should have configuration management processes in place that address implementing secure system control features at the initiation of the system life cycle. Furthermore, an organization should ensure configurations remain secure as modifications are made to the system. Configuration baselines should be documented so that agency personnel can effectively monitor actual configurations to ensure they align with established baselines. Also, policies and procedures should be in place that address how configuration baselines are managed.

CIS Control™ 6: Maintenance, Monitoring, and Analysis of Audit Logs

		Assessed Control Implementation Rating			
#	Sub-control Title	Performed	Defined	Automated	Continuously Improved
6.1	Utilize three synchronized time sources	◑	○	◑	▨
6.2	Activate audit logging	●	●	●	○
6.3	Enabled detailed logging	●	●	●	○
6.4	Ensure adequate storage for logs	◑	◑	○	○
6.5	Central log management	○	○	○	○
6.6	Deploy SIEM or log analytic tools	○	○	○	○
6.7	Regularly review logs	◑	◑	○	○
6.8	Regularly tune SIEM	○	○	○	○
	○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented ▨ = Not Applicable				

We evaluated DOR's processes to collect, manage, and analyze audit logs of events that could help the agency detect, understand, or recover from an attack. We found DOR adequately generates audit logs, but does not periodically monitor all of them. There is a security information and event monitoring system operating at the ESO that analyzes network device logs that also receives information from DOR web logs. The system has the potential to provide DOR with threat information based on rules developed by ESO personnel. However, analysis rules have not been developed that would allow DOR to better monitor its environment and DOR does not have visibility into this system. DOR uses other tools to help analyze threats, but these do not directly relate to these sub-controls.

Robust logging and log monitoring processes allow organizations to identify and understand inappropriate activity and recover more quickly from an attack. Deficient logging may allow attackers and malicious activity to go undetected for extended periods of time. Moreover, attackers know that organizations rarely review log information, allowing attacks to go unnoticed. The agency should ensure that information systems generate records that record the type, location, time, and source of events that occur. Additionally, processes should be established to ensure these logs are periodically reviewed so the agency can identify inappropriate or unusual activity and remediate security events.

Recommendations

To improve capability in the critical cybersecurity controls, we recommend DOR and the OSCIO work collaboratively, where appropriate, to:

1. Improve security management by documenting the degree to which DOR has adopted the statewide information security plan and ensuring DOR and ESO roles and responsibilities for information security are clearly defined.

2. Remedy weaknesses with CIS Control #1 – Hardware Inventory – by further developing written policies and procedures, automating asset discovery and inventory, and expanding hardware authentication.

3. Remedy weaknesses with CIS Control #2 – Software Inventory – by further developing written policies and procedures, improving tracking and documentation of approved software and software versions, and implementing software whitelisting.

4. Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by formally tracking the status of identified vulnerabilities to ensure they are timely remediated.

5. Remedy weaknesses with CIS Control #4 – Privileged Access – by updating policies and procedures to cover additional elements, implementing multifactor authentication and use of dedicated workstations for all administrative tasks, and implementing alerts associated with administrative account activities.

6. Remedy weaknesses with CIS Control #5 – Secure Configurations – through automated monitoring of configuration changes and by further developing written policies and procedures.

7. Remedy weaknesses with CIS Control #6 – Audit Logs – by developing a central logging solution, implementing log analytic tools, and automating log review.

Appendix A: CIS Controls™

CIS Control 1: Inventory and Control of Hardware Assets

Sub-Control	Title	Description
1.1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.
1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

CIS Control 2: Inventory and Control of Software Assets

Sub-Control	Title	Description
2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
2.2	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
2.3	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
2.4	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.

2.5	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
2.6	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.
2.7	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
2.8	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.
2.9	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.
2.10	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.

CIS Control 3: Continuous Vulnerability Management

Sub-Control	Title	Description
3.1	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
3.2	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
3.3	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
3.4	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
3.5	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
3.6	Compare Back-to-back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
3.7	Utilize a Risk-rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

CIS Control 4: Controlled Use of Administrative Privileges

Sub-Control	Title	Description
4.1	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
4.3	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
4.4	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
4.5	Use Multifactor Authentication For All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
4.6	Use of Dedicated Machines For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
4.7	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.
4.8	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
4.9	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Sub-Control	Title	Description
5.1	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.
5.2	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
5.3	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

5.4	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
5.5	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Sub-Control	Title	Description
6.1	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
6.2	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.
6.3	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
6.4	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.
6.5	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
6.6	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
6.7	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.
6.8	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

Oregon

Kate Brown, Governor

Department of Revenue
955 Center St NE
Salem, OR 97301-2555
www.oregon.gov/dor

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 **"Oregon Department of Revenue: Cybersecurity Controls Assessment."**

The Department of Revenue (DOR) Executive Management appreciates the collaborative approach taken by the Audits Division and generally agrees with these findings. DOR's mission is to make revenue systems work to fund the public services that preserve and enhance the quality of life for all citizens. We are committed to improving our capabilities in these areas, and have identified opportunities for improvements in recent years which this audit report validates. Below is our response to each recommendation in the audit. We look forward to sharing our successes with stakeholders over the next year and appreciate the opportunity to highlight the progress to date in addressing some of these recommendations. Fundamentally, DOR is committed to ensuring the safety and accessibility of data and technology resources, while balancing certain risks.

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

RECOMMENDATION 1 Improve security management by documenting the degree to which DOR has adopted the statewide information security plan and ensuring DOR and ESO roles and responsibilities for information security are clearly defined.		
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	6/30/2019	ESO

Narrative for Recommendation 1

Agreed. DOR submitted the DOR Gap Analysis of the Statewide Security Plan to ESO 10-26-2018. DOR will collaborate with ESO on a Plan of Action and Milestones (POAM) to address the security gaps over the next six months. DOR previously maintained a DOR specific Information

Security Plan. Going forward, this plan will be retired and DOR will adopt the Statewide Information Security Plan maintained by the Enterprise Security Office.

<table>
<tr><td colspan="3">RECOMMENDATION 2
Remedy weaknesses with CIS Control #1 – Hardware Inventory – by further developing written policies and procedures, automating asset discovery and inventory, and expanding hardware authentication.</td></tr>
<tr><td>Agree or Disagree with Recommendation</td><td>Target date to complete implementation activities (Generally expected within 6 months)</td><td>Name and phone number of specific point of contact for implementation</td></tr>
<tr><td>Agreed</td><td>6/30/2019</td><td>Kathy Terman, DCIO
503 945-8006</td></tr>
</table>

Narrative for Recommendation 2

Agreed. DOR Management will collaborate with OSCIO to strengthen its hardware inventory controls to remedy its identified weaknesses with CIS #1. Most end user devices are mobile and WiFi enabled. A single device can have several IP addresses per day depending on location. DHCP and DNS record updates are automated but asset inventory is not due to the ephemeral nature of IP addresses in DOR's environment. DOR will continue to work with ETS and ESO to implement Layer 2 NAC. As a compensating control, DOR will implement certificate based network authentication on all agency endpoints.

<table>
<tr><td colspan="3">RECOMMENDATION 3
Remedy weaknesses with CIS Control #2 – Software Inventory – by further developing written policies and procedures, improving tracking and documentation of approved software and software versions, and implementing software whitelisting.</td></tr>
<tr><td>Agree or Disagree with Recommendation</td><td>Target date to complete implementation activities (Generally expected within 6 months)</td><td>Name and phone number of specific point of contact for implementation</td></tr>
<tr><td>Agreed</td><td>6/30/2019</td><td>Kathy Terman, DCIO
503 945-8006</td></tr>
</table>

Narrative for Recommendation 3

Agreed. DOR Management will collaborate with OSCIO to strengthen its software inventory controls to remedy its identified weaknesses with CIS #2. Furthermore, DOR will evaluate the use of software whitelisting based on its risk to the agency. If, after a risk analysis categorizes this as a high risk, DOR will implement software whitelisting controls. Short term activities and process improvements will include: Evaluation of automated whitelist enforcement technologies. Work with ESO to establish a consistent approach to whitelisting technologies and strategy. Improve DOR tracking and documentation of approved software. Automate reporting on non-approved software. Create policy and process for removal of non-authorized software.

<table>
<tr><td colspan="3">RECOMMENDATION 4
Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by formally tracking the status of identified vulnerabilities to ensure they are timely remediated.</td></tr>
<tr><td>Agree or Disagree with Recommendation</td><td>Target date to complete implementation activities (Generally expected within 6 months)</td><td>Name and phone number of specific point of contact for implementation</td></tr>
<tr><td>Agreed</td><td>6/30/2019</td><td>Kathy Terman, DCIO
503 945-8006</td></tr>
</table>

Narrative for Recommendation 4

Agreed. DOR Management will evaluate the current tracking and remediation of vulnerabilities performed weekly to identify areas for improvement in its vulnerability management program by ensuring known vulnerabilities are tracked and remediated in accordance with the agency and statewide standards. DOR will create and manage service tickets for all critical vulnerabilities.

<table>
<tr><td colspan="3">RECOMMENDATION 5
Remedy weaknesses with CIS Control #4 – Privileged Access – by updating policies and procedures to cover additional elements, implementing multifactor authentication and use of dedicated workstations for all administrative tasks, and implementing alerts associated with administrative account activities.</td></tr>
<tr><td>Agree or Disagree with Recommendation</td><td>Target date to complete implementation activities (Generally expected within 6 months)</td><td>Name and phone number of specific point of contact for implementation</td></tr>
<tr><td>Agreed</td><td>6/30/2019</td><td>Kathy Terman, DCIO
503 945-8006</td></tr>
</table>

Narrative for Recommendation 5

Agreed. DOR will work to strengthen CIS #4 through administrative controls (i.e., policies, standards, and procedures.) and implement the use of dedicated workstations for all privileged user administrative tasks.

RECOMMENDATION 6 Remedy weaknesses with CIS Control #5 – Secure Configurations – through automated monitoring of configuration changes and by further developing written policies and procedures.		
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
Agreed	6/30/2019	Kathy Terman, DCIO 503 945-8006

Narrative for Recommendation 6

Agreed. DOR will collaborate with OSCIO/ESO to leverage Tenable (Nessus Security Center) to strengthen its secure configuration controls to remedy its perceived weaknesses with CIS #5. DOR has implemented weekly CIS specific Tenable scans to baseline and track our server and workstation configurations. DOR has also implemented policy enforced security settings in accordance with the IRS Office of Safeguards Computer Security Evaluation Matrix. IRS security setting recommendations are in alignment with the CIS recommendations and are validated every three years by IRS auditors. DOR will develop policies and procedures to continuously detect, track, and remediate deficiencies to ensure consistent and compliant configurations.

RECOMMENDATION 7 Remedy weaknesses with CIS Control #6 – Audit Logs – by developing a central logging solution, implementing log analytic tools, and automating log review.		
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
Agreed	Provided by auditee 6/30/2019	Kathy Terman, DCIO 503 945-8006

Oregon

Kate Brown, Governor

Department of Revenue
955 Center St NE
Salem, OR 97301-2555
www.oregon.gov/dor

Narrative for Recommendation 7

Agreed. DOR currently consumes OSCIO enterprise logging services. DOR will continue to collaborate with OSCIO to meet the audit requirements by creating and implementing appropriate use cases for security event logging and monitoring. Currently, DOR forwards web logs to QRadar, ETS's central logging solution. DOR has initiated the formal onboarding process with ETS to extend log aggregation and analysis to DOR's Microsoft Advanced Threat Analytics system and critical core database and application servers.

Please contact Gary Johnson at 503-945-8095 with any questions.

Sincerely,
Nia Ray, Director
Oregon Dept. of Revenue

cc:

Assessment Team

William K. Garber, CGFM, MPA, Deputy Director

Teresa L. Furnish, CISA, Audit Manager

Erika A. Ungern, CISA, CISSP, Principal Auditor

Jessica D. Ritter, CPA, 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