# Secretary of State
# Oregon Audits Division

## Oregon Department of Education
# Cybersecurity Controls Audit

November 2019
**2019-39**

Secretary of State **Bev Clarno**
Audits Division Director **Kip Memmott**

Secretary of State
Oregon Audits Division

# Executive Summary

## Oregon Department of Education
## Cybersecurity Controls Audit

### Why This Audit is Important

» The Oregon Department of Education (ODE) serves 197 school districts and 19 education service districts and oversees the education of over 580,000 students in Oregon's public K-12 education system

» ODE is subject to the Family Educational Rights and Privacy Act, which is a federal law that protects the privacy of student education records.

» ODE is required by law to collect and store student education records and is responsible for securing its information systems and protecting the privacy of data collected, used, shared, and stored by the department.

» This audit assessed critical security controls and the information technology (IT) security management practices at ODE.

### What We Found

Our review determined that ODE has implemented, or partially implemented, the majority of the controls reviewed during this audit. Specifically, ODE management has provided important protection measures for security, including tools for managing hardware and software inventories, tools for identifying and remediating security weaknesses, and implementing agency wide security awareness trainings. However, we identified the following specific areas where ODE could improve security controls.

1. ODE does not have a formal security management and compliance program that establishes a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures. (pg. 5)
2. ODE has partially implemented the majority of hardware inventory controls, but more work needs to be done to fully implement and mature hardware controls. (pg. 7)
3. ODE does not actively manage software to ensure that only authorized software is installed. (pg. 9)
4. Vulnerability assessments and remediation are effective, but processes and procedures should be matured. (pg. 11)
5. ODE does not appropriately manage all users who have significant high-level access to systems and data. (pg. 13)
6. ODE has not created secure configurations for all servers, network devices, and workstations. (pg. 15)
7. ODE does not have the necessary tools to monitor audit logs for all workstations, servers, and network devices. (pg. 16)

### What We Recommend

We made seven recommendations to ODE that include implementing a security management and compliance program and remedying weakness we identified in basic CIS Controls™.

ODE agreed with all of our recommendations. Their response can be found at the end of the report.

*The Oregon Secretary of State Audits Division is an independent, nonpartisan organization that conducts audits based on objective, reliable information to help state government operate more efficiently and effectively. The summary above should be considered in connection with a careful review of the full report.*

# Introduction

Cyberattacks, whether big or small, are a growing concern for both the private and public sector. Recent breaches at Oregon state agencies have only escalated this concern. In order to protect against growing threats, information technology (IT) management professionals should apply robust cybersecurity 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.

The Audits Division conducts cybersecurity audits to evaluate IT security risks and provide a high-level view of an agency's current state. We chose to use the Center for Internet Security's CIS Controls™, version 7.1. The CIS Controls™ are a prioritized list of 20 high-priority defensive actions that provide a starting point for enterprises to improve cyber defense. The controls are divided into three categories: basic, foundational, and organizational. This review includes the first six, the basic controls, which the Center for Internet Security, along with other security practitioners, defined as key controls that every organization should implement for essential cyber defense readiness.

In the following pages, we present the results as graphs depicting whether a particular control is not implemented, partially implemented, or fully implemented. This provides agency management, the Legislature, and others 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 informs our audit planning process and helps us focus limited audit resources where the risks are highest.

This audit does not consider an agency's risk appetite. Therefore, while these controls are considered basic by many security practitioners, agency management may choose not to fully implement a control if they determine within their strategic priorities whether the cost of doing so outweighs the risk. In addition, while we generally considered compensating controls that might mitigate some of the risks we identified, we did not perform a detailed review of potential compensating controls for each sub-control.

## State agencies and Enterprise Information Services share responsibility for cybersecurity in Oregon government

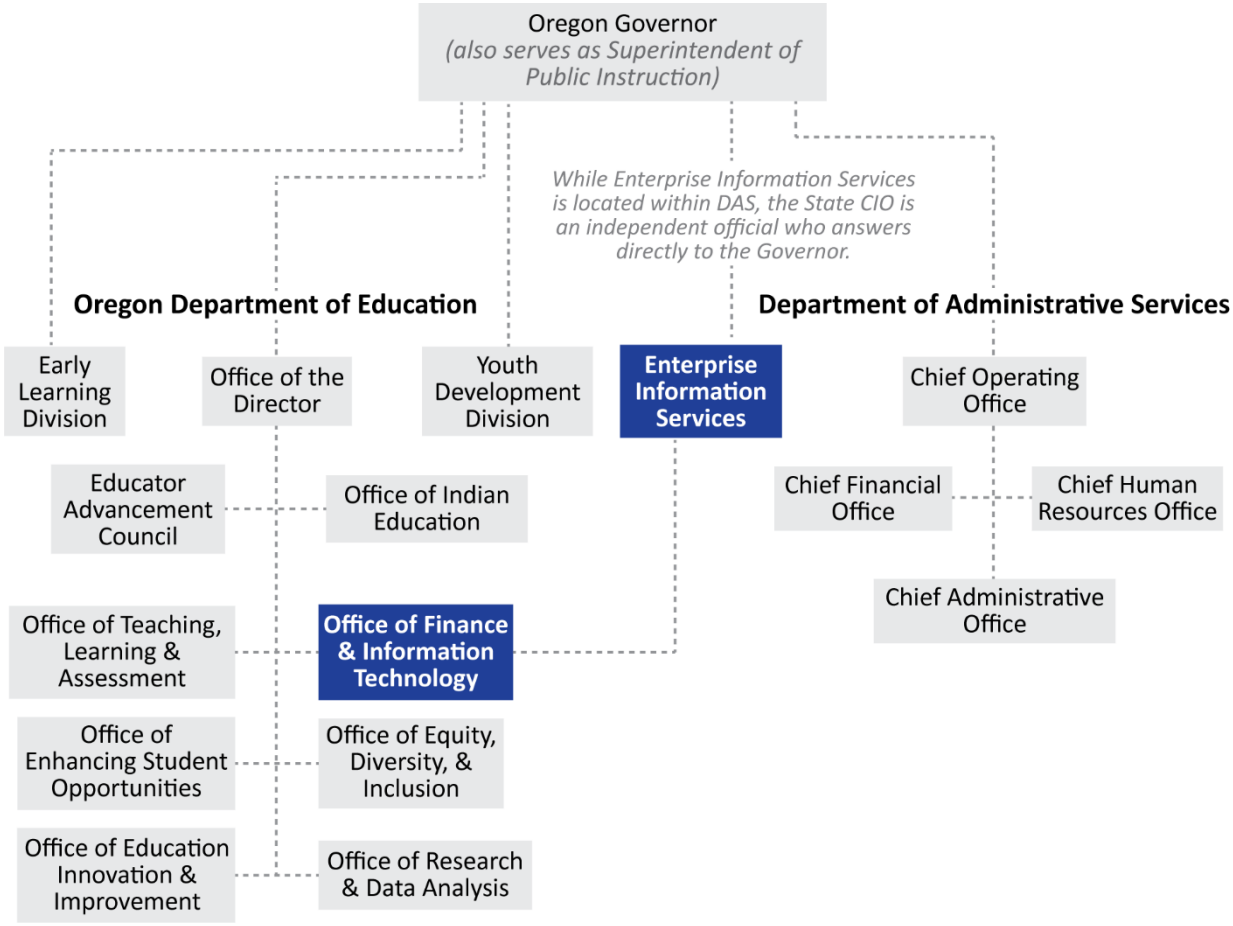
In September 2016, the Governor signed Executive Order 16-13, unifying IT security functions for the majority of state agencies in order to protect and secure information entrusted to the State of Oregon.[1] The order directed executive branch agencies to consolidate security functions and staffing into Enterprise Information Services (EIS), formerly known as the Office of the State CIO. 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 (CIO).

The passage of Senate Bill 90 in June 2017 made the order permanent, resulting in the transfer of 30 security-related positions from state agencies to EIS.[2] Two positions were transferred from ODE, including the agency's Chief Information Security Officer (CISO). After the shift in positions, executive branch agencies were assigned a Business Information Security Officer from EIS to

[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."

lead the activities normally undertaken by an agency CISO. However, at the time of this audit, EIS had not formally assigned anyone to assist ODE.

EIS maintains policy and statewide IT oversight functions. Cyber Security Services (CSS), a division of EIS formerly known as the Enterprise Security Office, 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 work collaboratively with the CSS to ensure the confidentiality, availability, and integrity of their sensitive business information. At the time of this audit, CSS had not fully defined the division of security responsibilities and functions between its office and the agencies.




## The Oregon Department of Education is subject to the Family Education Rights and Privacy Act

ODE is administered by the Governor, who acts as the Superintendent of Public Instruction. The Superintendent, by statute, appoints a deputy as a delegate to direct the department, and directors to administer the Early Learning Division (ELD) and the Youth Development Division (YDD). The State Board of Education, Early Learning Council, and Youth Development Council each provide policy guidance and oversight for different service delivery systems within the Department. The stated mission of the department is to foster equity and excellence for every learner through collaboration with educators, partners, and communities.

ODE serves 197 school districts and 19 education service districts and oversees the education of over 580,000 students (2017-18) in Oregon's public K-12 education system. Additionally, the

department operates the Oregon School for the Deaf, which serves approximately 120 students per year that are deaf or hard of hearing. The ELD works with more than 3,800 private and nonprofit early learning programs serving 100,000 children, while the YDD partners with nonprofit organizations, school districts, alternative schools, nine federally recognized Tribes, city and county governments, and 35 county juvenile departments to provide support for 15,000 youth ages six to 24. ODE's operations budget totals $225.6 million for 2017-19, funding 584 positions. ODE's total budget (not including the State School Fund) consists of over 50% in Federal Funds.

In addition to statewide cybersecurity requirements, ODE is subject to the Family Educational Rights and Privacy Act, which is a federal law that protects the privacy of student education records. The law applies to all schools, school districts, and governing organizations such as ODE that receive funds under an applicable program of the U.S. Department of Education. ODE is required by law to collect and store student education records and is responsible for securing its information systems and protecting the privacy of data collected, used, shared, and stored by the department.

The department is comprised of the following offices and divisions:

- Office of the Director
- Early Learning Division
- Youth Development Division
- Office of Enhancing Student Opportunities
- Educator Advancement Council
- Office of Indian Education
- Office of Equity, Diversity and Inclusion
- Office of Teaching, Learning, and Assessment
- Office of Research and Data analysis
- Office of Finance and Information Technology

Within the Office of Finance and Information Technology is the Information Technology Services group, which is led by the department's Chief Information Office (CIO). Information Services is composed of three distinct units: Application Development, Operations and Services, and Enterprise Services.

The **Application Development Unit** consists of 15 positions. This unit assists and supports ODE offices and divisions, school districts, and Education Service Districts (ESDs) with software application development and database management.

The **Operations and Services Unit** includes 15 positions and is responsible for managing the hardware and software that enables network connectivity, communication, and operations for all business units. This unit is also responsible for providing phone and email support to Oregon's ESDs, school districts, and schools for ODE web-based systems, as well as the acquisition and support services for ODE desktops, laptops, tablets, phones, and peripheral equipment.

The **Enterprise Services Unit** includes 13 positions and is responsible for providing business analyst support to all ODE offices, school districts, and ESDs in supporting the analysis, architecture, and maintenance of agency applications. Additionally, the unit provides strategic policy and operation support through the administration of IT governance; management of IT policies and procedures, and staffing IT agency and statewide initiatives.

While the state's data center hosts most executive branch agencies, ODE contracts with a third-party data center to lease floor space. This data center provides floor space, building security,

and electricity, while ODE is responsible for maintaining and securing its own hardware and software.

# Audit Results

Our review determined that ODE has implemented, or partially implemented, the majority of the controls reviewed during this audit. Specifically, ODE management has provided important protection measures for security, including tools for managing hardware and software inventories, tools for identifying and remediating security weaknesses, and implementing agencywide security awareness trainings. However, we identified specific areas where ODE could improve security controls. In particular, ODE does not have a formal security management and compliance program that establishes a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures. In addition, although ODE performs many critical security tasks, significant work remains to fully implement and mature all six basic cybersecurity controls.

## ODE lacks a formal security management and compliance program

Security management programs of all executive branch agencies should be collaborative efforts with CSS, located within EIS. Under this governance structure, CSS is responsible for enterprise information security strategy and planning, while each individual agency is responsible for the development, documentation, and implementation of a security management and compliance program for its specific environment, including workstations and applications.

To effectively manage security, agencies 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. Specifically, 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 party activities are adequately secured.

We determined ODE does not have a formal security management and compliance program and lacks robust policies and procedures for most security-related controls reviewed. Additionally, we found that ODE does not have processes in place to periodically assess and validate risks and lacks controls to ensure external third parties are adequately secured. This is due, in part, to the passage of Senate Bill 90. Prior to Senate Bill 90, the department had developed some elements of a security management program and had assigned dedicated security staff. After security staff were transferred to CSS, these efforts largely stalled.

While IT security has been largely consolidated within CSS, some aspects of IT security — such as application security, network vulnerability scanning and monitoring, and patching of servers not hosted at the state data center — remain with the agency. The passage of Senate Bill 90 transferred ODE's dedicated security staff to CSS. To compensate for the loss of security staffing, CSS assigned executive branch agencies a Business Information Security Officer to provide guidance, planning, and security leadership. However, at the time of this audit, CSS has not assigned anyone to ODE. In addition, ODE management has not sought resources from CSS. Without sufficient staff assigned to security tasks, some critical activities are performed on an ad hoc basis and ODE's ability to identify and respond to security incidents is hindered.

Without a well-designed program with appropriate staffing and resources, 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 Review

For this audit, 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 using four levels of implementation to provide an assessment of the agency's overall cybersecurity implementation.

**Figure 1: Control Implementation Level Hierarchy**

| | |
|---|---|
| **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 of the sub-controls specifically include automation in the description. For example, sub-controls 2.3 and 3.4 require the use of automated software tools to document software inventory and apply operating system patches, respectively. However, if the agency has manual processes in place that achieve the same objective, we may assess these sub-controls at the performed or partially performed level.

### *CIS Control 1™: Inventory of Authorized and Unauthorized Devices*

| Sub-Control | Title | Description | Assessed Control Implementation Rating: Performed | Defined | Automated | Continuously Improved |
|---|---|---|---|---|---|---|
| 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. | ◑ | ○ | ◑ | ○ |
| | | ○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented | | | | |

We evaluated ODE's processes to identify network devices, maintain an updated inventory of hardware devices, and control devices that can connect to the network. We found the agency has begun implementing the necessary tools to manage its hardware inventory, but generally does not have foundational policies and procedures to provide guidance and requirements for appropriately managing hardware asset inventory.

Although ODE has software for discovering all devices connecting to its network, they have not taken the necessary steps to utilize it to create a complete device inventory. For example, ODE partially automates the process to identify and update inventory for workstations but tracking inventory for other devices is a manual process. However, we found that the manual processes

did not include all hardware connected to the network. In addition, ODE does not have procedures in place to detect and remove unauthorized devices from its network.

We reviewed ODE's inventory lists and concluded they were generally incomplete, out-of-date, and contained numerous inaccuracies. For example, we found ODE did not timely remove decommissioned and disposed devices from the inventory records. Additionally, we found numerous entries that had blank fields or contained inaccurate information.

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 proper controls are in place for those devices.

Additionally, without an accurate, up-to-date inventory of authorized hardware, the agency cannot actively manage and monitor all hardware devices on the network so that only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access.

| Sub-Control | Title | Description | Assessed Control Implementation Rating: Performed | Defined | Automated | Continuously Improved |
|---|---|---|---|---|---|---|
| 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 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 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. | ○ | ○ | ○ | ○ |

○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented

We evaluated ODE's process to document approved software, segregate high-risk software, and identify software installed on its systems. We determined ODE has appropriate tools in place to identify and track software installed on devices connected to its network. However, much work

remains to ensure only authorized and supported software is installed on agency systems. We identified the following weaknesses:

- ODE does not have foundational policies and procedures in place and last updated the list of authorized software in 2014, which includes software with significant known vulnerabilities.
- Unauthorized software has been installed on numerous workstations.
- Numerous installations of middleware were significantly out of date or no longer supported by the vendor.
- While the appropriate tools are in place to do so, ODE does not integrate software and hardware asset inventories.
- ODE has not implemented application whitelisting to ensure only authorized software can be installed on agency systems.

Controls should be established by implementing software whitelisting, automating software inventory, and monitoring software installations on all systems. Organizations should maintain an inventory of software installed on their computer systems similar to the inventory of its hardware assets. Without a complete, accurate, and up-to-date list of the software 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, 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. Attackers can exploit systems with malicious or vulnerable software to gain unauthorized access to the agency's data or disrupt operations.

| Sub-Control | Title | Description | Assessed Control Implementation Rating: Performed | Defined | Automated | Continuously Improved |
|---|---|---|---|---|---|---|
| 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. | ● | ◑ | ● | ○ |

○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented

We evaluated ODE's processes for patching systems to prevent vulnerabilities and for identifying and remediating detected vulnerabilities. We found the department has adequate processes and makes appropriate efforts to keep systems up-to-date with current software patches and to identify and remediate vulnerabilities.

ODE works with CSS to perform weekly vulnerability scans. ODE then prioritizes and remediates the identified vulnerabilities. An analysis of back-to-back scans showed ODE achieved a significant 45% reduction in critical vulnerabilities identified. In addition, operating systems and critical middleware applications were current on most servers and workstations. Only a small number of systems had not been patched within the last month due to a conflict with the maintenance window falling on a scheduled holiday.

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. This could compromise the confidentiality, integrity, or availability of agency data. By scanning

the network for known vulnerabilities, an agency can identify and prioritize software patching and other remediation activities to ensure these known risks are controlled.

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*

| Sub-Control | Title | Description | Assessed Control Implementation Rating: Performed | Defined | Automated | Continuously Improved |
|---|---|---|---|---|---|---|
| 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, 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 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. | ● | ○ | ● | ○ |

○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented

We evaluated ODE's processes to grant privileged access accounts, log and monitor login activity, and to establish robust authentication procedures.[3] We found the agency partially performs activities for the majority of the sub-controls for managing and controlling the use of administrative privileges on its servers. However, ODE could not identify all local administrators on workstations because those accounts are not included in its list of privileged users. Local administrators have elevated privileges allowing them to install software on workstations

[3] 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 has.

without authorization. If attackers obtain these credentials through phishing emails or malicious websites, they may be able to gain access to sensitive data or compromise other systems.

In addition, we noted the agency lacked foundational policies, and its procedures and access request forms were out-of-date, inaccurate, and generally did not provide and audit trail or support for the type of access granted to ensure the application and enforcement of the principle of least privilege.[4]

Although ODE uses software and centrally automated rules to control user accounts with privileged access to servers, we found multiple weaknesses, including:

- Non-expiring passwords for some accounts;
- One active account where the user has not logged in for an extensive period of time;
- Lack of multifactor authentication; and
- Lack of periodic review of privileged accounts.

Management of privileged users should ensure 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, other 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. Therefore, use of accounts with these privileges should be effectively controlled by management, including implementing controls to segregate, manage, and monitor use of these accounts.

[4] Least privilege is a principal that states that users should have the least amount of privileges (access to services) necessary to perform their duties.

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

| Sub-Control | Title | Description | Assessed Control Implementation Rating: Performed | Defined | Automated | Continuously Improved |
|---|---|---|---|---|---|---|
| 5.1 | **Establish Secure Configurations** | Maintain documented, standard security configuration standards for all authorized operating systems and softw are. | ◑ | ○ | ○ | ○ |
| 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 w ith 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 w ill 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 w hen unauthorized changes occur. | ○ | ○ | ○ | ○ |

○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented

We evaluated ODE's processes to document and safeguard baseline configurations, deploy secure configurations, and monitor configurations on its network. We determined ODE has not established secure baselines for most servers, network devices, and workstations. We found ODE relies on staff to establish configuration baselines on a "best effort" basis using individual judgment instead of applying formal guidance or standards. Although centrally automated rules control most workstation configurations, no one reviews the rules or monitors existing configurations to detect unauthorized or inappropriate modifications.

Organizations should have processes in place to ensure hardware and software are securely configured. This should include verifying that default configurations align with business and security needs so that agency systems are not left vulnerable to attack. The agency should also 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. Baselines should be documented so 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.

| Sub-Control | Title | Description | Assessed Control Implementation Rating: Performed | Defined | Automated | Continuously Improved |
|---|---|---|---|---|---|---|
| 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 a 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. | ○ | ○ | ○ | ○ |

○ = Not Implemented ◑ = Partially Implemented ● = Fully Implemented

We evaluated ODE'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 synchronized logging enabled for all workstations, servers, and most network devices. However, we found some logs do not contain the necessary detail for useful analysis and most logs are not reviewed on a regular proactive basis.

In addition, we found ODE has not centralized logging or deployed tools that can provide real time analysis and correlation of event logs. This is due in part to the lack of clarity at CSS with the roles and responsibility over IT security. CSS has communicated its intent to provide statewide centralized logging and event management at some point in the future. Due to the significant costs involved in procuring and setting up centralized logging and event management, ODE management indicated the agency is hesitant to invest resources in these tools, only to have CSS take over responsibility.

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 many organizations rarely review log information, allowing attacks to go unnoticed. Agencies should ensure that information systems 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 critical cybersecurity controls, we recommend ODE, in cooperation with CSS:

1. Implement a security management and compliance program that includes an established framework and continuous cycle of activity for assessing risk, developing and implementing effective security controls and procedures, and monitoring the effectiveness of those procedures.
2. Remedy weaknesses with CIS Control #1 – Hardware Inventory – by developing written policies and procedures, fully automating asset discovery and inventory, and fully implementing hardware authentication controls.
3. Remedy weaknesses with CIS Control #2 – Software Inventory – by developing written policies and procedures, updating documentation of approved software and software versions, and implementing software whitelisting.
4. Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by refining and implementing written policies and procedures, and formally tracking the status of identified vulnerabilities to ensure timely remediation.
5. Remedy weaknesses with CIS Control #4 – Privileged Access – by developing written policies and procedures for granting, reviewing, and removing access for privileged accounts, removing end users administrative access to workstations, maintaining an inventory of administrative accounts, ensuring the use of dedicated administrative accounts, implementing multifactor authentication for all administrative access.
6. Remedy weaknesses with CIS Control #5 – Secure Configurations – by establishing secure configurations for all workstations, servers, and network devices. Additionally, establishing appropriate monitoring and alerts to ensure all changes to configurations are authorized and appropriate.
7. Remedy weaknesses with CIS Control #6 – Audit Logs – by developing a central logging solution, implementing log analytic tools, and automating log review.

# Objective, Scope, and Methodology

## Objective

The objective of this work was to determine the extent to which ODE has implemented an appropriate IT security management program, as well as selected controls from the Center for Internet Security's CIS Controls™, version 7.1.[5] These controls are a prioritized set of actions that collectively form a defense-in-depth structure to help protect systems and networks from the most common attacks.[6]

## Scope

The scope of this work included a review of security management and the first six of the 20 CIS Controls™ in place at ODE during the second and third quarters of 2019. Cybersecurity experts generally agree that these six "basic" controls should be implemented by all organizations for cyber defense readiness. Other elements of internal control were not deemed necessary to achieve the objective of the audit and were excluded from scope.

## Methodology

To assess whether management has established policies and implemented controls to stop cyberattacks that may target the agency, we interviewed agency staff, reviewed documentation, and performed limited testing of selected security management controls and CIS Controls™ one through six. The period for our testing included controls in place between May 2019 and August 2019. In addition to the CIS Controls™, we used the Federal Information System Controls Audit Manual as IT security management criteria.

Due to the sensitive nature of security and in accordance to ORS 192.345 (23) and generally accepted government auditing standards, we communicated the extent of the security weaknesses verbally to agency management to ensure that no critical security information is publicly disclosed.

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

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

---

[5] Center for Internet Security CIS Controls

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

Oregon
Kate Brown, Governor

OREGON DEPARTMENT OF EDUCATION
*Oregon achieves . . . together!*

**Colt Gill**
Director of the Oregon Department of Education

October 31, 2019

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 Education (ODE) – Cybersecurity Controls Audit.

We would like to thank the Secretary of State's staff assigned to the Cybersecurity Controls Audit on their courtesy, professionalism and expertise exhibited during the audit. It was evident early on in the process that we have a common goal of protecting agency information technology assets with standards-based processes and controls.

Below is our detailed response to each recommendation in the audit. For each recommendation, we will work with the Cyber Security Services Office to ensure state security policies, standards and guidelines are followed.

Following your review, we hope you find satisfactory the information in our responses to the recommendations. Should you have any additional questions regarding the information provided, please do not hesitate to contact me at (503) 947-5658 or Peter Tamayo, ODE Chief Information Officer at (503) 947-5705.

| **RECOMMENDATION 1**<br>Implement a security management and compliance program that includes an established framework and continuous cycle of activity for assessing risk, developing and implementing effective security controls and procedures, and monitoring the effectiveness of those procedures. | | |
|---|---|---|
| **Agree or Disagree with Recommendation** | **Target date to complete implementation activities** | **Name and phone number of specific point of contact for implementation** |
| Agree | June 2022 | Peter Tamayo |

**Narrative for Recommendation 1**

ODE regularly participates in the Cyber Security Services (CSS) Information Security Council (CIOC). ODE continues to seek guidance and clarity on the roles and responsibilities of ODE and the CSS as it relates to protecting ODE technology assets and will continue to work together to build a robust information security program.

| **RECOMMENDATION 2**<br>Remedy weaknesses with CIS Control #1 – Hardware Inventory – by developing written policies and procedures, fully automating asset discovery and inventory, and fully implementing hardware authentication controls. | | |
|---|---|---|
| **Agree or Disagree with Recommendation** | **Target date to complete implementation activities** | **Name and phone number of specific point of contact for implementation** |
| Agree | June 2021 | Peter Tamayo |

**Narrative for Recommendation 2**

ODE is currently in process to implement a hardware and software asset management solution to track assets, assist in inventory control of IT related hardware and software, and to detect and alert any unauthorized hardware discovered on the network. Policies and procedures are being crafted to manage the inventory lifecycle and ensure these assets are procured and recorded by IT to ensure this information is accurate at all times.

Further port level security is planned for implementation in the future to validate all hardware attached to the network before providing network access. This work is targeted for completion by the end of the current 2019-21 biennium.

| **RECOMMENDATION 3**<br>Remedy weaknesses with CIS Control #2 – Software Inventory – by developing written policies and procedures, updating documentation of approved software and software versions, and implementing software whitelisting. | | |
|---|---|---|
| **Agree or Disagree with Recommendation** | **Target date to complete implementation activities** | **Name and phone number of specific point of contact for implementation** |
| Agree | June 2021 | Peter Tamayo |

**Narrative for Recommendation 3**

As noted in Recommendation 2, the asset management system currently under review to track hardware assets will also be used to track software assets. This system is expected to be in place by the end of the 2019-21 biennium.

ODE IT is also working to implement a software whitelist limiting which applications will be allowed to run in the environment to the standard software offerings for ODE.

| RECOMMENDATION 4<br>Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by refining and implementing written policies and procedures, and formally tracking the status of identified vulnerabilities to ensure timely remediation. | | |
|---|---|---|
| **Agree or Disagree with Recommendation** | **Target date to complete implementation activities** | **Name and phone number of specific point of contact for implementation** |
| Agree | June 2020 | Peter Tamayo |

**Narrative for Recommendation 4**

ODE will continue to proactively scan for and remediate any vulnerabilities discovered using the CSS provided tools. Policies and procedures around these processes will be defined and documented including the tracking of the identified vulnerability by June 2020.

| RECOMMENDATION 5<br>Remedy weaknesses with CIS Control #4 – Privileged Access – by developing written policies and procedures for granting, reviewing, and removing access for privileged accounts, removing end users administrative access to workstations, maintaining an inventory of administrative accounts, ensuring the use of dedicated administrative accounts, implementing multifactor authentication for all administrative access. | | |
|---|---|---|
| **Agree or Disagree with Recommendation** | **Target date to complete implementation activities** | **Name and phone number of specific point of contact for implementation** |
| Agree | June 2022 | Peter Tamayo |

**Narrative for Recommendation 5**

ODE will define the processes for requesting, assigning, and managing privileged accounts within agency policy along with a stepped procedure that outlines the process for review and the granting of privilege access. In addition, continued process improvements will be established to review current assignment and for the regular auditing of privileged accounts. Processes will be defined for the annual review of required forms for requesting access and will be updated with a revision date of the review and acceptance.

ODE will work with CSS to implement policies around multifactor authentication requirements for all administrative accounts with implementation targeted for completion by the middle of the next biennium.

| RECOMMENDATION 6<br>Remedy weaknesses with CIS Control #5 – Secure Configurations – by establishing secure configurations for all workstations, servers, and network devices. Additionally, establishing appropriate monitoring and alerts to ensure all changes to configurations are authorized and appropriate. |
|---|

| Agree or Disagree with Recommendation | Target date to complete implementation activities | Name and phone number of specific point of contact for implementation |
|---|---|---|
| Agree | June 2022 | Peter Tamayo |

**Narrative for Recommendation 6**

ODE configures servers and network devices that follow best practices for the specific service being provided by the server or device. Workstations are currently constructed using an ODE approved server image ensuring all machines have the appropriate base configuration.

Moving forward, ODE will work to implement a baseline configuration compliance scan to automatically monitor for systems to ensure that any changes made to those baselines are sent to the appropriate personnel to ensure compliance. Implementation is targeted for completion by the middle of next biennium.

| **RECOMMENDATION 7**<br>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** | **Name and phone number of specific point of contact for implementation** |
| Agree | June 2021 | Peter Tamayo |

**Narrative for Recommendation 7**

ODE will work closely with the CSS to develop agency SIEM capabilities and identify what options are available for agency Implementation. ODE is currently reviewing what information is being logged in preparation for evaluating options for a secure central logging system to allow real-time analysis and correlation of events with our CSS partners.

ODE in collaboration with CSS will establish operational policies, procedures, roles and responsibilities in regards to the implementation of recommendation 7.

Sincerely,

Colt Gill
ODE Director

## Audit Team


William Garber, CGFM, MPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Matthew Owens, MBA, CISA, Principal Auditor

Sherry Kurk, CISA, Staff Auditor


## About the Secretary of State Audits Division

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


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

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

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