Oregon Department of Education

Opportunities Exist to Improve Web Application Security and Tracking of Website Accessibility Remediation Efforts

November 2021
Report 2021-32

OREGON SOS
Secretary of State
Shemia Fagan

OREGON AUDITS DIVISION
Audits Director
Kip Memmott

Audit Highlights

Oregon Department of Education

Opportunities Exist to Improve Web Application Security and Tracking of Website Accessibility Remediation Efforts

Why this audit is important

- Insecure web applications can put data at risk of inappropriate disclosure.
- The Oregon Department of Education (ODE) hosts several web applications containing sensitive student data.
- Though useful, web applications inherently increase security risks.
- Federal regulations require agencies that receive federal funding to provide equal access and services to people with disabilities.
- In 2016, ODE entered into a joint resolution with the United States Department of Education Office of Civil Rights to ensure web content is accessible to people with disabilities. In 2021, the agreement was terminated because the Office of Civil Rights determined ODE's actions resulted in equal opportunities for people with disabilities to participate in the agency's online activities.

What we found

1. ODE has multiple controls in place to ensure the security of the agency's web applications. However, opportunities exist for ODE to strengthen web application security by improving network and application development security processes. (pg. 5)
2. ODE should develop a more robust security program, including prioritizing and remediating identified deficiencies; ensuring policies and procedures are documented and up to date; and providing security training to key personnel. (pg. 9)
3. ODE has implemented a policy and procedures to ensure the accessibility of online content to people with disabilities. This includes processes to leverage automated solutions and manual review to remove accessibility barriers. However, there are opportunities to better track and document these efforts. (pg. 11)

What we recommend

We made 14 recommendations to ODE. ODE agreed with all of our recommendations. The response can be found at the end of the report.

OREGON SOS

OREGON AUDITS DIVISION

Introduction

The Oregon Department of Education (ODE) oversees the education of students in Oregon's public pre-kindergarten through 12th grade education system. This includes over 1,200 schools in 197 school districts as well as 19 education service districts.[1] While ODE does not provide direct classroom services, the agency helps districts by developing policies and standards, providing data to inform instruction, training teachers, and administering state and federal grants.

To this end, ODE maintains several web applications for school districts to submit student, staff, and institution data for state and federal reporting. Web applications are also used to support agency programs such as child nutrition, and operational needs such as grant management. Most of ODE's web applications are developed and managed by staff at ODE.

The purpose of this audit was to determine whether ODE has effective processes in place to mitigate risks to the confidentiality, integrity, and availability of information submitted through the agency's web applications. Additionally, we evaluated whether appropriate processes are in place to ensure the agency's online content is accessible to people with disabilities.

As the state's education agency, ODE collects a large amount of student data which may contain sensitive or private information

The Oregon Constitution identifies the Governor as the Superintendent of Public Instruction. The Governor has appointed a Deputy Superintendent, who serves as the director of ODE. In the 2019-21 biennium, the agency's legislatively approved budget exceeded $13 billion; however, most of these dollars pass through ODE as funding for schools, with only about 2% of the total budget allocated for department operations. ODE's operations budget includes funding for the department's Office of Finance & Information Technology, which had an operating budget of $77 million and 125 positions prior to the 21-23 legislative session. This office includes several units, such as Financial and Accounting Services, Procurement Services, and Information Technology Services. The Information Technology Unit consists of:

- **IT Operations & Support**, which manages ODE's network and servers, as well as provides technical support to agency staff and district partners;
- **IT Enterprise Services**, which includes business analysts and database architects. The business analysts work with customers to create requirements and manage the ODE collections for state and federal reporting. The enterprise architect team maintains ODE's technology infrastructure, including database architecture and access management;
- **IT Application Development**, which includes quality assurance and developers who develop and maintain ODE's web and internal applications, data, web services, application security, application accessibility, and testing; and

[1] Education service districts assist school districts and ODE in achieving Oregon's educational goals by providing regionalized core services to component school districts, including programs for children with special needs, technology support for component school districts, school improvement services, and administrative and support services.

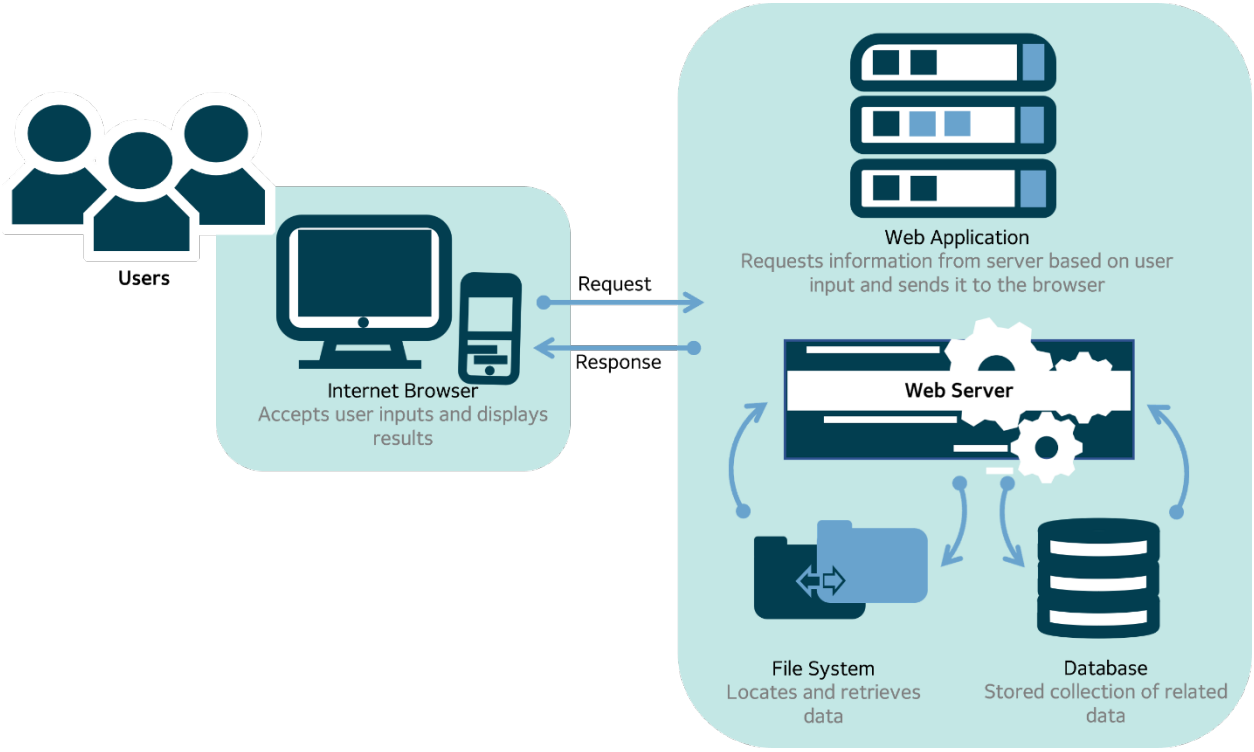
- **IT Governance, Policy, and Strategy**, which supports and improves users' experience through accessibility, training, standardizing and promoting technology tools, communication, and consistency for agency staff and district partners.

School districts submit student data via web applications to ODE for multiple purposes

ODE collects a large amount of data from schools pertaining to students, such as enrollment, assessment, and disciplinary data; school staff, including position, assignments, and demographics; and education institutions, such as budget, capacity, and services provided. Data collected through multiple applications is publicly available through ODE's Collection Catalog.[2]

To make it easier for districts to report this data to ODE, the agency developed and maintains more than 60 web applications to facilitate data reporting while maintaining data security. Some of these applications collect sensitive and private data. For example, Senate Bill 155 established requirements for ODE to conduct investigations related to reports of suspected abuse or sexual conduct that may have been committed by a school employee. Other applications are available to the public, including applications to look up information about ODE public staff, institution-related information, and a school and district's report card. A full list of ODE's web applications can be found in Appendix A.

Figure 1: Web application architecture includes multiple systems



Web applications are software programs that run on a web server — a computer providing World Wide Web services on the internet — and are accessible by users through an internet browser (such as Microsoft Edge, Google Chrome, Mozilla Firefox, or others).

[2] ODE's Collection Catalog is available at www.ode.state.or.us/apps/CollectionCatalog.

While web applications serve to improve operational and reporting efficiencies, they inherently add increased risk. This is because web applications are designed to facilitate the sharing of sensitive information over the internet, and therefore introduce a new attack surface for hackers. By targeting the user's browser, or the application code itself, attackers can glean information from unsuspecting users, access sensitive data, or disrupt operations. However, entities can mitigate this risk by ensuring the identification and remediation of vulnerabilities in web applications and the networks on which they are hosted.

Information security responsibilities are shared between Enterprise Information Services and state agencies

Information and cybersecurity at ODE is not the sole responsibility of ODE management. Enterprise Information Services (EIS), an organizational unit of the Department of Administrative Services, has a role to play from the enterprise perspective in ensuring information technology (IT) security.

In September 2016, the Governor signed Executive Order 16-13, unifying IT security functions for most state agencies to protect and secure information entrusted to the State of Oregon. The order directed executive branch agencies, including ODE, to consolidate security functions and staffing into the Office of the State Chief Information Officer, now known as EIS. 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 passage of Senate Bill 90 in June 2017 made the order permanent.

EIS maintains policy and statewide IT oversight functions. Cyber Security Services (CSS), a division of the EIS, brings together elements of enterprise security — including governance, policy, procedure, and operations — under a single accountable organization. CSS continues to define the division of security responsibilities and functions between its office and the executive branch agencies. However, in accordance with the Statewide Information Security Plan, agencies retain responsibility for many organization-level security controls. For example, the plan requires agencies to establish secure system development environments along with controls over access management, configuration management, malware protection, logging and monitoring, and other IT security areas.

ODE entered into a joint resolution to address potential barriers to website access for people with disabilities

Given the large role ODE plays in the lives of many of Oregon's children and their families, equity is an important consideration for the agency. This may include gathering data to track outcomes and progress for historically underserved populations, such as improvement efforts at schools receiving grants for low-income student populations.[3] Alternatively, equity considerations at ODE may involve ensuring students with disabilities have access to appropriate services and supports.[4] As with many

[3] See audit reports 2019-01, "ODE and PPS Must Do More to Monitor Spending and Address Systemic Obstacles to Student Performance, Particularly at Struggling Schools" and 2021-28, "Recommendation Follow-up Report: ODE Must Accelerate Efforts to Monitor Spending and Improve Initiatives to Help Vulnerable Students."
[4] See audit report 2020-24, "ODE Can Better Support Students Experiencing Disabilities Through Improved Coordination and Monitoring of Services."

state agencies, equitable services can also include ensuring public information and services online are available to all Oregonians — including those with disabilities.

In 2016, a special education advocate in Michigan filed approximately 500 complaints advocating for website accessibility for students with disabilities across the United States. Later that year, the United States Department of Education's Office for Civil Rights (OCR) announced it had entered into settlement agreements over website accessibility with schools, districts, and departments of education in multiple states, though it is unclear which settlement agreements were driven by the complaints.

ODE entered into a joint resolution agreement with the OCR in June 2016. The agreement explicitly states it was entered into voluntarily and does not constitute admission that ODE violated federal statutes. The agreement enumerates several remedies and reporting steps ODE would take to ensure its web content is accessible to people with disabilities, in accordance with recognized technology standards. These steps include:

- Submission of proposed policies and procedures to ensure online content and functionality will be accessible to people with disabilities;
- Proposal of an auditor to audit ODE's website content and functionality;
- Implementation of an approved Corrective Action Plan to address inaccessible content and functionality identified during the audit;
- Publication of a notice on its website to persons with disabilities regarding how to request access to online information; and
- Delivery of website accessibility training to appropriate ODE personnel.

In January 2021, the OCR notified ODE that the resolution agreement was terminated, and OCR would no longer monitor ODE's implementation of the agreement. This termination was based on OCR's testing and monitoring, through which it determined ODE's actions resulted in equal opportunities for people with disabilities to participate in the agency's online programs and activities as well as effective communication of those programs and activities. OCR found ODE had successfully remediated the identified barriers on selected web pages and had posted an accessible notice on its website outlining procedures for users to notify ODE of, or request access to, inaccessible online content.

Audit Results

Robust web application security requires a multi-faceted information and cybersecurity control system. We found ODE has designed multiple controls to protect the confidentiality, integrity, and availability of data submitted through web applications, including both application-level and network-level controls. However, several of the controls we identified were not fully or appropriately implemented. Moreover, we identified some opportunities for the agency to improve the design of its control system to better safeguard its web application security environment.

We also found ODE has developed a policy and procedures to ensure web content is accessible to people with disabilities. This includes ongoing review of information on the agency's website to ensure common barriers to accessibility are identified and remediated. However, we found this important work could be improved by ensuring policy and procedural documentation is up to date and remediation work is tracked more consistently. Though the agency has requested additional funding to support this effort, the request was not approved by the legislature.

ODE should bolster controls protecting web applications

We evaluated whether ODE has processes in place to ensure its web applications are appropriately secure. Securing web applications includes validating the security of the web application itself, but also involves securing the various layers of the environment within which the application operates. Although envisioned differently throughout the information security realm, these layers often include:

- Policies, procedures, and awareness as the foundation;
- Physical security controls, such as locked doors for rooms housing critical hardware;
- Network security, such as intrusion detection and prevention mechanisms;
- Endpoint or Server security, such as processes to ensure patches are up-to-date;
- Application security, such as vulnerability scanning; and
- Data security, such as encryption.

This layered approach creates a series of barriers that are more robust than any single line of defense. Such is the premise of "defense in depth" — an information security concept intended to ensure security mechanisms are layered throughout the IT system to protect the confidentiality, integrity, and availability of the network, applications, and data.

Processes to secure agency web applications are generally in place, but should be enhanced

Statewide standards, set forth by EIS, state that personnel duties should be separated to minimize the potential for abuse of privileges; this includes ensuring system developers do not have unmonitored access to production environments. Further, these standards require that developers should implement only approved changes to systems containing sensitive data; this requirement aligns with best practices which also state entities should document policies and procedures governing how such processes should be implemented. State standards also require agencies to scan systems for vulnerabilities, analyze scan reports, and remediate legitimate vulnerabilities. Finally, state standards require user accounts accessing systems with sensitive data to be disabled when the account has been

inactive for 60 days. However, if the standards cannot be implemented, they allow for agencies to document deviations and indicate compensating protection mechanisms, with the approval of EIS.

We found appropriate processes are in place to review and approve code changes to web applications before they are deployed; however, this process could be enhanced by developing formal code review processes to ensure only approved changes are put into operation. Additionally, the agency has tools and processes to scan applications for vulnerabilities at least annually, though scans are not always performed at this frequency. We also determined ODE has not obtained a written exception for deviations from statewide standards in processes to disable some inactive accounts.

We reviewed a selection of changes to web applications and found changes were appropriately reviewed and approved. Further, we found duties were separated so developers did not both edit code and put code into operation. However, we determined ODE does not have clearly documented processes to ensure only approved changes are made to agency systems. While management indicated lead developers perform code review on all changes made by new developers, once a developer has proven they are following standards and best practices the lead developers choose to review code based on best judgement. Without thorough code review processes, unintended changes may be put into operation, which could inadvertently introduce security vulnerabilities.

We also found development staff and management at ODE work together to develop a schedule to scan web applications at least annually using software designed to identify vulnerabilities. Management indicated applications are also scanned prior to promoting any major change to production, to identify vulnerabilities which may have been introduced during development. Application scans are performed in addition to network scans, which are performed more frequently and are discussed in the network security section of this report.

We found one application had not been scanned in the 12 months prior to our review. According to ODE management, a full scan of this application would require ODE staff to open each collection within the application. This work would need to take place during a time when no districts are using the system, which would require significant coordination and effort. Prior attempts to scan the system proved to be disruptive to users. Despite this, agencies should periodically scan systems and hosted applications

for vulnerabilities. Known vulnerabilities create an easy target for attackers, which puts agency systems at risk of disruption and sensitive data in peril of inappropriate disclosure.

We reviewed controls in place to manage access to ODE's Central Login, the online portal through which districts access most of the agency's externally facing web applications. ODE has a process to automatically disable user accounts accessing Central Login after they have been inactive for a defined period, which can happen if a district user leaves their job, changes roles, or simply doesn't have a business reason to access the application frequently. However, we found the length of time a user is inactive before their account is disabled exceeds the 60-day period defined in statewide standards.

Management indicated they have extended the allowable inactive account period because they expect some users will not log in every 60 days, though they still have a valid reason to maintain access. This is because some users only log in to submit certain reports that are not submitted every 60 days. While statewide standards do allow for deviation from the rule for business reasons, so long as it is approved by EIS, ODE has not documented this approval.

When user accounts retain access unnecessarily, they may have access to data they do not require, which violates best practices indicating users should only have access to information required for their professional role. Moreover, these stale accounts provide an avenue for bad actors to inappropriately access data, increasing the risk that sensitive data may be inappropriately disclosed.

We also identified deficiencies in data storage, access, and logging. Agency management stated there are projects underway to address some of these issues. The details of these findings were communicated to the agency in a confidential appendix due to the sensitivity of the deficiencies, in accordance with ORS 192.345(23).

Network security practices should be strengthened

In addition to ensuring web applications themselves are securely developed, organizations should have appropriate processes in place to protect the network on which applications are hosted. This provides a layered approach to security so attackers are less likely to succeed in accessing sensitive data or otherwise disrupting entity operations. We identified several opportunities for ODE to improve network security practices.

Statewide security standards require executive branch agencies to develop, document, and maintain current baseline configurations for network devices. Documentation of baseline configurations allows management to ensure devices are configured securely by defining expected settings and monitoring actual settings to ensure they align with baselines. However, ODE has not documented baseline hardware and software configurations for network devices. Without clearly defined baselines, management may not identify when unauthorized configuration changes occur, which can introduce vulnerabilities to the agency's network.

ODE also performs periodic network scans to identify security vulnerabilities. However, we found some vulnerabilities were not timely remediated. Agencies should use a risk-rating process to prioritize the remediation of discovered vulnerabilities, to ensure the vulnerabilities of the highest risk are addressed more quickly. Furthermore, agencies should compare the results of scans to verify vulnerabilities have been remediated in a timely manner. ODE did not have a process to prioritize identified vulnerabilities

nor develop a formal plan of action for identified weaknesses. Attackers commonly exploit systems that have known vulnerabilities.

We found two servers where the agency did not have antivirus software installed. Staff indicated they had removed antivirus software on the two servers earlier in the month for troubleshooting purposes and then did not reinstall it. Staff reinstalled the software on the servers when it was brought to their attention; however, improving monitoring processes would allow ODE to identify instances such as this and ensure malware protection remains installed on servers. Statewide standards require all systems to employ malicious code protection mechanisms on servers. Without appropriate protection mechanisms in place, attackers can use malicious code, such as viruses, to exploit systems to gain unauthorized access to data or disrupt operations.

During our review, we also found multiple gaps in privileged access management. At least one user had elevated privileges they did not need. Elevated privileges allow users to access advanced system functions, and actions under these accounts may have critical effects on agency systems and may permit access to sensitive data or system information. We also identified a service account with elevated privileges which network staff stated was no longer necessary.

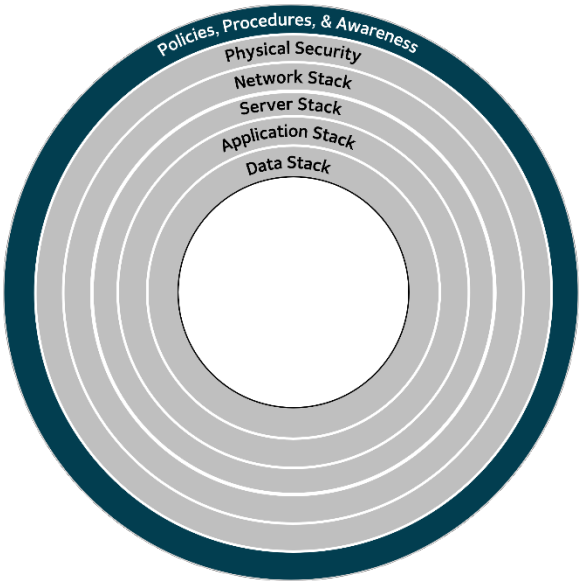
Management was unable to provide documentation authorizing elevated access for some privileged users. Though agency staff indicated they periodically review privileged access for appropriateness, processes are not well defined or documented. Management is responsible for ensuring privileges assigned to users are reviewed to validate the need for such privileges and restricting privileged accounts to authorized individuals with a need for elevated privileges.

We also determined ODE does not employ multifactor authentication for privileged access users accessing the network. Multifactor authentication requires the use of two or more different factors when verifying a user's identity for a system. Authentication factors include something you know (such as a password), something you are (such as a fingerprint), or something you have (such as a cryptographic key). Statewide standards state that agencies should implement multifactor authentication for access to privileged accounts. The use of multifactor authentication reduces the risk

of an attacker gaining access to a privileged account, and thereby, to sensitive data or system resources.

ODE has not developed a well-defined security program

A well-defined and continuously monitored security program is foundational for effective security control operations. The program should have processes to identify, prioritize, and remediate deficiencies in the entity's security control framework. A robust security program also includes formal, management-approved policies and procedures which clearly describe security controls, roles, and responsibilities. Once defined, the organization should establish a training program to ensure employees and partners have adequate training to carry out their security responsibilities. We identified several gaps in ODE's security management program.



ODE lacks processes to ensure remediation of identified deficiencies

During our audit, we found several deficiencies identified in two prior audits and an external, sensitive security assessment remained unresolved.[5] When initially asked about the implementation status of prior findings related to our audit objective, the information was not readily available. Management indicated the lack of a documented remediation plan was, in part, due to shifts in department management over the past several years.

Statewide standards state agencies should develop a plan of action and milestones for systems to document the planned remedial actions to correct identified weaknesses or deficiencies. A documented action plan allows management to track the status of remedial actions and reduces the risk that monitoring will be disrupted by staffing changes. Without a plan of action to remediate identified deficiencies, security weaknesses such as those identified in this report are not adequately prioritized nor remediated in a timely manner.

[5] See audit report 2016-32, "Oregon Department of Education: Computer Systems Ensure Integrity of Data, But Other Processes Need Improvement" and audit report 2019-39, "Oregon Department of Education Cybersecurity Controls Audit."

Policies and procedures are generally outdated, and in some cases have not been developed

ODE lacks policies and formal procedural documentation around several security topics relevant to our audit objective. The agency frequently pointed to its Information Security Plan for security policies; however, this document was outdated and, in many cases, did not accurately reflect the technology or processes employed by agency staff.

Security topics not addressed in up-to-date formal policies include:

- Vulnerability Scanning;
- System Security Plans; and
- Privileged Access.

Best practices advise that security controls and procedures at all levels should: be documented; appropriately consider risk; address purpose, scope, roles, and responsibilities; and be approved by management. Without clearly documented policies and procedures, personnel may not have a clear understanding of operational objectives or their role and responsibility in achieving those objectives.

The agency has not implemented a security training program for internal or external users

ODE does not have a training program in place to ensure key agency employees and other education partners receive security-related training relevant to their role and duties. Agency staff receive annual security training through EIS; however, this training covers only basic security concepts and is targeted at a broad range of state workers. Additionally, while management indicated they used to provide security training to district security staff, that training no longer occurs.

Although security management for state executive department agencies is centralized at CSS, agencies maintain responsibility for some security functions. For example, developers are responsible for ensuring security is built into systems they design and maintain. Additionally, privileged access users should be familiar with security best practices related to their responsibilities to manage sensitive technology assets.

Statewide standards require executive department agencies to provide role-based, security-related training to software development personnel and personnel with privileged access. Appropriate training increases the likelihood that key staff will be familiar with security threats as well as best practices to defend against them.

Additionally, while ODE's technology group is responsible for managing privileged access, as well as provisioning access to users throughout the agency, management in other areas are responsible for approving access to the systems and data owned by their department and notifying the technology department when users no longer require access. Yet according to management in the technology department, management in other areas of the agency do not always include an end date in access requests and are not always timely in communicating when access should be terminated.

For example, we identified one user with access to Central Login who no longer worked for ODE. Failure to disable access when it is no longer required violates the principle of least privilege, wherein users should only have access to information they require for their role, and increases the risk of

inappropriate access to data. Management in ODE's IT department should ensure all individuals responsible for approving access are trained in expected procedures for authorizing, monitoring, and terminating access for individuals with access to systems they own.

Further, access to ODE's Central Login system allows users at school districts and education service districts to access many of ODE's web applications. These applications are used by district staff to submit information to meet state and federal reporting requirements. Since it would be inefficient for ODE to directly manage the access to these systems for employees at all the districts in the state, ODE grants district security administrators the ability to provision and revoke access to employees within their district.

However, ODE does not currently have a formal training program to ensure security administrators are aware of best practices concerning system access security. There are several security concerns around granting and monitoring access to systems, especially those with sensitive data. For example, we found multiple users with generic names (e.g., Accountant01); though best practices state users should be uniquely identifiable so their actions in a system can be traced to the individual.[6]

The Privacy Technical Assistance Center at the U.S. Department of Education advises that education leaders should recognize the importance of security training for all data users and employ best practices. This includes ensuring all employees and partners with access to personally identifiable information be trained to protect data confidentiality and preserve system security. Moreover, the center notes that effective training includes content with tailored elements for different employee job categories and responsibilities.

The agency has developed processes to ensure equitable accessibility to its public websites, though processes should be matured

We found ODE has developed a policy and procedures to ensure people with disabilities are able to access the agency's electronic content; though documentation should be updated to ensure they reflect current processes and objectives. The agency's procedures include reviewing website content to ensure it is accessible to people with disabilities by identifying and remediating common barriers, as well as providing training to agency staff and training resources to external partners. However, we identified a risk that unstable funding may hinder the consistency of this work.

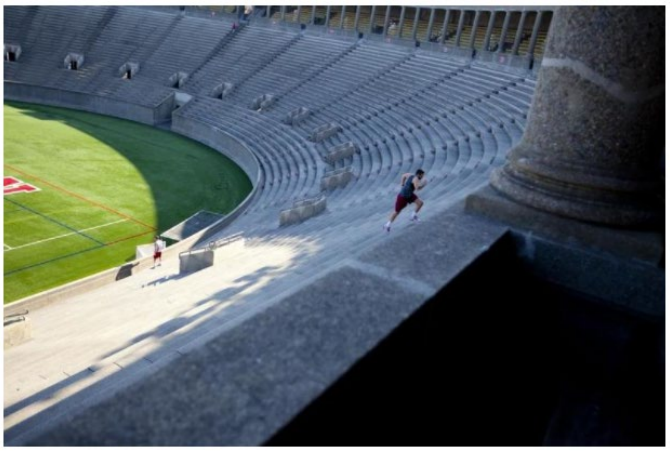
Documented policies allow agency management to define operational objectives and controls to ensure the effectiveness of those objectives, as well as roles and responsibilities so parties can be held accountable for their assigned responsibilities. We found ODE has documented a policy and procedure on website accessibility; however, these documents are outdated. The current policy states it should be reviewed annually, but the last review date was September 2018. Moreover, we found procedure documentation has not been formally approved by management and does not reflect all roles, responsibilities, and processes — specifically, it does not include the duties of the web accessibility technician performing website remediation.

[6] The username provided in this example is a hypothetical demonstration and was not actually identified by auditors during our review of usernames in ODE's system.

We also found the current policy and procedures do not address how feedback from individuals with disabilities will be reviewed and incorporated in accessibility efforts. The motto "Nothing About Us Without Us" emphasizes the importance of participation of people with disabilities in strategies and policies which affect their lives. While ODE has performed some outreach both indirectly through survey questions collected to address the joint resolution with OCR, and directly by soliciting feedback from those experiencing accessibility issues on their website, the agency would benefit from continued outreach and cooperative work with the disability community as they move forward with accessibility efforts.

ODE has established processes to review content published on its website and remediate deficiencies in content accessibility. Part of the review process involves checking for accessibility problems using software. However, management indicated they rely more heavily on the knowledge, skills, and abilities of their staff when reviewing web content for accessibility issues, as the software tools are limited in the problems they can identify. For example, the tools used by the agency may be able to determine whether an image has alternative text; however, a human is needed to look at whether the alternative text on the image is useful to users.[7]

Figure 2: Contextually relevant descriptive alternative text is more accessible to people with disabilities



Alt-text with no context:

A mostly empty stadium.

Alt-text on a page about recent turnout for track tryouts:

Harvard Stadium with two lone runners bounding up the steps.

Alt-text on page about renovation projects:

Harvard Stadium with cracked concrete pillars.

Source: Harvard.edu digital accessibility website

When ODE's web content editors make changes or additions to web content, a web accessibility technician receives an automated alert that the website is ready to be reviewed for accessibility

[7] Alternative text, commonly referred to as "alt text," provides a text alternative for images. Alternative text can be read by screen readers in place of images, allowing the content and function of the image to be accessible to those with visual or certain cognitive disabilities.

deficiencies. Using a combination of automated tools and professional knowledge, the technician reviews the content for common problems likely to make the information inaccessible to people with disabilities.

To track the remediation work, the web technician maintains a spreadsheet listing the website pages and elements reviewed on each page by date. We found gaps where review had not been documented for several months. Management indicated the remediation work had continued during this time, and provided example emails they had received during this gap period which demonstrated the technician was performing remediation work. However, those emails were very high-level, only providing the number of pages reviewed, rather than the substance of the review conducted. Without proper documentation, management cannot track the progress of pending and completed website accessibility review work, increasing the risk of some web content containing accessibility impediments.

In January 2021, the agency's web accessibility technician left the role to take another position with the agency. The technician position remained vacant until June. During the vacancy, remediation efforts slowed, as pages were only remediated at the request of the agency's webmaster.

The web accessibility technician is currently staffed as a limited duration position, due to lack of dedicated funding for the position. During our audit, ODE requested funding in the 2021 legislative session to hire additional staff to support the agency's efforts to ensure the accessibility of online content. The request included funding for two positions: a permanent web accessibility technician and a web accessibility specialist. Although the agency did not receive approval for either position, ODE plans to maintain the technician as limited duration until stable funding can be secured for the position.

As part of the agency's efforts to ensure website content is accessible to users with disabilities, ODE has developed training resources for internal and external staff on best practices in accessible website development. Several internal staff have received at least basic training in accessible web development. ODE staff have also provided training to external groups, including Oregon's Electronic Government Program user group.[8] Developing and providing training demonstrates management's commitment to competence by enabling individuals to develop proficiencies appropriate for their role.

[8] Oregon's Electronic Government Program, or E-Government Program, manages the Oregon.gov portal hosting over 165 websites. According to its website, it is the largest enterprise provider of websites, internet applications, transparent government data, collaboration tools, and online payment processing within state government.

Recommendations

To improve web application and network security processes, we recommend ODE:

1. Document and implement code review processes to ensure that only approved changes are made during application development.
2. Ensure all web applications are scanned at least annually. Where barriers exist to the annual performance of application vulnerability scans, document a plan of action to address those barriers so scans can be performed.
3. Work with CSS to determine if it is appropriate to extend the allowable time for user inactivity before disabling Central Login accounts. If both parties agree to an extended inactive period, document the deviation, and indicate the compensating controls put in place. In alignment with statewide standards, ensure the documentation is signed by the ODE director and approved by EIS.
4. Document baseline configurations for all network devices. Review and update baseline configurations periodically, as defined by Statewide Information and Cyber Security Standards. Ensure subsequent changes are managed in accordance with statewide standards.
5. Develop a risk-rating process to prioritize the remediation of vulnerabilities discovered in network scans and compare the results of back-to-back scans to verify vulnerabilities have been remediated in a timely manner.
6. Periodically review anti-malware software to ensure each of the agency's servers remain protected.
7. Document authorization for all privileged access users. Review privileged access accounts at least semi-annually for continued appropriateness, including service accounts with elevated privileges.
8. Implement multifactor authentication at the system level for access to privileged accounts.
9. Implement recommendations associated with separately communicated confidential findings.

To improve ODE's security management program:

10. Develop a documented plan of action and milestones to correct weaknesses identified in this audit, as well as outstanding deficiencies identified in other audits and assessments.
11. Ensure policies and procedures governing web application and network security are documented and up to date.
12. Provide role-based, security-related training for software developers, privileged access users, data owners approving access to agency systems, and district security administrators.

To enhance efforts to ensure the accessibility of website content:

13. Update policies and procedures governing website accessibility, including processes to incorporate feedback from members of the disability community, to ensure they reflect current program objectives and address key roles and responsibilities.

14. Periodically review website remediation tracking to ensure documentation is complete and effective in achieving the agency's objectives related to website accessibility remediation.

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether ODE has:

1. Implemented effective controls to ensure the agency's web applications are adequately secure.
2. Implemented effective controls to ensure web content is accessible to persons with disabilities.

Scope

The focus of this audit was to assess the design and implementation of controls over web application security, as well as network security as it relates to the security of web applications within our scope. We also assessed the design and implementation of controls over the accessibility of website content to people with disabilities.

Our evaluation of web application security was limited to externally facing applications (i.e., applications accessible by users that are not ODE employees). The majority of ODE's externally facing web applications are built and managed by ODE staff; however, we performed a limited review of contract language for third-party agreements.

Our review of website accessibility was limited to ODE's website. Although we identified two resolution agreements between ODE and OCR, in accordance with audit standards, we determined further inquiry as to ODE's compliance with these resolutions may interfere with OCR's ongoing investigation.

We focused on controls and processes as they existed during 2021 through November.

Methodology

To gain an understanding of web application and network security controls, as well as website accessibility processes, we conducted inquiries of management and program staff in ODE's Office of Finance and Technology; specifically, those in the IT Operations & Support, IT Enterprise Services, and IT Application Development, and IT Governance, Policy, and Strategy units.

We observed network device settings and website accessibility review processes. We also examined privileged access users and account settings; external user accounts; and application change history records.

We inspected:

- ODE's information security plan, policies, and procedures;
- ODE's web application inventory;
- Website accessibility policy and procedures;
- Website accessibility remediation tracking documentation;
- Prior audit findings and recommendations;
- Training records;
- Application and network scan reports; and
- Project documentation.

For our criteria, we used the Statewide Information and Cyber Security Standards published by CSS, where applicable. We also used the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 5 and the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM) to identify best practices and controls deemed relevant to our audit objectives.

Internal control review

We determined the following internal controls were relevant to our audit objective.[9]

- Control Activities
  - We considered whether management has designed control activities to achieve objectives and respond to risk.
  - We considered whether management has designed the entity's information system and related control activities to achieve objectives and respond to risks.
  - We considered whether management has implemented control activities through policies.

Deficiencies with these internal controls were documented in the results section of this report.

We considered the risks posed by publicly releasing any information related to security findings. As part of our consideration, we balanced the need for stakeholders, such as the Legislature, to be informed on critical or systemic IT security issues affecting the State against the need to protect the agency from cybersecurity threats. Consequently, in accordance with ORS 192.345(23) and generally accepted government auditing standards, we excluded some security weaknesses from this public report and provided them to agency management in a confidential appendix.

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

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

Audit team
Teresa Furnish, CISA, Audit Manager
Jessica Ritter, CPA, CISA, Senior Auditor
Courtney Pearcy, Staff Auditor
Sheila Faulkner, Staff Auditor

[9] Auditors relied on standards for internal controls from the U.S. Government Accountability Office, report GAO-14-704G.

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.

Appendix A: ODE Web Applications

The following list is based on the inventory of ODE web applications provided by the agency's management and adapted to remove extraneous information in the description field:

Application Name	Description
Data Collection Container	**Accessed through Central Login**
Student Level Collections	Each student level collection requires districts, schools, ESD's to login through our Central Login system to gain access to the respective collection. Each district and/or ESD has a security administrator (DSA) registered with ODE. These DSA's grant access to those staff that require access to submit data to collections, access secured reports, verify data, etc.
Staff Level Collections	Each staff level collection requires districts, schools, ESD's to login through our Central Login system to gain access to the respective collection. Each district and/or ESD has a security administrator (DSA) registered with ODE. These DSA's grant access to those staff that require access to submit data to collections, access secured reports, verify data, etc.
Institution Level Collections	Each institution level collection requires districts, schools, ESD's to login through our Central Login system to gain access to the respective collection. Each district and/or ESD has a security administrator (DSA) registered with ODE. These DSA's grant access to those staff that require access to submit data to collections, access secured reports, verify data, etc.
Secure Web Applications	Accessed thru Central login or other application portal
Sexual Conduct Verification System	Senate Bill 155 established requirements for ODE to conduct investigations related to reports of suspected sexual conduct that may have been committed by a school employee, contractor, agent, or volunteer who is not licensed by the Teacher Standards and Practices Commission.
Youth Development Division Data Manager	Youth Development Division Data Manager - The Youth Development Council was created to support Oregon's education system by developing state policy and administering funding to community and school-based youth development programs, services, and initiatives for youth ages 6-24 in a manner that supports educational success, and career and workforce development, juvenile crime prevention, and is integrated, measurable and accountable.

Application Name	Description
Accountability Warehouse Extract	Tool used by districts/institutions to extract accountability data
CIP Budget Narrative	Describes how Federal funds will supplement District funds and programs and captures how ESEA and Perkins funds will be spent to support the attainment of the Districts' improvement goals.
Child Nutrition Direct Certification Match	Child Nutrition Programs gather three data sets from DHS/OHA and one from ODE: SNAP (Supplemental Nutrition Assistance Program) participants, students in the Foster system, Medicaid recipients, and SSID (Statewide Student Identifier), respectively.
Child Nutrition Programs Web Application	Application used the CNP to administer Child Nutrition programs
Electronic Grant Management System	This is the system through which subrecipients receive subgrant notifications from ODE and submit claims for subgrant funding.
Oregon Migrant Student Information System*	This application gathers eligible migrant student information (demographic, attendance, credits, supplemental services, etc.) data that are required by the federal government and the National Migrant Student Information eXchange system
Special Ed Performance Review & Improvement	This system focuses on procedural compliance and performance indicators identified through federal and state regulation and previous state monitoring findings.
Secure Assessment Reports 2.0	Secure Assessment Report Application
Special Ed Post School Outcomes 2.0*	Special Ed Post School Outcomes Application
Student Centered Staging	The Student Centered Staging application contains test event records that have been received by ODE from an external vendor, which include student demographics and other attributes, institution identifiers, test attributes, and record resolution attributes calculated by ODE.
Bus Driver Portal	Pupil Transportation Bus Driver Application Portal
IDEA Data Manager*	The IDEA Data Manager Application is a web-based application that contains tools and serves as the submission site for certain special education data collections.

*Vendor Application

Application Name	Description
Indirect Cost Rate Certification	Application tracks the status of the LEA's annual indirect rates. Integrated with an Extranet web application that allows districts/schools to submit adjustment data for approval by ODE fiscal staff.
Career and Technical Education	Data system and dashboard for CTE/STEAM and High School Success to track all aspects of Programs of Study (POS), courses, post-secondary affiliations, and contacts.
Achievement Data Insight	Application used by district to validate data.
Student Enrollment	Student enrollment is based on the students who were attending your district or school on the first school day in May, as submitted in the 3rd Period Cumulative ADM Collection. Demographic data are used to populate the School and District Profile sections of the School and District Report Cards.
4-Year Cohort Graduation Rate	The four-year cohort graduation rate is the percentage of students in a cohort, adjusted for transfers into and out of the school, district, or state, that graduate with a standard high school diploma within four years of entering high school. A cohort is composed of students who first started high school in a given school year.
5-Year Cohort Graduation Rate	The five-year cohort graduation rate is the percentage of students in a cohort, adjusted for transfers into and out of the school, district, or state, that graduate with a standard high school diploma within five years of entering high school. A cohort is composed of students who first started high school in a given school year.
Annual Measurable Achievement Objectives	The Annual Measurable Achievement Objectives (AMAO) report is comprised of three categories: 1) AMAO 1: Percentage of students on track to attain English language as measured by number and percent of students with individual growth percentiles equal to or greater than their individual growth target. 2) AMAO 2: Percentage of students attaining academic English proficiency. AMAO 2A: fewer than 5 years identified as English learner, AMAO 2B: 5 or more years identified as an English learner. 3) AMAO 3 the AMO for the LEP subgroup as defined in the ESEA waiver – growth model. Districts and School level data is provided to assist Districts with program evaluation and improvement.

Application Name	Description
Class Size	Beginning in 2014-15, the Oregon Department of Education began producing and reporting class size data for all subjects. A summary of the Class Size data will appear on school and district report cards (http://www.oregon.gov/ode/reports-and-data/Pages/Class-Size-Report.aspx) will be available on the website.
CTE 90% Met Report Combined	The Oregon Department of Education produces yearly Career and Technical (CTE) 90% Met Reports based on performance measures.
CTE 90% Met Report District School	The Oregon Department of Education produces yearly Career and Technical (CTE) 90% Met Reports based on performance measures.
English Language Arts Student Performance	RC Summary tab shows counts and percents that will be used for the Achievement, Growth, and Participation Indicators on the Report Card Rating Details Report.
Essential Skills	The Essential Skills validation reports on the essential skills codes submitted for the 0809 cohort five-year graduation rate and the 0910 cohort four-year graduation rate.
Expulsions & Suspensions	Suspensions and expulsions are collected through the Discipline Incidents Collection.
Fall Membership	Fall Membership is the list of students attending in your district on the first school day in October, as submitted in the first period Cumulative ADM collection.
Freshman On-Track Validation	Freshman On-Track, the percentage of students in their first year of high school who have earned at least 25% of the number of credits required for a high school diploma. This is a minimum of 6 credits, but may be higher in districts that require more credits for a diploma than the state's minimum.
Highly Qualified Teachers	The Classes Taught by Highly Qualified Teachers is the portion of the State report card for which Teacher Quality Data is reported.
Institutions for Accountability Reporting	This validation displays a list of institutions, along with several fields that are used in report card calculations.
Math Student Performance	Statewide mathematics assessment data

Application Name	Description
Mathematics Student Performance	RC Summary tab shows counts and percents that will be used for the Achievement and Growth Indicators and Participation details on the Rating Details Report. Detail tab includes all students reported as resident and enrolled in your district/school on the first school day in May.
NCES Dropout and Graduation Rates	The NCES rate is a measure of the number of students who dropped out or earned a credential in a single school year, as reported in the Cumulative ADM Collection.
Not Chronically Absent	The inverse of chronic absenteeism, the percent of students who are not chronically absent is a measure of the number of students who were present for more than 90% of the days they were enrolled. It will be used to populate the School and District Profile sections of the School and District Report Cards, and to produce the annual Chronic Absenteeism Report.
Perkins Career and Technical Education	New Validation for the CTE 90% Reports
Reading Student Performance	Statewide Reading Assessment data
Report Card	This validation provides districts and schools with an opportunity to preview the Report Card summary and the Report Card Rating Details report.
Report Card Narrative Collection	This collection gathers narrative information from schools and districts for the At-A-Glance report. Including information about school and district goals, school environment, and opportunities for student and parent engagement.
Science Student Performance	RC Summary tab shows counts and percents that will be used on school and district At-A-Glance reports.
Special Education Report Card	The Oregon Department of Education produces yearly special education report cards for EI/ESCSE and school age programs/districts providing special education services.
Spring Membership	Data report for spring membership data
Staff Ethnicity	This validation includes ethnicity and grade level data for teachers, principals, and certain other school-based staff members, for the purpose of populating the District Profile on district report cards.

Application Name	Description
Staff FTE	Staff are reported by full-time equivalency (FTE) which refers to the proportion of a full day that the staff member works. The actual number of hours or classes that a person must work to be full time varies by their employer. FTE data will be used in a report to the federal Department of Education.
Student Attendance	The attendance rate is the average percentage of enrolled students attending school each day.
Student Mobility	The mobility rate is the percentage of students who attended an institution in a given year who enrolled late, left early, transferred schools, or had a significant gap in enrollment at any point during the school year.
Teacher Qualifications	Validation for teacher experience and licensure
Unsafe Schools	Watch List School criteria depends on school size (from the Fall Membership collection) and the count of Expulsions due to weapons possession and/or violent criminal offenses, including: arson, battery, homicide, kidnapping, robbery, school threat, sexual battery, and other violent criminal offenses.
Writing Student Performance	Summary data include students reported as resident and enrolled in your district/school on the first school day in May. This data will be used for the Achievement, Growth, and Participation Indicators in the report card rating system.
Kindergarten Assessment Validation	The Kindergarten Assessment for 2017-2018 includes the following three segments: Approaches to Learning, Early Mathematics, and Early Literacy.
Public Applications	Applications available to the general public - these require no login/password
Web Security	ODE Extract Central Login application
Staff Search	ODE public staff lookup application
Central Login	Application used by districts to access the ODE secure web sites
Free Reduced Lunch	Free Reduce Lunch Application use by customers to application for Free school food for students
District Site Home Page	District Site Home Page or ODE Extranet Site Home Page
Institution Lookup	Web site used by public to lookup institution related information
Public Report Card	Public Report Card distribution application

Application Name	Description
Info Application - Schedule of Due Dates, Public Report, Secure Report, Data Collection Dtls	Info Application - Schedule of Due Dates, Public Report, Secure Report, Data Collection Dtls.
Secure File Transfers	Application used to secure transfer files. Used by District and customers to secure send files to ODE employees
Special Education Report Card	Application developed to do Special Education Report Card maintenance and production.
CACFP Reimbursement Calculator	CACFP Reimbursement Calculator
ODE Collections Catalog	The searchable ODE Collections Catalog is a publicly-accessible tool that will enable users in the field to find information about ODE's data collections, such as which ones contain data relevant to their research interests, or which ones they are required to submit data to.

Oregon
Kate Brown, Governor

OREGON DEPARTMENT OF EDUCATION
Oregon achieves . . . together!

Colt Gill
Director of the Department of Education

November 2, 2021

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 Opportunities Exist to Improve Web Application Security and Tracking of Website Accessibility Remediation Efforts.

The Oregon Department of Education (ODE) appreciates the time and effort the SoS Audit Division took to evaluate and understand ODE's web application and network security standards and practices as well as our commitment to both security and accessibility of our public-facing applications and online presence.

With all audits, this has been an opportunity to learn and evaluate our goals and priorities. The ODE is committed to providing a secure and accessible environment for all our customers, partners and employees. The Application Development, Enterprise and Network teams have focused and prioritized security efforts over the past several years and this audit has afforded us the opportunity to take pride in the work we have completed, while understanding those areas of needed growth.

The ODE has invested substantial resources to provide an accessible online experience for our employees, community partners, school districts, education service districts, and the public and is proud of the initial work completed and our continued commitment and effort of our agency.

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

RECOMMENDATION 1
Document and implement code review processes to ensure that only approved changes are made during application development.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	March 31, 2022	Sandee Hawkins Sandee.Hawkins@state.or.us

Narrative for Recommendation 1

The ODE agrees to further document the process for code review prior to deploying code changes to the production environment. This documentation will include updates to the SDLC and development work-flow documentation as well as core processes.

RECOMMENDATION 2

Ensure all web applications are scanned at least annually. Where barriers exist to the annual performance of application vulnerability scans, document a plan of action to address those barriers so scans can be performed.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	January 21, 2022	Sandee Hawkins Sandee.Hawkins@state.or.us

Narrative for Recommendation 2

The ODE scans web applications in the TEST environment using Acunetix. The scan tool requires that the application be open before the scan can be executed. The ODE has resolved the issue with the individual application in question. The aforementioned application will be scanned each January moving forward.

RECOMMENDATION 3

Work with CSS to determine if it is appropriate to extend the allowable time for user inactivity before disabling Central Login accounts. If both parties agree to an extended inactive period, document the deviation, and indicate the compensating controls put in place. In alignment with statewide standards, ensure the documentation is signed by the ODE director and approved by EIS.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	November 1, 2022	Sandee Hawkins Sandee.Hawkins@state.or.us

Narrative for Recommendation 3

The ODE has submitted a deviation from the 2019 Statewide Information and Cybersecurity Standard section AC-2(3) Account Management (pages 4-5) where it states that agencies are to automatically disable system accounts when the account has been inactive for 60 days. Our current system setting is for 24 months and the ODE is asking to update this to 13 months to assure our district and ESD partners are not adversely burdened. Upon submission of this form on 10/28/21 we were informed that CSS does not require this type of exception recorded for Secretary of State Audits and that ODE should record this information internally only. We have complied with CSS' recommendation and will begin updating our system to reflect the deviation from standard to be 13 months.

RECOMMENDATION 4 Document baseline configurations for all network devices. Review and update baseline configurations periodically, as defined by Statewide Information and Cyber Security Standards. Ensure subsequent changes are managed in accordance with statewide standards.		
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	Harris Geddes Harris.Geddes@state.or.us

Narrative for Recommendation 4

The ODE is working to establish baseline configurations with assistance from Cybersecurity Services (CSS).

RECOMMENDATION 5 Develop a risk-rating process to prioritize the remediation of vulnerabilities discovered in network scans and compare the results of back-to-back scans to verify vulnerabilities have been remediated in a timely manner.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	December 2021	Harris Geddes Harris.Geddes@state.or.us

Narrative for Recommendation 5

The ODE Network team has created a SmartSheet to track vulnerabilities discovered in network scans, the recommendations, and the results of follow-up scans to ensure vulnerabilities have been remediated. Tickets are created as part of the patching process to track server vulnerabilities that have been remediated.

RECOMMENDATION 6 Periodically review anti-malware software to ensure each of the agency's servers remain protected.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	March 2022	Harris Geddes Harris.Geddes@state.or.us

Narrative for Recommendation 6

ODE plans to create and maintain a policy and process to review anti-malware software is installed and updated on agency servers on a semi-annual basis. Working with CSS and the DART engagement to install Microsoft Defender Advanced Threat Protection on all servers, which monitors all systems for malware attacks.

RECOMMENDATION 7 Document authorization for all privileged access users. Review privileged access accounts at least semi-annually for continued appropriateness, including service accounts with elevated privileges.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	December 2023	Harris Geddes Harris.Geddes@state.or.us

Narrative for Recommendation 7

All privileged users will review and agree to acceptable use policy before being granted privileged access accounts. Privileged access accounts will be reviewed quarterly to ensure they are up-to-date. Permissions will be modified based on the required level of access. Track quarterly review of permissions in Smartsheet.

RECOMMENDATION 8 Implement multifactor authentication at the system level for access to privileged accounts.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	December 2023	Harris Geddes Harris.Geddes@state.or.us

Narrative for Recommendation 8
ODE will research and implement Multifactor Authentication for all privileged accounts and access to all restricted systems.

RECOMMENDATION 9 Implement recommendations associated with separately communicated confidential findings.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	July 2023	Peter Tamayo Peter.Tamayo@state.or.us

Narrative for Recommendation 9
See confidential narrative responses

RECOMMENDATION 10 Develop a documented plan of action and milestones to correct weaknesses identified in this audit, as well as outstanding deficiencies identified in other audits and assessments.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	November 30, 2021	Peter Tamayo Peter.Tamayo@state.or.us

Narrative for Recommendation 10
The ODE Director Team and CIO have created a secured environment to track all audit findings, both past and present, that allows for documentation, assignment of responsible staff, timeline for completion and notification through a Smartsheet.gov environment. This will allow the team visibility into what is in process, what is complete, and creates an environment that is easily accessible and transferable to incoming leadership and staff.

RECOMMENDATION 11 Ensure policies and procedures governing web application and network security are documented and up to date.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	January 1, 2023	Peter Tamayo Peter.Tamayo@state.or.us

Narrative for Recommendation 11

The ODE is working through the policy process established in 2020 to update and document changes to existing policies and write new policies where current do not exist. This process requires approval by the ODE Executive Team, as well as communication and implementation plans be established and documented. Based on current knowledge of the timeline constraints associated with this new process, the ODE IT leaders concluded that this will take until January of 2023 to complete.

RECOMMENDATION 12 Provide role-based, security-related training for software developers, privileged access users, data owners approving access to agency systems, and district security administrators.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	March 2023	Peter Tamayo Peter.Tamayo@state.or.us

Narrative for Recommendation 12

The ODE IT leadership team is working with the ODE Data Governance Committee, individual IT teams and human resources to update and deploy new required security training. The Director of Application Development and the Director of Enterprise Services have established budgetary plans for purchasing outside training for development and architect staff that will include security related topics. The development team currently uses OWASP and other security groups for knowledge and best practices.

RECOMMENDATION 13 Update policies and procedures governing website accessibility, including processes to incorporate feedback from members of the disability community, to ensure they reflect current program objectives and address key roles and responsibilities.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	October 2022	Melissa Garner melissa.garner@ode.oregon.gov

Narrative for Recommendation 13

Work has already begun on updating the accessibility policy and creating the accompanying procedure. Portions of the existing policy will be updated to the new format used by ODE, though the essential content will not change.

The procedure will include topics covered in this audit including engaging communities who use the accessibility features of our website. It will also include accessibility procedures for files, web pages, and applications.

Given the current extended time for policy to be approved, we anticipate this work will be completed in approximately one year, though the documents will be completed before then.

RECOMMENDATION 14 Periodically review website remediation tracking to ensure documentation is complete and effective in achieving the agency's objectives related to website accessibility remediation.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	Quarterly scheduled event starting December 2021	Melissa Garner melissa.garner@ode.orgon.gov

Narrative for Recommendation 14

Using the website accessibility tracking spreadsheet, both the Director of IT Governance, Policy & Strategy and the Webmaster will check recently remediated webpages on a no-less-than quarterly basis. This will constitute part of the quarterly employee review of the Web Accessibility Tech employee.

In the past, we did a full page by page remediation of every page we have... at least one revolution of our complete site - and that entire effort included oversight from an external auditor. Our current process includes remediation for every page change. The Web Accessibility Tech and Webmaster regularly meet to go over issues to help train for prevention; common problems are presented to Web Editors.

Please contact Peter Tamayo at 503.559.3718 or Peter.Tamayo@state.or.us with any questions.

Sincerely,

Colt Gill
Director of the Oregon Department of Education, and
Deputy Superintendent of Public Instruction

cc:
Peter Tamayo, ODE CIO
Sandee Hawkins, Director of Application Development

OREGON SOS

Secretary of State
Shemia Fagan

OREGON AUDITS DIVISION

Audits Director
Kip Memmott

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
audits.sos@oregon.gov
sos.oregon.gov/audits