PERFORMANCE AUDIT

Office of the Washington State Auditor
Pat McCarthy

Continuing Opportunities to Improve State Information Technology Security – 2020

December 24, 2020

Report Number: 1027593

Table of Contents

State Auditor's Office contacts

State Auditor Pat McCarthy
564-999-0801, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance and IT Audit
564-999-0809, Scott.Frank@sao.wa.gov

Peg Bodin, CISA – Assistant Director of IT Audit
564-999-0965, Peggy.Bodin@sao.wa.gov

Erin Laska – IT Security Audit Manager
564-999-0970, Erin.Laska@sao.wa.gov

Joseph Clark, CISA – IT Security Assistant Audit Manager
564-999-0968, Joseph.Clark@sao.wa.gov

Clyde Meador, CISA, SSCP – IT Auditor
564-999-0971, Clyde.Meador@sao.wa.gov

Robert Pratt – IT Auditor
564-999-0956, Robert.Pratt@sao.wa.gov

Kathleen Cooper – Director of Communications
564-999-0800, Kathleen.Cooper@sao.wa.gov

To request public records

Public Records Officer
564-999-0918, PublicRecords@sao.wa.gov

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email *Webmaster@sao.wa.gov* for more information.

Background

Critical state services depend on IT systems which must be protected to avoid service disruptions and financial losses

Washington state agencies depend on information technology (IT) systems to deliver an array of critical functions, such as public safety, tax collection, social services and transportation systems. The security of state agency IT systems and related data underpins the stability of government operations, and the safety and well-being of the state and its residents. The public expects state agencies to protect these systems from IT security incidents that could disrupt government services. Therefore, protecting these systems is paramount to public confidence in government.

These IT systems also process and store vast amounts of confidential data, from Social Security numbers and federal tax information to health care and criminal records. People are often required to share personal information with government agencies, especially if they wish to participate in government programs or receive services. Aside from the loss of public confidence, a data breach involving this information can cause governments to face considerable tangible costs, including those associated with identifying and repairing damaged systems, notifying and helping victims, and paying fines.

IT security incident – Any unplanned or suspected event that could pose a threat to the confidentiality, integrity, or availability of information assets.

Data breach – An IT security incident that results in the confirmed disclosure of confidential information to an unauthorized party.

Agency IT systems and data are attractive targets for cyberattacks

Government IT systems present a particularly tempting target to cyber criminals. Some attackers may attempt to steal and sell sensitive information for financial gain. Others may employ ransomware, which essentially renders IT systems and data unavailable until the attackers unlock it, extorting victims into paying the ransom by threatening to destroy or leak stolen sensitive information. Attacked governments are often placed in the difficult position of either failing to fulfill their obligations to residents or paying an expensive ransom to the attackers.

Government organizations across the United States and around the world have been and continue to be critically affected by cybercrime. In addition to harming governments' ability to access their data and carry out operations, hackers have managed to disable telephone systems, email, water utility pumps, emergency

dispatch centers, online tax and utility payment systems, and the ability to open jail cell doors remotely. According to a study by Emsisoft, at least 113 state and local governments in the United States were affected by ransomware in 2019 alone. When combined with ransomware attacks on healthcare and education organizations, the study estimated that the total cost of these attacks in 2019 may have exceeded $7.5 billion. School districts nationwide have continued to be targeted in 2020, resulting in increased disruption for students who are already adapting to remote learning due to COVID-19.

Washington has also been targeted by cyberattacks. Since 2016, nine state or local governments have reported data breaches to the state Office of the Attorney General as a result of a cyberattack, and many have reported cyber-related incidents, including frauds, to the State Auditor. As recently as September 2020, Washington state agencies were attacked by a coordinated phishing campaign.

This audit looked for opportunities for state agencies to improve their IT security

To help state agencies protect their mission-critical IT systems and secure the data they need to operate, we conducted a performance audit designed to identify opportunities to improve IT security. This audit included a total of five state agencies. Of the five, one is a large, three are medium-sized, and one is a small state agency. The audit answered the following question:

- Can selected agencies make their IT systems more secure, and better align their IT security practices with leading practices?

Next steps

Our performance audits of state programs and services are reviewed by the Joint Legislative Audit and Review Committee (JLARC) and/or by other legislative committees whose members wish to consider findings and recommendations on specific topics. Representatives of the Office of the State Auditor will review this audit with JLARC's Initiative 900 Subcommittee in Olympia. The public will have the opportunity to comment at this hearing. Please check the JLARC website for the exact date, time, and location (www.leg.wa.gov/JLARC). The Office conducts periodic follow-up evaluations to assess the status of recommendations and may conduct follow-up audits at its discretion. See **Appendix A**, which addresses the I-900 areas covered in the audit. **Appendix B** contains information about our methodology.

Audit Results

Can selected agencies make their IT systems more secure, and better align their IT security practices with leading practices?

Answer in brief

While agencies in this audit have taken steps to secure their IT systems, our technical testing identified vulnerabilities which agencies can address to improve security. State agencies can also strengthen their IT security posture and meet state standards by aligning IT security programs with leading practices, such as the *CIS Controls* published by the Center for Internet Security. The agencies in this audit have aligned parts of their IT security programs with the *CIS Controls* we examined. However, these agencies can better protect their IT systems by further aligning their IT security programs with the *CIS Controls*. Finally, agencies cited resource availability as a notable factor in implementing IT security controls.

While agencies have taken steps to secure their systems, our technical testing identified vulnerabilities which can be addressed to improve security

We conducted technical testing at all five agencies and found controls in place to secure agency IT systems. However, we also identified opportunities to better protect those systems. Tests consisted of a vulnerability assessment and a partial review of administrative privileges – the methods in place to restrict users to only those portions of software or networks necessary for their work.

These tests indicated that all five agencies had ongoing patch management in place to keep systems up to date and protect against known vulnerabilities. Agencies also used privilege-management practices to restrict administrative accounts to only authorized staff. These restrictions are essential to minimize the effect of a cyberattack because hackers with access to administrator-level IT functions can easily advance their attacks, such as by installing ransomware. Although our results indicated the agencies had generally implemented these controls, our testing did identify some issues. We gave the results of our assessments to each agency so it could address issues as it determined appropriate.

We also conducted penetration testing on selected networks and applications at one agency. We had planned to conduct penetration testing at all five agencies, but we were unable to do so at the remaining four agencies due to the COVID-19 pandemic. We now plan to conduct additional testing at most of these agencies in 2021. The penetration testing examined both external and internal perspectives, replicating the types of attacks that both hackers on the internet and insiders could make. Our technical testing almost always identifies some vulnerabilities in IT systems. Agency IT environments are complex and regularly changing, and new weaknesses in software and methods of attack can be discovered at any time. As expected, this audit's testing uncovered issues that the agency can address to improve its IT security.

We briefed the agency daily during our penetration testing, and gave detailed results to the agency and to the Office of Cybersecurity after testing was completed. Agency managers reported addressing significant vulnerabilities immediately and said they are continuing to make improvements.

State agencies can also strengthen their IT security posture and meet state standards by aligning IT security programs with leading practices

State agencies are required to comply with state IT security standards published by the Office of the Chief Information Officer (OCIO) in OCIO 141.10: Securing Information Technology Assets Standards. These standards offer agencies a framework for an IT security program, and require them to document and implement appropriate security practices. However, agencies are also required to assess their own risk environment and then select specific security practices to put in place based on their individual needs. Agencies can use leading practices to identify those specific IT security practices.

The Center for Internet Security publishes detailed guidance as the *CIS Controls*

One resource state agencies can turn to for help complying with state standards and enhancing their security posture is the detailed list of IT security controls published by the Center for Internet Security (CIS). CIS works with a community of public- and private-sector partners that have a wide portfolio of cybersecurity expertise. This group assembles a list of practices that can help organizations reduce the likelihood and severity of a successful cyberattack. CIS regularly updates the list based on an ongoing analysis of real-world attack data.

The prioritized list, published as the *CIS Controls*, describes 20 broad topics of IT security practices. Depending on each agency's existing control activities, we selected four control areas from the following list of *CIS Controls* to evaluate at each of the five state agencies in this audit:

- Control 1: Inventory and control of hardware assets
- Control 2: Inventory and control of software assets
- Control 3: Continuous vulnerability management
- Control 4: Controlled use of administrative privileges
- Control 5: Secure configuration for hardware and software on mobile devices, laptops, workstations and servers
- Control 6: Maintenance, monitoring and analysis of audit logs
- Control 11: Secure configuration for network devices, such as firewalls, routers and switches

We selected from among these controls for our assessments because, although they are not an absolute safeguard against cyberattacks, CIS sees the first six controls as "the basic things that [organizations] must do to create a strong foundation for [their] defense." We also considered Control 11 in our assessments because it is closely related to Control 5.

Each control is expanded into detailed sub-controls: practices that, together, support the goal of the control. **Appendix C** contains the full list of sub-controls for each of the *CIS Controls* considered in this audit.

Agencies in this audit have aligned parts of their IT security programs with the *CIS Controls* we examined

This audit assessed the extent to which agencies' IT security programs, including their implementation and documentation, aligned with the selected *CIS Controls* and the supporting sub-controls.

All programs, particularly in their technical implementation, partially or fully aligned with several sub-controls of the *CIS Controls* we tested. Although the degree of alignment varied by agency, all five have already applied elements of the selected *CIS Controls* that enhanced their IT security posture. For example, some agencies had robust vulnerability management programs, while others focused their efforts on asset management; one agency strengthened its systems using security assessments conducted by third-party vendors. Additionally, two agencies leveraged extensive technical solutions in ways that addressed multiple CIS sub-controls.

These agencies can better protect their IT systems by further aligning their IT security programs with the *CIS Controls*

This audit identified opportunities for agencies to improve their IT security by further aligning with the *CIS Controls*. For instance, the *CIS Controls* require keeping IT systems up to date to address newly discovered vulnerabilities. Although all five agencies had patch management processes, we noted two did not have vulnerability scanners. Regular vulnerability scanning provides assurance that systems are patched as necessary to protect systems from known vulnerabilities. This is especially important when the agency makes changes to hardware or software. Software that has not been properly patched leaves gaps that allow an attacker to compromise agency systems with much less effort.

The audit also found agencies can improve the documentation of the practices they have in place that already align with the *CIS Controls*. Documenting IT security practices through policies and procedures is important because it helps an organization set priorities for IT security activities and gives staff authority to act on approved practices. Documentation can also provide an accountability mechanism in case practices are not implemented as required. Additionally, documentation preserves institutional knowledge of the practices that are already in place, helping ensure those practices are maintained over time. Finally, documentation is important in organizations where IT responsibilities are decentralized, because written policies and procedures can effectively define how different business units with IT responsibilities will communicate and coordinate with each other to ensure the organization's overall IT security.

Issues around documentation noted during this audit are not unique to these agencies. All five of our previous state IT security audits, covering 18 more agencies, included a similar observation.

Agencies cited resource availability as a notable factor in implementing IT security controls

All five agencies said resource availability, particularly qualified staff, was a significant factor in implementing cybersecurity initiatives. Of the five agencies, four said employing or retaining sufficient staff was a challenge. However, one of those four agencies, which aligned well with the *CIS Controls*, attributed its success to the attention and skillsets that each staff member brought to the agency despite it having few IT staff. Additionally, the fifth agency, which also aligned particularly well with the *CIS Controls*, attributed its performance to its focus on attracting key IT security staff. This agency described its staff recruitment efforts as part of a deliberate IT security initiative that also included investing in new security tools.

State Auditor's Conclusions

As we have noted in previous cybersecurity audits over the past few years, protecting the state from the evolving landscape of cyber threats requires a significant investment by state agencies. This includes both technological tools that help protect the state's systems and the staff who operate those tools. These needs have become more pronounced as state agencies continue to deal with the ongoing COVID-19 pandemic. So many agencies have had to quickly adjust their operations to support extensive teleworking, stretching their IT staff to capacity and making agencies more vulnerable to cyberattacks. These circumstances make it especially important for state agencies to have strong security programs in place.

Recommendations

For the five selected agencies

To help strengthen IT security programs, and to protect agency systems and the information within those systems, we recommend the agencies:

1. Further align agency IT security programs with leading practices recommended in the *CIS Controls*
2. Identify and continue to periodically assess the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security
3. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them

Agency Response

JAY INSLEE
Governor

JAMES WEAVER
Director &
State Chief Information Officer

STATE OF WASHINGTON
WASHINGTON TECHNOLOGY SOLUTIONS
Washington's Consolidated Technology Services Agency
1500 Jefferson Street SE ▪ Olympia, Washington 98504-1501

December 22, 2020

The Honorable Pat McCarthy
Washington State Auditor
P.O. Box 40021
Olympia, WA 98504-0021

Dear Auditor McCarthy:

On behalf of the audited entities, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report "Continuing Opportunities to Improve State IT Security – 2020."

We agree that the security of IT systems and data underpins the stability of government operations, and the safety and well-being of the state and its residents. Protecting these systems is of paramount interest to all of us and a responsibility of every state organization.

We value the commitment from your office to help improve the state's security posture. Cyber threats continue to evolve rapidly and we all must continually strengthen protections of our systems and data. We appreciate the efforts of your team in helping us do so.

We also appreciate the SAO's recognition of the steps the audited entities have already taken to protect systems and data. Please thank your team for their collaborative approach throughout this performance audit.

We continue to welcome the SAO's observations and recommendations of what to improve.

Sincerely,

James Weaver
Director & State Chief Information Officer

Enclosure

cc: Jamila Thomas, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Keith Phillips, Director of Policy, Office of the Governor
David Schumacher, Director, Office of Financial Management
Christine Bezanson, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
Vinod Brahmapuram, State Chief Information Security Officer, Washington Technology Solutions
Scott Bream, State Information Security Policy Officer, Washington Technology Solutions
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor

Official Response to the Performance Audit on Continuing Opportunities to Improve State IT Security – 2020 Dec. 22, 2020

This management response to the State Auditor's Office (SAO) performance audit report received December 2, 2020, is coordinated by the State's Chief Information Officer on behalf of the audited entities.

SAO Performance Audit Objectives:

The SAO sought to answer this question:

1. Can selected agencies make their IT systems more secure, and better align their IT security practices with leading practices?

SAO Recommendations to the five selected state agencies: to help strengthen IT security programs, and to protect agency systems and the information within those systems, we recommend:

1. Further align agency IT security programs with leading practices recommended in the Center for Internet Security "CIS" Controls.
2. Identify and continue to periodically assess the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.
3. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them.

STATE RESPONSE:
We agree with the opportunities for improvement identified by the SAO to help strengthen IT security and are committed to ongoing assessment and improvement. The state recognizes the importance of continuously improving security and takes that charge seriously. The organizations audited have already made improvements and continue to work carefully through the findings and recommendations. Consideration will also be given to further aligning IT security programs with the leading practices recommended in the CIS Controls. These controls are more prescriptive than the OCIO IT security standards 141.10 that agencies are required to follow. The OCIO will use the findings and observations of this and previous audits to work with all state organizations to improve the state's security posture.

Action Steps and Time Frame

- Each audited entity will work with the appropriate governing bodies to address vulnerabilities, improvements and considerations suggested by the SAO during calendar year 2021.

Appendix A: Initiative 900 and Auditing Standards

Initiative 900 requirements

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Results and Recommendations sections of this report.

I-900 element	Addressed in the audit
1. Identify cost savings	**No.** The audit did not identify measurable cost savings. However, strengthening IT security could help agencies avoid or mitigate costs associated with an IT security incident or data breach.
2. Identify services that can be reduced or eliminated	**No.** The audit did not address services that could be reduced or eliminated.
3. Identify programs or services that can be transferred to the private sector	**No.** While state agencies can outsource some IT services to the private sector, state law and IT security policy do not allow them to outsource responsibility for protecting their IT environments and the data in those environments.
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**No.** The audit did not identify gaps or overlaps related to programs or services.
5. Assess feasibility of pooling information technology systems within the department	**No.** The audit did not assess the feasibility of pooling information systems; it focused on select agencies' IT security postures.

I-900 element	Addressed in the audit
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** The audit recommended each audited agency periodically assess its own IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit did not recommend statutory or regulatory changes.
8. Analyze departmental performance data, performance measures and self-assessment systems	**Yes.** Although the audit did not review indicators of each agency's performance of its core mission, it did review certain controls that provide metrics on how each agency's security program is performing.
9. Identify relevant best practices	**Yes.** The audit identified and used leading practices maintained by the Center for Internet Security to assess select agencies' IT security programs.

Compliance with generally accepted government auditing standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with generally accepted government auditing standards as published in *Government Auditing Standards* (July 2018 revision) issued by the U.S. Government Accountability Office. 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.

The mission of the Office of the Washington State Auditor

To provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective. The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic subscription service. We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program. For more information about the State Auditor's Office, visit www.sao.wa.gov.

Appendix B: Scope, Objectives and Methodology

Scope

This audit included a total of five state agencies. Of the five, one is a large, three are medium-sized, and one is a small state agency.

The audit used vulnerability scanning and a partial review of administrative privileges at each agency to assess what each could do to make IT systems more secure. The audit also conducted penetration testing at one agency. We planned to conduct penetration testing at all five, but were unable to do so due to the COVID-19 pandemic; we plan to conduct penetration testing at most of the remaining agencies in 2021.

This audit also assessed the extent to which the five agencies' IT security programs, including their implementation and documentation, aligned with four of the seven *CIS Controls* listed below and the supporting sub-controls. This audit did not assess agencies' alignment with federal laws or requirements or agencies' compliance with Washington state's IT security standards, published by the Office of the Chief Information Officer (OCIO) in *OCIO 141.10: Securing Information Technology Assets Standards*.

Objectives

To help state agencies protect their mission-critical IT systems and secure the data they need to operate, we conducted a performance audit designed to identify opportunities to improve IT security.

The audit answers the following question:

- Can selected agencies make their IT systems more secure, and better align their IT security practices with leading practices?

Methodology

To answer the audit objective, we conducted technical testing at all five agencies, including penetration testing of one agency's select internal and external applications and underlying networks. We also compared the five agencies' IT security programs to selected leading practices.

Selecting state agencies for testing

We selected five state agencies that store confidential information and provide critical government services to the people of Washington. After we selected the agencies, we consulted with the state's Chief Information Security Officer at the Washington Technology Solutions (WaTech) Office of Cybersecurity (OCS) to ensure a coordinated approach to audit work and to reduce the effect of our testing on agency operations.

Technical testing, including penetration testing

To determine whether there are opportunities for agencies to improve the security of their IT systems and the confidential information maintained in those systems, we conducted vulnerability scanning and a partial review of administrative privileges at all five agencies. We completed this work between March and September 2020.

We also conducted external and internal penetration testing at one agency. We conducted external and internal penetration testing of the agency's key applications, systems and their underlying networks. We completed this work between March and April 2020. This included identifying and assessing vulnerabilities and determining whether they could be exploited.

With the involvement of the agency's IT staff, and in consultation with OCS, we selected several applications for the external and internal testing. Applications were selected for testing based on several factors, including their criticality to the agency's mission and the sensitivity of the data within those applications. In addition to testing applications available only to agency employees on internal networks, we also tested applications available to the public online because agencies offer many of their services through the internet. External testing requires coordination with OCS, because the state's managed security perimeter is designed to block external scanning of assets within that security perimeter.

Comparing state agencies' IT security programs to leading practices

To determine whether agency IT security practices align with leading practices, we interviewed key agency IT staff, reviewed agencies' IT security policies and procedures, observed agency practices and security settings, and conducted vulnerability scanning and a partial review of administrative privileges as discussed above. We performed this work for each agency at its offices and remotely between January and September 2020, with some additional follow-up afterwards.

We used selected *CIS Controls, version 7.1*, as our criteria to assess agencies' IT security programs and to identify areas that could be made stronger.

The Center for Internet Security is a nonprofit organization focused on safeguarding public and private organizations against cyber threats. Its *CIS Controls* are a prioritized set of leading practices for cyber defense created to stop the most pervasive and dangerous attacks, are informed by analysis of real-world attack data, and are developed and vetted across a broad community of government and industry practitioners. Contributors to the *CIS Controls* have included the U.S. Department of Defense, the National Security Agency, the U.S. Department of Energy national energy labs, law enforcement organizations, Verizon, HP and Symantec.

Because the *CIS Controls* are prioritized, we selected from the top six controls because, although they are not an absolute safeguard against cyberattacks, the Center for Internet Security sees these as "the basic things that you must do to create a strong foundation for your defense." We also considered Control 11 because, as does Control 5, it pertains to securely configuring devices in ways that could mitigate a cyberattack.

These *CIS Controls* represent the following areas:

- #1 – Inventory and control of hardware assets
- #2 – Inventory and control of software assets
- #3 – Continuous vulnerability management
- #4 – Controlled use of administrative privileges
- #5 – Secure configuration for hardware and software on mobile devices, laptops, workstations and servers
- #6 – Maintenance, monitoring, and analysis of audit logs
- #11 – Secure configuration for network devices, such as firewalls, routers and switches

Each control consists of a series of sub-controls, which are distinct and measurable tasks that, when implemented together, fully meet the requirements of the overall control. We assessed each agency against those sub-controls to determine its alignment with the overall controls. See Appendix C for a list of the sub-controls that were considered for this audit.

We reviewed each agency's alignment with the controls by assessing the extent to which the agency met each sub-control in three areas:

1. Implementing the sub-control
2. Automating or technically enforcing the sub-control, which minimizes the possibility of the sub-control failing due to human error or inconsistent processes
3. Maintaining documentation to support the sub-control, such as policies or procedures

We also assessed the extent to which each agency was reporting on the control overall. A higher score here indicates that agency IT management has been kept aware of certain key areas within that control.

Work on Internal Controls

This audit assessed the IT security internal controls at five state agencies. We used a selection of controls from the 20 *CIS Controls* as the internal control framework for the assessment. The first six are considered among the most important controls to put in place to protect an organization and Control 11 is closely related to Control 5. Based on scoping conversations at each of the five state agencies, we selected four from the top six controls and Control 11 to include in the scope. We completed our assessment for the purpose of identifying opportunities for the agencies to improve internal IT security controls. However, this assessment is not intended to provide assurance on the agencies' current IT security posture.

Reporting confidential or sensitive information

To protect the agencies' IT systems, and the confidential and sensitive information contained in those systems, this report does not include the agencies' names or the detailed descriptions of our results. This information is exempt from public disclosure in accordance with RCW 42.56.420(4).

We gave the five state agencies the detailed results of their respective assessments as we completed them, as well as detailed recommendations. We also gave all detailed results and recommendations to OCS.

Appendix C: List of CIS Sub-Controls

This audit included the following *CIS Controls* and their respective sub-controls. We have edited the text of some sub-controls for clarity and consistency.

Figure 1 – Control 1 sub-controls: Inventory and control of hardware assets

Sub-control	Activity
1.1	Use an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
1.2	Use 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 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 an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.
1.5	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	Ensure that unauthorized assets are either removed from the network, quarantined, or that the inventory is updated in a timely manner.
1.7	Use 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	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

Figure 2 – Control 2 sub-controls: Inventory and control of software assets

Sub-control	Activity
2.1	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 that only software applications or operating systems which are currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
2.3	Use software inventory tools throughout the organization to automate the documentation of all software on business systems.
2.4	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	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	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.
2.7	Use application allowlisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
2.8	The organization's application allowlisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.
2.9	The organization's application allowlisting software must ensure that only authorized, digitally signed scripts (such as *.ps1,*.py, macros, etc.) are allowed to run on a system.
2.10	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.

Figure 3 – Control 3 sub-controls: Continuous vulnerability management

Sub-control	Activity
3.1	Use an up-to-date Security Content Automation Protocol (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 with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
3.3	Use a dedicated account for authenticated vulnerability scans. The account should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
3.4	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 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	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
3.7	Use a risk-rating process to prioritize the remediation of discovered vulnerabilities.

Figure 4 – Control 4 sub-controls: Controlled use of administrative privileges

Sub-control	Activity
4.1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
4.2	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
4.3	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should be used only for administrative activities and not internet browsing, email, or similar activities.
4.4	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
4.5	Use multi-factor authentication and encrypted channels for all administrative account access.
4.6	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 email, composing documents, or browsing the internet.
4.7	Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.
4.8	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	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

Figure 5 – Control 5 sub-controls: Secure configuration for hardware and software on mobile devices, laptops, workstations and servers

Sub-control	Activity
5.1	Maintain documented security configuration standards for all authorized operating systems and software.
5.2	Maintain secure images or templates for all systems in the organization 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	Store the template images on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
5.4	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
5.5	Use a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

Figure 6 – Control 6 sub-controls: Maintenance, monitoring, and analysis of audit logs

Sub-control	Activity
6.1	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	Ensure that local logging has been enabled on all systems and networking devices.
6.3	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
6.4	Ensure that all systems which store logs have adequate storage space for the logs generated.
6.5	Ensure that appropriate logs are aggregated to a central log management system for analysis and review.
6.6	Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis.
6.7	On a regular basis, review logs to identify anomalies or abnormal events.
6.8	On a regular basis, tune the SIEM system to better identify actionable events and decrease event noise.

Figure 7 – Control 11 sub-controls: Secure configuration for network devices, such as firewalls, routers and switches

Sub-control	Activity
11.1	Maintain documented security configuration standards for all authorized network devices.
11.2	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, the name of the person responsible for that business need, and an expected duration of the need.
11.3	Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.
11.4	Install the latest stable version of any security related updates on all network devices.
11.5	Manage all network devices using multi-factor authentication and encrypted sessions.
11.6	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed internet access. This machine shall not be used for reading email, composing documents, or surfing the internet.
11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

"Our vision is to increase **trust** in government. We are the public's window into how tax money is spent."

– Pat McCarthy, State Auditor

Washington State Auditor's Office
P.O. Box 40031 Olympia WA 98504

www.sao.wa.gov

1-564-999-0950

Office of the Washington State Auditor