PERFORMANCE AUDIT

Office of the Washington State Auditor
Pat McCarthy

Continuing Opportunities to Improve State IT Security – 2019

January 28, 2020

Report Number: 1025655

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.gov

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

Rhianna Hruska – IT Auditor
564-999-0964, Rhianna.Hruska@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 Communications@sao.wa.gov for more information.

Background

Critical state services depend on IT systems with confidential information, 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. Therefore, protecting these systems is paramount to public confidence, because the public expects state agencies to protect these systems from IT security incidents that could disrupt government services.

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 jeopardize 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. In addition to selling stolen information for financial gain, attackers often target government systems with ransomware, essentially rendering IT systems and data unavailable until the attackers are paid. Because government IT systems support critical operations, attacked governments are often placed in the difficult position of either failing to deliver core services or paying an expensive ransom to the attackers.

Government organizations across the country and around the world have been critically affected by cyber crime. Since 2017, the United Kingdom's National Health Service, the cities of Atlanta and Baltimore, Garfield County in Utah, and 22 municipalities in Texas, to name a few, have been attacked with ransomware that crippled or disrupted their operations.

Washington governments have also been affected by cyberattacks. Since 2016, six government organizations have reported data breaches to the state Office of the Attorney General as a result of a cyberattack. Multiple state agencies and local governments have also reported cyber-related incidents, including frauds, to the State Auditor.

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 three large agencies and one small agency, one of which volunteered to participate. 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?

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 shared detailed results with each of the audited agencies and with the Office of CyberSecurity at Washington Technology Solutions (WaTech). The Governor's Office was also made aware of the four state agencies included in the audit.

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, including the tests performed and the Center for Internet Security's *CIS Controls*.

Audit Results

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

Answer in brief

The four agencies we audited have taken steps to address vulnerabilities we found and better protect their systems and data. Most 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*. We found the agencies in this audit have aligned parts of their IT security programs with the *CIS Controls* we examined. However, they can better protect their IT systems by further aligning their IT security programs with those *CIS Controls*. When asked about these results, the two agencies that most closely align with the *CIS Controls* cited strong executive support, greater resource availability, and higher IT staffing levels.

The agencies in this audit have taken steps to address vulnerabilities we found and better protect their systems and data

The first part of our audit work tested select networks and applications at four agencies to identify security gaps or vulnerabilities in their IT systems. We conducted this testing from both external and internal perspectives, replicating the types of attacks that hackers on the internet and insider threats could conduct. This type of security testing almost always identifies some vulnerabilities in IT systems. For example, agency IT environments are complex and regularly changing, and new weaknesses in software and methods of attack might be discovered at any time. As expected, this audit's testing uncovered issues that the agencies can address to improve their IT security.

We briefed the agencies weekly during testing, and gave full, detailed results to the agencies and to the Office of CyberSecurity after testing was completed. The agencies reported addressing significant vulnerabilities immediately and are continuing to make improvements.

Most 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*

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 provide the framework for an IT security program, and require agencies to document and implement security practices based on their individual needs. However, the standards require agencies to identify many of the specific IT security practices to put in place, depending on their risk. Agencies can use leading practices, such as the *CIS Controls*, 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. This audit selected eight topic areas to examine at all four agencies. They are:

- 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 7: Email and web browser protections
- Control 11: Secure configuration for network devices, such as firewalls, routers and switches

We selected controls 1 through 6 because, although they are not an absolute safeguard against cyberattacks, CIS sees these as "the basic things that [organizations] must do to create a strong foundation for [their] defense." Control 7 can provide some additional defense against phishing emails, which are a prevalent way of executing cyberattacks. We included Control 11 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* evaluated in this audit.

The 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 eight *CIS Controls* listed above and their supporting sub-controls.

The agency IT security 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 four have taken key steps to protect their IT systems and data maintained in those systems. For example, all four agencies have implemented vulnerability scanning to identify and manage vulnerabilities, and segmented high-risk assets to better protect them. Additionally, all four have identified benchmarks for configuring devices, and have automated mechanisms to alert on specific changes to those configurations.

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

The extent of an organization's vulnerabilities is a function of multiple factors including, for example, size and complexity of the IT environment and dependence on IT vendors. However, our internal and external security testing generally identified fewer higher-priority vulnerabilities for agencies that were more closely aligned with the *CIS Controls*. These results suggest that better alignment with the *CIS Controls* could reduce the significance of those issues.

This audit identified opportunities for agencies to improve their IT security by further aligning with the *CIS Controls*. For instance, the *CIS Controls* we examined include keeping IT systems up-to-date to address newly discovered vulnerabilities. We noted three agencies relied, in part, on aging IT equipment, a practice that does not align with the *CIS Controls*. While still functional, aging equipment is harder to secure because manufacturers eventually discontinue support for these products, including security updates. Although the agencies had practices in place to compensate for the age of the equipment, protecting older devices through those compensating practices creates more work for IT security staff.

Further aligning policies and procedures with the *CIS Controls* can also help agencies improve their IT security. For example, agencies can improve the documentation of the IT security practices they already have in place that 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 implement new IT security practices. Documentation also preserves institutional knowledge of the practices already in place, helping ensure those practices are maintained over time. Additionally, it can provide an accountability mechanism in case practices are not implemented as required. Documentation is also 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 four of our previous state IT security audits, covering 15 more agencies, included a similar observation.

Agencies that more closely align with leading practices cited strong executive support, greater resource availability, and higher IT staffing levels

Key IT staff at the two agencies that most closely aligned with the *CIS Controls* cited the investments leadership made in cybersecurity as a significant factor in their success. Staff said these investments – in both equipment and personnel – were backed by strong involvement in IT security issues by agency leadership. Among the examples of involvement staff described, they noted high awareness among executives about the potential ramifications of a security incident and a spirit of open and frequent communication between leadership and IT management, which contributed to a general culture of security awareness in the agency.

Conversely, staff at the agencies that were not as closely aligned with the *CIS Controls* emphasized a stronger need for additional resources, both equipment and staffing levels. They described the difficulties they had in getting those additional resources. Earlier state IT security audits have also noted agencies' concerns around insufficient resources, including staffing, to improve their overall IT security posture.

Our own analysis, using data from the Office of Financial Management, found agencies more closely aligned with the *CIS Controls* had more IT staff as a proportion of total agency staff. For example, one higher-performing agency had almost twice as many IT staff as a lower-performing agency, even though it was about half the size of the larger agency as measured by total staff count. Because IT security responsibilities often are shared among the IT staff in an organization, lower proportions of IT staff can seriously impair an agency's ability to implement beneficial IT security practices.

State Auditor's Conclusions

Executive management plays a key role in an agency's IT security program. In organizations with strong security programs, top management helps develop an environment that emphasizes the importance of security. Executives in these organizations set up structures to make sure they are aware of key security risks, and they incorporate this awareness into their decision making. Although resources are not infinite, top managers do their best to support the needs of their agencies' security functions. For some agencies, a solid step toward a higher level of awareness and risk management would be to elevate the security function in the organization's structure. All agencies should stay aware of the staffing and other resource needs of their security programs.

Recommendations

To the four selected state agencies:

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

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

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

January 23, 2019

Dear Auditor McCarthy:

On behalf of the audited agencies, 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 – 2019.

We appreciate the SAO's continued investment toward improving the state's IT security. The audited agencies have found immense value in these performance audits.

We agree that the security of state agency 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 us.

We appreciate the SAO's recognition of the improvements agencies have taken to better protect systems and data — and align their security program with some leading practices. We agree that there is opportunity to further strengthen our IT systems and have an ongoing commitment to do so. Strengthening the state's IT posture is a continuous responsibility of every state agency.

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

cc: David Postman, 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
Inger Brinck, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
John Cooper, Sr. Performance Project Manager, Results Washington, Office of the Governor
Vinod Brahmapuram, State Chief Information Security Officer, Washington Technology Solutions
Scott Bream, State Information Policy Officer, Washington Technology Solutions
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor

Official State Cabinet Agency Response to the Performance Audit on Continuing Opportunities to Improve State IT Security –Jan. 23, 2020

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

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

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

STATE RESPONSE:
Agencies embrace their responsibility to continuously improve State IT security. We agree with the opportunities for improvement identified by the SAO to strengthen IT security and are committed to ongoing assessment and improvement. The audited agencies have already made improvements and will continue to work diligently to address the findings. Agencies will also consider further aligning IT security programs with the leading practices recommended in the CIS Controls. To leverage leading practices, the Office of Cybersecurity will use the findings and observations of this audit to work with all state agencies to better improve the state's security posture.

Action Steps and Time Frame

- Each audited agency will establish a timeline to address vulnerabilities, improvements and considerations identified. *By March 31, 2020*.

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.** Because state law and IT security policy assign state agencies the responsibility of protecting their IT environments and the data in those environments, we did not assess this.
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit compares agencies' IT security programs against leading practices, and makes recommendations to align them.
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 evaluates the roles and functions of certain IT security areas at the agencies, and makes recommendations to better align them with leading practices.
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit does not recommend statutory or regulatory changes.
8. Analyze departmental performance data, performance measures and self-assessment systems	**Yes.** The audit examined and made recommendations to improve certain IT security programs at state agencies.
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 (December 2011 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

The audit assessed four state agencies' IT security through external and internal security testing at each agency. The testing focused on judgmentally selected applications and their underlying networks. The audit did not test all internal or all external applications and network ranges. Applications were selected for testing based on several factors, including, for example, criticality to each agency's mission and category of data.

This audit also assessed the extent to which agencies' IT security programs, including their implementation and documentation, aligned with the eight *CIS Controls* listed below and their supporting sub-controls. This audit did not assess 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. This audit tested the internal IT security controls in place at three large agencies and one small agency. One of the four total agencies volunteered.

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 of select internal and external applications and their underlying networks, and we compared the agencies' IT security programs to select leading practices.

Selecting state agencies for testing

We selected four state agencies – three large and one small agency – that store confidential information and provide critical government services to the people of Washington. One agency asked to be included

in this audit after being included in a previous IT security audit we performed. 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 and to reduce the impact of our testing on agency operations.

External and internal security 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 external and internal security testing of each agency's key applications, systems and their underlying networks. We completed this work between February and July 2019. This included identifying and assessing vulnerabilities and determining whether they could be exploited. To help ensure a real-world response to the external security testing, only agency executives and a few key staff knew about the testing in advance.

With the involvement of each agency's IT staff, and in consultation with OCS, we selected several mission-critical applications for the external and internal testing. Because agencies offer many of their services through the internet, the testing included applications available to the public online as well as applications available only to agency employees on their internal network. 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 limited technical analysis of agency systems. This work was completed at the four state agencies between April and September 2019, with some additional follow-up afterwards.

We used selected *CIS Controls*, version 7, 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 reviewed 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 reviewed CIS Control 7 because it can provide some additional defense against phishing emails, which have become a prevalent way of initiating cyberattacks. Additionally, we included CIS Control 11 because, as with CIS 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

#7 – Email and web browser protections

#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 their alignment with the overall controls. See Appendix C for a list of the sub-controls that were included in 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.

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 four state agencies the detailed results of their respective tests 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 controls and their respective sub-controls.

ID	Control 1 sub-controls: Inventory and control of hardware assets
1.1	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
1.3	Use 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 hardware 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 the inventory is updated in a timely manner.
1.7	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
1.8	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

ID	Control 2 sub-controls: Inventory and control of software assets
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 currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
2.3	Utilize software inventory tools 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	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
2.8	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.
2.9	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.
2.10	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.

ID	Control 3 sub-controls: Continuous vulnerability management
3.1	Utilize 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, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
3.4	Deploy automated 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 back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
3.7	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

ID	Control 4 sub-controls: Controlled use of administrative privileges
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 only be used 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.

ID	Control 5 sub-controls: Secure configuration for hardware and software on mobile devices, laptops, workstations and servers
5.1	Maintain documented, standard security configuration standards for all authorized operating systems and software.
5.2	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
5.3	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
5.4	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
5.5	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

ID	Control 6 sub-controls: Maintenance, monitoring and analysis of audit logs
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 that store logs have adequate storage space for the logs generated.
6.5	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
6.6	Deploy Security Information and Event Management (SIEM) or log analytic tool 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 your SIEM system to better identify actionable events and decrease event noise.

ID	Control 7 sub-controls: Email and web browser protections
7.1	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
7.2	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
7.3	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.
7.4	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
7.5	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.
7.6	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
7.7	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.
7.8	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.
7.9	Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.
7.10	Use sandboxing to analyze and block inbound email attachments with malicious behavior.

ID	Control 11 sub-controls: Secure configuration for network devices, such as firewalls, routers and switches
11.1	Maintain standard, 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, a specific individual's name 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 e-mail, 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

1-866-902-3900

Office of the Washington State Auditor