Office of the Washington State Auditor
Pat McCarthy

Performance Audit

Continuing Opportunities to Improve State Information Technology Security – 2018

December 20, 2018

Report Number: 1022918

Table of Contents

The mission of the Washington State Auditor's Office

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**.

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.

State Auditor's Office contacts

State Auditor Pat McCarthy
360-902-0360, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance Audit
360-902-0376, Scott.Frank@sao.wa.gov

Erin Laska – Principal Performance Auditor
360-778-2697, Erin.Laska@sao.wa.gov

Joseph Clark, CISA – Performance Auditor
360-725-5572, Joseph.Clark@sao.wa.gov

Clyde Meador, CISA , SSCP – Performance Auditor
360-725-5403, Clyde.Meador@sao.wa.gov

Kathleen Cooper – Director of Communications
360-902-0470, Kathleen.Cooper@sao.wa.gov

To request public records

Public Records Officer
360-725-5617, PublicRecords@sao.wa.gov

Background

Washington's state government depends on information technology (IT) systems to deliver an array of critical functions, such as public safety, tax collection, social services and transportation systems. These state IT systems process and store vast amounts of public and confidential data, from Social Security numbers and federal tax information to health care and arrest records. People are often required to share personal information if they wish to participate in government programs or receive services. They expect the state to protect their data as carefully as they would themselves to avoid financial harm and identity theft.

Government IT systems present a particularly tempting target to malicious hackers. In some cases, the aim is theft, as confidential information often can be sold for financial gain. In other cases, the goal is to disrupt vital government services. The security of state IT systems and related data are paramount to public confidence, the stability of government operations, and the safety and well-being of the state and its residents. Aside from such intangible losses, governments also face considerable tangible costs in dealing with data breaches, including the costs of identifying and repairing damaged systems, notifying and helping victims, and paying fines.

Government organizations across the country and around the world have been affected by cyber crime, including here in Washington. Since 2016, 11 Washington state public entities, including at least four state agencies, submitted breach notifications to the Washington State Office of the Attorney General.

State law (RCWs 19.255.010 and 42.56.590) requires any business, individual or public agency to notify the Washington State Office of the Attorney General when more than 500 Washington residents have their data stolen as a result of a single security breach.

To help Washington protect its mission-critical IT systems and secure the data it needs to carry on state business, we conducted a performance audit designed to identify opportunities to improve IT security.

Three state agencies volunteered to participate in this audit. To protect the state's 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).

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 State Auditor's Office 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 State Auditor's 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 state requirements and leading practices?

Answer in brief

State agencies must protect their IT systems, are required to meet the state's IT security standards, and can enhance their overall security posture by incorporating controls identified in leading practices. Agencies have already put numerous security controls in place, but they can further protect their IT systems by strengthening the implementation and documentation of those controls. In many cases, agencies did not tailor their documentation to reflect specific agency needs, leaving it open to interpretation and making it more difficult to enforce. Agencies can also supplement the state's IT security standards with leading practices to better secure their systems and data. Agency officials said limited resources contributed to the problems they had meeting state requirements. The Office of CyberSecurity, though positioned to help agencies meet requirements, could do more with additional resources.

State agencies must protect their IT systems, are required to meet the state's IT security standards, and can enhance their overall security posture by incorporating controls identified in leading practices

Washington state relies on complex IT systems to carry out critical government functions, such as public safety, tax collection, social services and transportation. Because of the state's reliance on these systems, as well as the sensitivity of the data within those systems, the state must protect those systems and the data they process. Security testing, both externally over the internet as well as internally within an agency's network, can provide a point-in-time assessment of an agency's security over its IT systems and data, identifying opportunities for the agency to improve its security.

Additionally, in order to help agencies protect these systems, the state's Office of the Chief Information Officer (OCIO) published IT security standards as OCIO 141.10: Securing Information Technology Assets Standards; these standards are under the authority of the state Office of CyberSecurity (OCS). Because the standards must apply to all state agencies, and take into account that risk can vary from agency to agency, they tend to be broad in nature. The standards provide instructions on how agencies should create an agency IT security program establishing a formal risk assessment process, and document how risk relates to an agency's operations, systems and personnel. Each agency is then required to develop detailed policies and procedures that comply with the standards, but are tailored to meet its individual needs.

The state's security standards represent baseline requirements for agencies' security practices. Agencies can also enhance their overall security posture by adopting leading practices, such as the Critical Security Controls from the Center for Internet Security. The Center for Internet Security is a nonprofit organization focused on safeguarding public and private organizations against cyber threats. These Critical Security Controls are a prioritized set of leading practices for cyber defense created to stop the most pervasive and dangerous attacks.

This audit assessed agencies' IT security practices against the top five Critical Security Controls, listed in the sidebar. While these controls do not represent an absolute safeguard against a cyberattack, according to the Center for Internet Security, aligning with the top five Critical Security Controls can provide an effective defense against the most common cyberattacks. We also reviewed Control # 11 because it is closely related to Control #3.

The Top 5 + 11: The Critical Security Controls used in this audit

#1 – Inventory of Authorized and Unauthorized Devices

#2 – Inventory of Authorized and Unauthorized Software

#3 – Secure Configurations for Hardware and Software

#4 – Continuous Vulnerability Assessment and Remediation

#5 – Controlled Use of Administrative Privileges

#11 – Secure Configurations for Network Devices

Agencies have already put numerous security controls in place, but they can further protect their IT systems by strengthening the implementation and documentation of those controls

The three state agencies included in this audit have taken significant measures to protect their IT systems and the confidential information maintained in those systems from risk. However, our external and internal security testing uncovered vulnerabilities that should be addressed. Agencies have begun addressing those vulnerabilities, sometimes even while the testing was still in progress.

The security controls in policies, procedures and technical implementation we tested at the agencies partially or fully align with several required state standards and leading practices. However, there are areas where agencies can improve both implementation and documentation of IT security controls.

In many cases, agencies did not tailor their documentation to reflect specific agency needs, leaving it open to interpretation and more difficult to enforce

Agencies can improve their IT security policies and procedures by more precisely describing how controls should be implemented. The agencies' documentation did include general requirements to comply with state standards, but their policies and procedures lacked specifics about which controls staff must implement to comply with the standards and ensure the security of agency systems and data. This problem is not unique to these agencies: all three prior state IT security audits, covering 12 more agencies, have included a similar comment.

State IT security standards require agencies' policies and procedures to contain details of the security controls applied to agency systems. When agencies do not meet this requirement, the consequence is a higher risk that security will not be implemented as intended. Detailed policies and procedures provide a clear roadmap for compliance; more general policies and procedures are open to interpretation, and different personnel may implement the same control differently, especially where agencies experience turnover in IT staff, which is not uncommon. Detailed policies and procedures, clearly outlining security expectations and approved by agency leadership, also give security personnel authority to implement and enforce robust security.

Agencies can also supplement the state's IT security standards with leading practices to better secure their systems and data

Although not required, leading practices such as the Critical Security Controls can also help agencies enhance their overall security posture. The subset of Critical Security Controls assessed in this audit align with about one-third of the requirements in the state's IT security standards. Implementing all of the Top 20 Critical Security Controls would align with more of the standards. As the standards require agencies to document and implement security controls based on each agency's needs, but do not always provide details about how to do this, agencies may benefit from implementing the Critical Security Controls because those controls provide more specific steps for implementing IT security practices.

Agency officials said limited resources contributed to the problems they had meeting state requirements

When asked about problems in both documentation (policies and procedures) and implementation, agencies cited limited resources as a key contributing factor. Specifically they cited having too few staff. One agency said its requests for additional staff have been denied for almost 10 years. This agency also has one of the lowest ratios of IT staff to agency personnel compared to other agencies in this and other state IT security performance audits. Another agency said they have difficulty justifying requests for additional IT staff given the agency's resource limitations. The state's acting Chief Information Security Officer (CISO) also noted agencies often have difficulty recruiting and retaining enough IT security staff. Without adequate staffing, current staff must focus on day-to-day operations, and have limited capacity to develop policies and procedures, and implement IT security controls accordingly.

The Office of CyberSecurity, though positioned to help agencies meet requirements, could do more with additional resources

The state's acting CISO acknowledged OCS has a role in ensuring agencies are implementing controls and developing the related detailed IT security policies and procedures to comply with the state's IT security standards. Previous state IT security audits recommend OCS conduct outreach and provide guidance to state agencies to help them better align agency IT security practices with the state's IT security standards. In response, OCS has held frequent meetings for agency IT staff – sometimes monthly – including seminars on state IT security requirements and hands-on training using virtual labs to improve agency security capabilities. However, the CISO also said OCS itself lacks the resources needed to conduct sufficient outreach to individual agencies.

State Auditor's Conclusions

State agencies make tempting targets for malicious hackers. In some cases, the goals are financial, such as attempts to steal and sell confidential information maintained by agencies. In other cases, the goals are disruptive, such as attacks that slow down or disable important government services. Either way, it is important that state agencies protect their critical systems from these attacks.

Protecting the state from the evolving landscape of cyberthreats requires a significant investment at a number of different levels. State agencies need resources to build and maintain adequate security controls to protect their IT systems. The state's Office of CyberSecurity also needs resources to assist agencies in building those controls. Finally, external organizations like the Office of the State Auditor need sufficient resources to ensure the agencies use the resources effectively and build adequate controls that meet state requirements and incorporate leading practices. While no amount of resources can completely eliminate all cyberthreats, making strong investments at each of these levels can reduce the risk.

Recommendations

To help strengthen IT security controls and protect the confidential information within the state's networks and systems, we make the following recommendations.

To the three selected state agencies:

1. Continue remediating issues identified during security testing
2. Continue remediating gaps between agency IT security implementation or written policies and procedures and the state's IT security standards
3. Consider also further aligning agency IT security controls with leading practices recommended in Critical Security Controls #1 through #5 and #11
4. Continue periodically assessing IT needs and resources, including personnel and technology, to develop and maintain sufficient IT security

To the Office of CyberSecurity, WaTech:

5. Continue to reach out to state agencies to identify what information would help agencies:
   - Incorporate detailed controls into their policies and procedures
   - Align agency practices with state IT security standards
6. Continue to develop and provide that additional clarity or guidance to state agencies
7. Continue to assess resources to better assist agencies in developing and implementing their IT security programs

Agency Response

JAY INSLEE
Governor

STATE OF WASHINGTON
WASHINGTON TECHNOLOGY SOLUTIONS
1500 Jefferson Street SE • Olympia, Washington 98504-1501

December 14, 2018

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

Dear Auditor McCarthy:

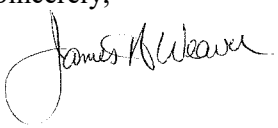
On behalf of the audited agencies, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report Continuing Opportunities to Improve State Information Technology Security – 2018.

We appreciate the report's recognition of the numerous security controls agencies have put in place. We agree that cyber threats and IT security is an evolving landscape and there is opportunity to further strengthen the implementation and documentation of controls.

We view strengthening our IT posture as a continuous responsibility of every agency. We continue to welcome the SAO's observations and recommendations of what to improve.

Please thank your team for their collaborative approach throughout this performance audit.

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, Senior Performance Project Manager, Results Washington, Office of the Governor
Scott Bream, Acting Chief Information Security 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 – 2018 DEC. 14, 2018

This management response to the State Auditor's Office (SAO) performance audit report received December 3, 2018, 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 state requirements and leading practices?

SAO Recommendations 1-4 to the three selected state agencies:

1. Continue remediating issues identified during security testing
2. Continue remediating gaps between agency IT security implementation or written policies and the procedures and the state's IT security standards
3. Consider also further aligning agency IT security controls with leading practices recommended in Critical Security Controls #1 through #5 and #11
4. Continue periodically assessing IT needs and resources, including personnel and technology, to develop and maintain sufficient IT security

STATE RESPONSE:
Agencies are committed to ongoing assessment and improvement of IT security needs. We agree with the opportunities for improvement identified to strengthen IT security by the SAO. The audited agencies will continue to work diligently to remediate the gaps identified between agency IT security implementation or written policies and procedures and the state's IT security standards. Agencies will also consider further aligning IT security controls with the leading practices the SAO identified.

Action Steps and Time Frame

- Each audited agency will establish a timeline to address the gaps, improvements and considerations identified. *By March 31, 2019*.

SAO Recommendation 5-7 to the Office of Cyber Security, WaTech:

5. Continue to reach out to state agencies to identify what information would help agencies:
    - Incorporate detailed controls into their policies and procedures
    - Align agency practices with the state IT security standards
6. Continue to develop and provide that additional clarity or guidance to state agencies
7. Continue to assess resources to better assist agencies in developing and implementing their IT security programs.

STATE RESPONSE:

The state Office of Cyber Security will survey state agencies to identify areas of security policy where agencies need additional clarification or interpretation in order to focus ongoing education and training programs.

OCS will use information from the survey to identify topics that will be addressed during its monthly technical and policy training sessions. In addition, OCS will prepare handouts to address frequently asked policy questions that can be provided to IT security staff by email, or when they visit OCS during weekly open office hours. OCS makes all staff available every Tuesday morning between 9:00 a.m. to Noon to address security questions and other issues. No appointment is necessary.

Action Steps and Time Frame

- OCS will survey state agencies and analyze the information collected to focus its education efforts. *By March 31, 2019*
- OCS will use the survey information during its ongoing outreach in order to help agencies incorporate detailed controls into their policies and procedures, and align agency practices with the state IT security standards. *By June 30, 2019*
- OCS will prepare explanatory handouts and continue to develop and provide that additional clarity or guidance to state agencies *Ongoing.*
- OCS will continue to assess resources to better assist agencies in developing and implementing their IT security programs. *Ongoing.*

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 section 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 a 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.** Since 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 controls against required state standards and 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.
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 required state standards and 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. However, it does recommend WaTech provide additional clarity or guidance to agencies to help them better align their IT security programs with state IT security standards.
8.	Analyze departmental performance data, performance measures and self-assessment systems	**Yes.** The audit examined and made recommendations to improve certain IT security controls 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 controls.

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.

Appendix B: Scope, Objectives and Methodology

To determine whether there were opportunities to strengthen IT security controls at three state agencies, we asked the following question:

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

To help conduct the audit, we hired subject matter specialists with expertise in conducting security testing of organizational IT infrastructure and applications.

Selecting state agencies for testing

We selected three medium-sized state agencies that rely on confidential information to serve the people of Washington. All three agencies asked to be included in this audit following the publication of our second and third cybersecurity performance audits for 2016 and 2017. 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.

To protect the state's 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).

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 applications, systems and their underlying networks, including identifying and assessing issues 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 external and internal security testing. Because the state offers many of its 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, as the state's managed security layer is designed to block external scanning of assets within the state's security layer.

Comparing state agencies' security programs to leading practices and state standards

To determine whether agency IT systems align with selected Critical Security Controls and related state IT security controls, we reviewed agencies' IT security policies and procedures and the technical implementation of those controls.

Leading practices

We used select Critical Security Controls from the Center for Internet Security, version 6, as our criteria to assess agencies' IT security controls 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. The Controls are a prioritized set of leading practices for cyber defense created to stop the most pervasive and dangerous attacks, and are developed and vetted across a very broad community of government and industry practitioners including, for example, 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.

As the Critical Security Controls are prioritized, we reviewed the top five because, although not an absolute safeguard, according to the Center for Internet Security, aligning with the top five Controls can provide an effective defense against the most common cyberattacks. We also reviewed Control #11 because it is closely related to Control #3. Specifically, we reviewed the following Critical Security Controls:

- #1 – Inventory of Authorized and Unauthorized Devices
- #2 – Inventory of Authorized and Unauthorized Software
- #3 – Secure Configurations for Hardware and Software
- #4 – Continuous Vulnerability Assessment and Remediation
- #5 – Controlled Use of Administrative Privileges
- #11 – Secure Configurations for Network Devices

State standards

We also determined two agencies' compliance with the state's required IT security standards that are related to the six Critical Security Controls reviewed. We did not complete this partial review of the state IT security standards at one agency because the agency already planned a full review of the standards, and as a result this work would be largely redundant. The state's security standards are published by the Office of the Chief Information Officer under the authority of OCS as Securing Information Technology Assets Standards (141.10).

We determined state standards were related to the six Critical Security Controls if assessing a Control could also address a state standard. We reviewed about 100 of the 270 required state IT security controls at two agencies. This allowed us to give the agencies an assessment of how their IT security practices and policies align with the six Critical Security Controls, which are optional leading practices, and the related state standards, which are required.

Agency feedback on audit results

We gave each of the three state agencies the detailed results of their individual agency's tests as we completed them, as well as detailed recommendations. We also gave all detailed results and recommendations to OCS.