PERFORMANCE AUDIT

Office of the Washington State Auditor
Pat McCarthy

Continuing Opportunities to Improve State Information Technology Security – 2021

December 14, 2021

Report Number: 1029582

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

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.

Introduction

Critical government services depend on IT systems with confidential information that must be protected to avoid service disruptions and financial losses

Governments depend on information technology (IT) systems to deliver an array of critical functions. The security of IT systems and related data underpins the stability of government operations, and the safety and well-being of residents. Therefore, protecting these systems is paramount to public confidence, because the public expects governments to protect these systems from IT security incidents that could disrupt government services.

These IT systems also process and store confidential data. 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 and notifying and helping victims.

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.

Government IT systems and data are attractive targets for cyberattacks

Government IT systems present a particularly tempting target to cybercriminals. In addition to selling stolen information for financial gain, attackers target government systems with ransomware, essentially rendering IT systems and data unavailable until the attackers are paid. Because government IT systems support operations, attacked governments are often placed in the difficult position of either failing to deliver services 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 pump stations, emergency dispatch centers, and online tax and utility payment systems. Attackers have even disabled the ability for prison guards to open jail cell doors remotely.

According to a study by antivirus-software developer Emsisoft, a total of at least 225 federal, state and local governments in the United States were affected by ransomware in the years 2019 and 2020. When combined with ransomware attacks on healthcare and education organizations, the study estimated that the total cost of these attacks in 2019 alone may have exceeded $7.5 billion.

Washington governments have also been affected by cyberattacks. Since 2016, 24 Washington public organizations have reported data breaches to the Washington State Attorney General's Office as a result of a cyberattack. This includes the State Auditor's Office, which was alerted in January 2021 to a potential cybersecurity incident involving its third-party file transfer service. Multiple state and local governments have reported other kinds of cybersecurity incidents, such as fraud, to the State Auditor's Office, including a city where operations were crippled by ransomware.

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. The audit covered in this report included six state agencies: three large, one medium-sized, two small. Two had participated in earlier IT security performance audits. This audit also included work at three agencies where 2020 audit work was partially delayed due to COVID-19. 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?

Testing to see if agencies can make their IT systems more secure

To determine if the selected state agencies can make their IT systems more secure, we conducted penetration testing of selected applications and networks. We performed testing at nine agencies: the six planned for this audit, plus the three where penetration testing in 2020 was delayed due to COVID-19.

Comparing state agency IT security programs to leading practices

We considered IT security practices at the six agencies scheduled for this audit. We assessed five of the six agencies' IT security policies, procedures and practices to selected leading practices to identify any improvements that could

make them stronger. The sixth agency had recently completed comparable audit work. After reviewing the most relevant portions of this work, we decided it would not be a good use of our resources to perform duplicative work.

We selected leading practices from version 7.1 of the Center for Information Security's Controls (CIS Controls), which were developed by a broad community of private and public sector stakeholders after examining the most common attack patterns. The CIS Controls are a prioritized list of control areas designed to help organizations with limited resources optimize their security defense efforts to achieve the highest return on investment.

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 a list of CIS Controls considered for this audit.

Audit Results

We communicated the detailed results of our audit work as we completed it. At that time, we gave each agency's management recommendations for its review, response and action. We found that while each agency's IT policies and practices partially align with the CIS Controls, all can further align those policies and practices with the Controls. The agencies have already begun addressing significant issues we identified, and continue to make improvements.

Because the public distribution of tests performed and test results could increase the risk to the state, distribution of this information is kept confidential under RCW 42.56.420 (4), and under Generally Accepted Government Auditing Standards, Sections 9.61-9.67.

State Auditor's Conclusions

The State Auditor's Office recognizes the agencies' willingness to participate in this audit, demonstrating their dedication to making government work better. It is apparent that agency management and staff want to be accountable to the citizens and good stewards of public resources. Throughout the audit, they fostered a positive and professional working relationship with our Office.

Recommendations

To protect agency systems and the information within those systems, we recommend the six audited agencies:

1. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them.
2. Continue to identify and periodically assess the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.
3. In addition, we recommend the five agencies whose IT security practices we reviewed further align their IT security programs with leading practices recommended in the CIS Controls.

Agency Response

JAY INSLEE
Governor

WILLIAM S. KEHOE
Director &
State Chief Information Officer

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

December 13, 2021

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

Dear Auditor McCarthy:

On behalf of the audited participants, 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 – 2021."

We appreciate the report recognizing state government auditees' dedication to making government work better.

We must vigilantly continue to strengthen protections of state government systems and data. We appreciate the SAO continuing to identify opportunities to help us do so.

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,

William S. Kehoe
Director & State Chief Information Officer

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 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 – 2021 Dec. 13, 2021

This management response to the State Auditor's Office (SAO) performance audit report received November 29, 2021, 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 selected state agencies: to protect agency systems and the information within those systems, we recommend the six audited agencies:

1. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them.
2. Continue to identify and periodically assess the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.
3. In addition, we recommend the five agencies whose IT security practices we reviewed further align their IT security programs with leading practices recommended in the CIS controls.

STATE RESPONSE:
We agree with the opportunities for improvement identified by the SAO to help protect agency systems and data. We also recognize our responsibility to continue improving state government security and take that duty seriously. Audited agencies have already implemented improvements and will continue to remediate any remaining vulnerabilities. The agencies will also continue to assess and make improvements to IT security needs – including further alignment with leading practices recommended in the CIS controls where appropriate. These controls are more prescriptive than the OCIO IT security standards 141.10 that agencies are required to follow.

The OCIO will use the SAO's findings and observations of this and previous audits to work with all state organizations to better improve the state's security posture.

Action Steps and Time Frame

- Each audited entity will work with their appropriate governing bodies to address and prioritize vulnerabilities, improvements and considerations suggested by the SAO during calendar year 2022.

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 assessed select security practices and vulnerabilities at a total of nine state agencies.

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 nine agencies, including penetration testing of selected internal and external applications and underlying networks. We also compared five agencies' IT security programs to controls selected from those published by the Center for Internet Security as the CIS Controls (described in the sidebar on page 14).

Selecting state agencies for testing

For this audit, we selected six state agencies that store confidential information and provide critical government services to the people of Washington. Three are large agencies, one is medium-sized, and two are small; two had participated in an earlier IT security performance audit. After making our selection, 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. We followed the same process for the three agencies selected to participate in our 2020 audit but whose penetration testing was delayed due to COVID-19.

Penetration testing

We conducted external and internal penetration testing at all nine agencies and evaluated each agency's key applications, systems and their underlying networks. We completed this work between November 2020 and September 2021. 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. We based our selection on several factors, including criticality to the agency's mission and the sensitivity of the data within those applications. We tested applications available only to agency employees on internal networks, as well as applications available to the public 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

This audit also assessed the extent to which five agencies' IT security programs, including their implementation and documentation, aligned with selected practices from the CIS Controls. The sixth agency had recently completed comparable audit work. After reviewing the most relevant portions of this work, we decided it would not be a good use of our resources to perform duplicative work. 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.

The Center for Internet Security (CIS) 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.

To determine whether agency IT security practices align with the CIS Controls, 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 on a sample of systems. We performed this work for five agencies remotely between September 2020 and September 2021, with some additional follow-up afterwards.

Assessment criteria: Selecting the CIS Controls

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.

Because the CIS Controls are prioritized, we selected from the top six controls because, although they are not an absolute safeguard against cyberattacks, CIS 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 are listed in **Figure 1**.

Figure 1 – CIS "Basic Six" plus Control 11

- **#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.

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 of the five agencies was **reporting** on the control overall. A higher level of alignment 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 nine 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.

"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