Office of the Washington State Auditor
Pat McCarthy

Performance Audit Report

Opportunities to Improve State Information Technology Security – 2022

Published January 23, 2023

Report No. 1031903

Find out what's new at SAO by scanning this code with your smartphone's camera

TABLE OF CONTENTS

Americans with Disabilities

In accordance with the Americans with Disabilities Act, we will make this document available in alternative formats. For more information, please contact our Office at (564) 999-0950, TDD Relay at (800) 833-6388, or email our webmaster at webmaster@sao.wa.gov.

ABOUT THE AUDIT

Critical government services depend on IT systems with confidential information, which 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 such data can cause governments to face considerable tangible costs. These include identifying and repairing damaged systems as well as and notifying and helping victims of the breach.

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.

This audit looked for opportunities to improve the IT security at four state agencies

To help the selected state agencies protect their 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 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 and vulnerability scanning of selected key systems.

Comparing agencies' IT security programs to leading practices

We compared the four agencies' IT security policies, procedures and practices to selected leading practices to identify any improvements that could make them stronger. We selected the practices from the Center for Internet Security's Controls (CIS Controls). These controls 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. **Appendix C** lists other performance audits in this series.

AUDIT RESULTS

We communicated the detailed results of our tests and assessments as we completed them. At that time, we gave each agency's management recommendations for its review, response and action. While each agency's IT policies and practices partially aligned with the CIS Controls, we found areas where each one could make improvements. The agencies have already taken steps to address our recommendations, and continue to make improvements.

Because the public distribution of tests performed, test results, specific recommendations and the agencies' specific responses 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.

Recommendations

To protect agency IT systems and the information contained in them, we recommended the audited agencies:

- Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them.
- Continue to identify and periodically assess the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.

Auditor's Remarks

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

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

January 18, 2023

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 "Opportunities to Improve State Information Technology Security – 2022."

We appreciate the report recognizing state government auditees' have already taken steps to address recommendations and continue to do so.

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
Nick Streuli, Executive Director of Policy and Outreach, Office of the Governor
David Schumacher, Director, Office of Financial Management
Mandeep Kaundal, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
Ralph Johnson, 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 OPPORTUNITIES TO IMPROVE STATE INFORMATION TECHNOLOGY SECURITY – 2022 JAN. 18, 2023

This management response to the State Auditor's Office (SAO) performance audit report received December 19, 2022, 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 IT systems and the information contained in them, we recommend:

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.

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. As noted in the report, 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 continue to work with their appropriate governing bodies to address and prioritize vulnerabilities, improvements and considerations suggested by the SAO during calendar year 2023 and beyond.

APPENDIX A: INITIATIVE 900 AND AUDITING STANDARDS

Appendix A: Initiative 900 and Auditing Standards

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 the U.S. Government Accountability Office's *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 Schedule of Audit Findings and Responses 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 beach or security incident.
2. Identify services that can be reduced or eliminated	No. The audit objectives 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 the agencies' IT security posture.

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 identify a need for statutory or regulatory change.
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 published by the Center for Internet Security to assess selected 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 (July 2018 revision) by the U.S. Government Accountability Office and *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: SCOPE, OBJECTIVES AND METHODOLOGY

Scope

This audit assessed the extent to which four selected agencies' IT security programs, including their implementation and documentation, aligned with selected CIS Controls and their supporting sub-controls. This audit did not assess the agencies' alignment with federal or state special data-handling laws or requirements.

Objectives

To help the selected state agencies protect their 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 answered 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 objectives, we conducted technical testing on each agency's network, and we compared each agency's IT security programs to selected leading practices.

Internal and external security testing

To determine if each selected agency had vulnerabilities in its IT environment, we conducted internal and external penetration testing of selected key applications, systems and networks. A third-party vendor performed this work on our behalf between October 2021 and December 2022. Our own auditors and IT security specialists also conducted additional, limited, technical testing of separately sampled systems within each agency during this general timeframe. This work included identifying and assessing vulnerabilities, and determining whether they could be exploited.

Comparing agencies' IT security programs to leading practices

To determine whether each agency's IT security practices could better align with leading practices, we interviewed key IT staff, reviewed agency IT security policies and procedures, observed agency security practices and settings, and conducted limited technical analysis of agency systems. This work was completed at the four agencies between January and November 2022.

We used selected controls from the CIS Controls, version 7.1, as our criteria to assess the IT security programs at three of the agencies and to identify areas that could be strengthened. We used selected controls from version 8 of the CIS Controls at the fourth agency.

CIS is a nonprofit organization focused on securing public and private organizations against cyber threats. The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense and others.

Each control consists of a series of sub-controls that are distinct and measurable tasks; when the sub-controls are implemented together, they fully meet the requirements of the overall control. We assessed each agency against those sub-controls to determine how well it aligned with the control overall. We did this by assessing the extent to which each agency met each sub-control in at least two areas:

1. **Implementing** the sub-control
2. **Maintaining documentation** to support the sub-control, such as policies or procedures

Work on Internal Controls

This audit assessed the IT security internal controls at four state agencies. We used a selection of controls from the CIS Controls as the internal control framework for the assessment. Based on an initial assessment, we selected between four and six controls to include in the scope. We completed our assessment for the purpose of identifying opportunities for each agency to improve its internal IT security controls, but not to provide assurance on the agencies' current IT security posture.

APPENDIX C: EARLIER STATE CYBERSECURITY AUDITS

Cybersecurity audits examine information technology systems used in government operations. They look for weaknesses in that technology and propose solutions to help strengthen those systems. Cybersecurity audits are a type of performance audit and are provided at no cost to state and local governments, thanks to 2005's voter-approved Initiative 900. Our portfolio of IT-related audits also includes topics like the safe disposal of data and computers, with a new audit looking at critical infrastructure across the state due to publish early in 2023.

You can learn more about our work in this field on our website at: https://sao.wa.gov/about-audits/about-cybersecurity-audits/

Read a special report, issued in 2022, about our cybersecurity audit findings.

Earlier state cybersecurity audits

Continuing Opportunities to Improve State Information Technology Security – 2021

Continuing Opportunities to Improve State Information Technology Security – 2020

Continuing Opportunities to Improve State IT Security – 2019

Continuing Opportunities to Improve State Information Technology Security – 2018

Continuing Opportunities to Improve State Information Technology Security – 2017

Continuing Opportunities to Improve State Information Technology Security – 2016

Opportunities to Improve State IT Security

ABOUT THE STATE AUDITOR'S OFFICE

The State Auditor's Office is established in the Washington State Constitution and is part of the executive branch of state government. The State Auditor is elected by the people of Washington and serves four-year terms.

We work with state agencies, local governments and the public to achieve our vision of increasing trust in government by helping governments work better and deliver higher value.

In fulfilling our mission to provide citizens with independent and transparent examinations of how state and local governments use public funds, we hold ourselves to those same standards by continually improving our audit quality and operational efficiency, and by developing highly engaged and committed employees.

As an agency, the State Auditor's Office has the independence necessary to objectively perform audits, attestation engagements and investigations. Our work is designed to comply with professional standards as well as to satisfy the requirements of federal, state and local laws. The Office also has an extensive quality control program and undergoes regular external peer review to ensure our work meets the highest possible standards of accuracy, objectivity and clarity.

Our audits look at financial information and compliance with federal, state and local laws for all local governments, including schools, and all state agencies, including institutions of higher education. In addition, we conduct performance audits and cybersecurity audits of state agencies and local governments, as well as state whistleblower, fraud and citizen hotline investigations.

The results of our work are available to everyone through the more than 2,000 reports we publish each year on our website, www.sao.wa.gov. Additionally, we share regular news and other information via an email subscription service and social media channels.

We take our role as partners in accountability seriously. The Office provides training and technical assistance to governments both directly and through partnerships with other governmental support organizations.

Stay connected at sao.wa.gov

- Find your audit team
- Request public records
- Search BARS manuals (GAAP and cash), and find reporting templates
- Learn about our training workshops and on-demand videos
- Discover which governments serve you — enter an address on our map
- Explore public financial data with the Financial Intelligence Tool

Other ways to stay in touch

- Main telephone: (564) 999-0950
- Toll-free Citizen Hotline: (866) 902-3900
- Email: webmaster@sao.wa.gov