Office of the
Washington
State Auditor
Pat McCarthy

PERFORMANCE AUDIT

Opportunities to Improve IT Security at Local Governments Fiscal Year 2023

September 11, 2023

Report Number: 1033173

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

Washington local governments must protect the IT systems they rely on to deliver critical government services to their residents

People depend on Washington's state and local governments for many different services, from public safety and tax collection, to social services, transportation systems and fresh water. Governments in turn depend on information technology (IT) to provide these services. The security of these systems underpins the stability of government operations, and the safety and well-being of residents. 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 breach involving such data can present the affected government with considerable tangible costs, from identifying and repairing damaged systems to notifying and helping victims of the breach.

Across the country and throughout the world, governmental technology is increasingly under attack, leaving people vulnerable. Those attacks add up, costing taxpayers money and eroding trust in institutions.

The Office of the Washington State Auditor has worked with state agencies and local governments to improve IT security for more than a decade. Our cybersecurity audits examine IT systems, looking for weaknesses that attackers could exploit and proposing solutions to help strengthen those systems. Our cybersecurity audits are a type of performance audit and are provided at no cost to the audited governments thanks to 2005's voter-approved Initiative 900.

About the Audits

This report summarizes fiscal year 2023 results from two types of local government cybersecurity audits

We conducted two types of cybersecurity audits at a total of 35 local governments in FY 2023. We have already issued reports for a total of 18.

- **Thorough cybersecurity audits.** This report covers audits at five local governments; we have already published individual reports for six more. These audits included internal and external penetration testing and a review of their IT security controls compared to leading practices. We discuss our work in this area and our recommendations in Chapter One and **Appendix A**.
- **Limited-scope cybersecurity audits at local governments with critical infrastructure functions.** This report covers audits at 12 such governments; we have already published information on 12 more. These audits focused on their external security posture and IT security controls more directly related to their specialized functions. We describe our work in this area and our recommendations in Chapter Two and **Appendix B**.

We communicated the detailed results of our tests and assessments as we completed them. At that time, we gave each local government's management recommendations for its review, response and action. Because the public distribution of tests performed, test results, recommendations, and the government's 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.

Initiative 900 (I-900) requirements and compliance with generally accepted government auditing standards

All the audit work discussed in this report was conducted to address the standards of I-900. This initiative, approved by Washington voters in 2005 and enacted into state law (RCW 43.09.470) 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." We detail the elements of I-900 examined in each type of audit in the relevant appendix.

I-900 also specified that performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards. The work in this report was performed 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.

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. Appendices A and B address the I-900 areas covered and information about our methodology for each type of audit. **Appendix C** lists other performance audits that address cybersecurity issues.

Audit Results

Chapter One: A review of leading practices and security testing identified opportunities to improve IT security at five local governments

To help five selected local governments protect their IT systems and secure the data they need to operate, we conducted a comprehensive performance audit designed to identify opportunities to improve IT security. This audit answered the following question:

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

Audit results

Our security testing found that while each local government had good IT security practices in place, there were opportunities to make IT systems more secure. Additionally, while each local government's IT policies and practices were partially aligned with the CIS Controls, we noted areas where each one could make improvements. Responsible officials and staff expressed agreement with the audit results and said they intend to use them as they continue to improve their cybersecurity posture. The governments have since taken steps to address our recommendations and continue to make improvements.

Recommendations

To protect local government IT systems and the information contained in those systems, we recommended the audited governments:

- Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them.
- Revise IT security policies and procedures to align more closely with leading practices.
- Continue to identify and periodically assess the local government's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.

Chapter Two: Assessments found 12 governments with critical infrastructure systems have opportunities to strengthen their external security posture

Threats to critical infrastructure operations have grown more urgent since Russia's full-scale invasion of Ukraine in early 2022. In response to warnings released by the U.S. government's Cybersecurity and Infrastructure Security Agency (CISA), we performed audits which looked for opportunities to improve IT security at 12 local governments that provide critical infrastructure services. To help them improve their IT security, this audit answered the following question:

- Are there opportunities to strengthen the external security posture of select governments with critical infrastructure?

Audit results

While each local government had good IT security practices in place, we found opportunities to make their IT systems more secure. Responsible officials and staff expressed agreement with the audit results and said they intended to use them as they continue to improve their cybersecurity posture. The governments have since taken steps to address our recommendations and continue to make improvements.

Recommendations

To protect local government IT systems and the critical infrastructure functions those local governments provide, we recommended the audited local governments:

1. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them
2. Consider strengthening IT security controls as detailed in the tailored recommendations provided to each local government
3. Continue implementing guidance and leveraging free and low-cost resources made available by the U.S. Cybersecurity and Infrastructure Security Agency

State Auditor’s Remarks

The Washington State Auditor’s Office recognizes each local government’s willingness to participate in this audit, demonstrating their dedication to making government work better. It is apparent each government’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.

Appendix A: Scope, Objectives and Methodology – Cybersecurity Leading Practices

Scope

This audit identified opportunities for five local governments to improve their IT security. All five volunteered for a cybersecurity audit. The audit assessed the extent to which five selected local governments' IT security programs, including their implementation and documentation, aligned with selected CIS Controls and tested the effectiveness of external and internal IT security controls using penetration testing to assess if there were opportunities to make them more secure. This audit did not assess the governments' alignment with federal or state special data-handling laws or requirements.

Objectives

To help the selected local governments 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 local governments 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 on each local government's network, and we compared each government's IT security programs to selected leading practices.

Internal and external penetration testing

To determine if each selected government has vulnerabilities in its IT environment, we conducted internal and external penetration testing of selected key applications, systems and networks. This work was performed between January and March 2023 by a third-party vendor on our behalf. Our own auditors and IT security specialists also conducted additional, limited, technical testing of separately sampled systems within each local government during this general timeframe. This work included identifying and assessing vulnerabilities, and determining whether they could be exploited.

Comparing government' IT security programs to leading practices

To determine whether each local government's IT security practices could better align with leading practices, we interviewed key IT staff, reviewed local government IT security policies and procedures, observed local government security practices and settings, and conducted limited technical analysis of government systems. This work was completed at the five selected governments between June 2022 and June 2023.

We used selected controls from the CIS Controls, version 8, as our criteria to assess the IT security programs at the five local governments to identify areas that could be made stronger.

CIS is a nonprofit organization focused on safeguarding 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 safeguards that are distinct and measurable tasks. We assessed each local government against selected safeguards to determine alignment with each selected safeguard in two areas:

1. Implementing the safeguard
2. Maintaining documentation to support the safeguard, such as policies or procedures

Work on internal controls

This audit assessed the IT security internal controls at five selected local governments. 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 an average of 30 safeguards to include in the scope of each audit. We completed our assessment for the purpose of identifying opportunities for each selected local government to improve its internal IT security controls, but not to provide assurance on the governments' current IT security posture.

Initiative 900 requirements

I-900 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 summarizes the I-900 elements considered inside or outside the scope of these cybersecurity audits.

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 governments avoid or mitigate costs associated with a data beach or security incident.
2. Identify services that can be reduced or eliminated	**No.**
3. Identify programs or services that can be transferred to the private sector	**No.** While governments 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.**
5. Assess feasibility of pooling information technology systems within the department	**No.**
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** The audit recommended each audited government 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.**
8. Analyze departmental performance data, performance measures and self-assessment systems	**Yes.** Although the audit did not review indicators of each government's performance of its core mission, it did review certain controls that provide metrics on how each government'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 governments' IT security controls.

Appendix B: Scope, Objectives and Methodology – Critical Infrastructure

Scope

This audit identified opportunities for 12 local governments with critical infrastructure functions to improve their IT security. "Critical infrastructure functions" means that they provide critical services to the public, such as airports, dams, power stations, public hospitals and wastewater services. Of the local governments in the state that provide these services, we began by reviewing those which had already expressed interest in a cybersecurity performance audit. We then selected additional governments based on a variety of factors, such as the number of customers they serve. All 12 governments volunteered for the audit.

This audit tested the effectiveness of external IT security controls using penetration testing to assess if there were opportunities to make them more secure. The audit also included a review of the design of key IT security controls in place as they relate to critical infrastructure. These key IT security controls were identified by our IT security subject matter experts. This audit did not assess the documentation associated with these internal controls or the governments' alignment with federal or state special data-handling laws or requirements.

Objectives

To help the selected local governments 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:

- Are there opportunities to strengthen the external security posture of selected local governments with critical infrastructure?

Methodology

To answer the audit objectives, we conducted penetration testing on each local government's internet-facing systems, completed an open-source intelligence assessment which includes reviewing information publicly available on the internet, and conducted interviews with key IT management and staff.

External penetration testing

To determine if the local government can strengthen its external security posture, we conducted external penetration testing of each government's internet-facing assets, such as a public website. A third-party vendor performed this work on our behalf between January and May 2023.

Open-source intelligence assessment

Our third-party vendor also conducted a review of publicly available information on the internet about each selected local government (known as open-source intelligence). In this case, we wanted to identify potential breaches of each government's data as well as compromised accounts. Evidence of a data breach, especially one that the government was not aware of, could indicate an ongoing attack against or within its systems, and compromised accounts could be used to launch or further attack it. We assessed the result of this review and advised each government of actions it could take in this area to improve its IT security posture. This work was performed between January and May 2023.

Interviews with IT management and staff

We also interviewed each local government's key IT management and staff to gain an understanding of the IT and operational technology infrastructure within their organization, and the security controls protecting that infrastructure. Following each interview, we gave the government detailed recommendations tailored to its specific situation. This activity was based solely on each government's attestation and did not include any testing or verification beyond the interview itself. This work was performed between January and April 2023 by State Auditor's Office auditors and cybersecurity specialists.

Work on internal controls

This audit reviewed the design and tested the effectiveness of limited IT security internal controls at 12 local governments. The work on internal controls included a review of the design of the controls related to each government's critical infrastructure and the effectiveness of the security controls related to each government's internet-facing assets, such as their public websites. The audit did not review their related policies or procedures. We completed our assessment for the purpose of identifying opportunities for each selected local government to improve its IT security internal controls, but not to provide assurance on each government's current IT security posture.

Initiative 900 requirements

I-900 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 summarizes the I-900 elements considered inside or outside the scope of these cybersecurity audits.

I-900 element	Addressed in the audit
1. Identify cost savings	**No.**
2. Identify services that can be reduced or eliminated	**No.**
3. Identify programs or services that can be transferred to the private sector	**No.**
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**No.**
5. Assess feasibility of pooling information technology systems within the department	**No.**
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**No.**
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.**
8. Analyze departmental performance data, performance measures and self-assessment systems	**No.**
9. Identify relevant best practices	**Yes.** The audit made recommendations to improve IT security based on the subject matter expertise of our cybersecurity specialists and the U.S. Cybersecurity and Infrastructure Security Agency. The audit also assessed the effectiveness of the local governments' IT security controls according to best practices identified by our third-party penetration testers.

Appendix C: Other Cybersecurity Audit Work

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.

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

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

Read this report to learn about our cybersecurity work in 2020 and 2021.

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