Office of the Washington State Auditor
Pat McCarthy

Performance Audit Report

Opportunities to Improve Information Technology Security at Critical Infrastructure Organizations – 2022

Published January 23, 2023

Report No. 1031904

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, which must be protected to avoid disruptions to services essential to the safety, health and well-being of Washingtonians

Governments depend on information technology (IT) systems to deliver an array of essential services to the public, including clean water, reliable energy and emergency healthcare services. These functions are part of the state's critical infrastructure. The security of IT systems and related data underpins the stability of these government operations, and the safety and well-being of residents. Protecting these systems is therefore paramount to public confidence, because the public expects governments to reliably provide these services.

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.

Threats to critical infrastructure operations have grown more urgent since Russia's full-scale invasion of Ukraine in early 2022. The U.S. government's Cybersecurity and Infrastructure Security Agency (CISA) released warnings to state and local governments about the potential for cyberattacks by Russia or Russian-aligned actors. The warning suggested attacks might target critical infrastructure in the United States in retaliation for the United States' support of Ukraine. While these warnings were general in nature and did not identify specific targets, they urgently encouraged state and local governments to improve their IT security posture to protect against potential attacks.

This audit looked for opportunities to improve the IT security at 20 local governments with critical infrastructure functions

In response to these warnings, this audit looked for opportunities to improve IT security at 20 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?

Evaluating whether local governments with critical infrastructure can strengthen their external security posture

To identify these opportunities, we conducted work in three areas.

First, we conducted external penetration testing of each government's internet-facing systems. We looked for any weaknesses that could be used by an attacker over the internet, such as a foreign adversary, to cause a security breach or disrupt the government's essential activities.

Second, we conducted a limited open-source intelligence assessment of freely available information associated with each local government on the internet. In this case, we were looking for evidence of data breaches or compromised accounts associated with each local government. A previously undiscovered data breach could point to an ongoing attack within the organization, and compromised accounts could be used to launch an attack against the organization.

Finally, we interviewed each local government's key IT management and staff to gain an understanding of their IT and operation technology infrastructure. These interviews identified key areas of strength and opportunities for improvement, and resulted in tailored recommendations on specific steps for improving IT security.

We reported the results of our work to each audited local government as we completed it.

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 that address cybersecurity issues.

AUDIT RESULTS

While each local government had areas of strong IT security practices, we found areas where each one could improve. We communicated the detailed results of our work as we completed it. At that time, we gave each government's management recommendations for its review, response and action. The responsible officials and staff agreed with the audit results and expressed their intention to use them to continue to improve their cybersecurity posture. The governments have since 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 local government IT systems and the critical infrastructure functions those local governments provide, we recommended the audited local governments:

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

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: 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 local governments 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. The audit was not designed to identify services that can be transferred to the private sector, but to instead assess IT security controls that are in place.
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 local government programs or services.
5. Assess feasibility of pooling information technology systems within the department	No. The audit focused on reviewing the design and testing the effectiveness of security controls. It did not analyze the feasibility of pooling information technology systems.

I-900 element	Addressed in the audit
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	No. While the audit focused on reviewing the design and testing the effectiveness of security controls, it did not analyze departmental roles and functions.
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	No. The audit did not analyze departmental performance data, performance measures or self-assessment systems.
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.

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 identified opportunities for 20 local governments with critical infrastructure functions to improve their IT security. We selected governments that provide critical services to the public, such as public hospitals and energy, water, and wastewater services. Of the local governments in the state that provide these services, we began by selecting 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 amount of customers they serve. We plan to continue conducting this type of audit at additional local governments which have critical infrastructure functions.

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 the local governments' critical infrastructure. These key IT security controls were identified by our IT security subject matter experts. This audit did not assess the documentation associated 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 their 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 publicly-available information available on the internet, and conducted interviews with key IT management and staff.

External penetration testing

To determine if each selected local government can strengthen their external security posture, we conducted external penetration testing of each government's internet-facing assets, such as their public websites. A third-party vendor performed this work on our behalf between March and December 2022.

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 March and December 2022.

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 June and December 2022 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 20 local governments. This 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.

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. A new audit looking at the cybersecurity of four state agencies is due to publish early in 2023, and 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: https://sao.wa.gov/about-audits/about-cybersecurity-audits/

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

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