PERFORMANCE AUDIT

Office of the Washington State Auditor
Pat McCarthy

Opportunities to Improve IT Security at Local Governments – FY 2025

September 8, 2025

Report Number: 1038033

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

Tina Watkins – Director of Local Audit
360-260-6411, Tina.Watkins@sao.wa.gov

Peg Bodin, CISA – Assistant Director for IT Audit
564-999-0965, Peggy.Bodin@sao.wa.gov

Erin Laska – IT Security Audit Manager
564-999-0615, Erin.Laska@sao.wa.gov

Michael Hjermstad – IT Security Assistant Audit Manager
564-999-0874, Michael.Hjermstad@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 help them deliver 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 critical to maintaining public confidence in government.

Some of 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. The effects of these attacks add up rapidly, 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. These 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.

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.

About the Audits

This report summarizes fiscal year 2025 results from three types of local government cybersecurity audits

We completed three types of cybersecurity audits at a total of 52 local governments in fiscal year (FY) 2025. The sidebar summarizes the total results of the year's activities.

- **Cybersecurity leading practices audits.** This report covers audits at seven local governments. 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 39 such governments. 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**.
- **Improving ransomware resiliency at local governments.** This report covers audits at six governments. These audits focused on IT security controls more directly related to ransomware prevention, detection and response. We describe our work in this area and our recommendations in Chapter Three and **Appendix C**.

We communicated the detailed results of our tests and assessments to each local government's IT staff as we completed them. We also 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 individual responses could increase the risk to these governments, 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.

Breakdown of FY 2025 IT security audits at local governments

- Cybersecurity: 7
- Critical infrastructure: 39
- Ransomware resiliency: 6

Total: 52

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 local 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 (https://leg.wa.gov/about-the-legislature/committees/joint/jlarc-i-900-subcommittee). The Office conducts periodic follow-up evaluations to assess the status of recommendations and may conduct follow-up audits at its discretion. **Appendices A, B** and **C** address the I-900 areas covered and information about our methodology for each type of audit. **Appendix D** lists other performance audits that address cybersecurity issues

Audit Results

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

To help protect IT systems and secure the data the governments need to operate, we conducted cybersecurity leading practices performance audits designed to identify opportunities to improve IT security at seven selected local governments. These audits 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 some good IT security practices in place, there were also opportunities to make IT systems more secure. Additionally, while each local government's IT practices were partially aligned with the leading IT security practices we selected to review, we noted areas where each one could make improvements. Governments supplied a formal response to our recommendations that 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:

1. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them.
2. Revise IT security policies and procedures to align more closely with leading practices.
3. 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 39 governments with critical infrastructure systems have opportunities to strengthen their external security posture

Threats to critical infrastructure operations have grown more urgent since the invasion of Ukraine in early 2022 followed by heightened conflicts in the Middle East and serious threats from foreign state-sponsored actors. Multiple organizations, including federal agencies and experts in foreign countries (some listed in the sidebar), have issued warnings to the critical infrastructure community, relaying concerns about persistent malicious cyberattacks that could affect them. In March 2024, the National Security Council asked the governors of all 50 states to develop cybersecurity plans to protect both drinking water and wastewater systems. The Council recommended each plan determine where these systems are vulnerable to cyberattacks and include the actions states will take to build in cybersecurity protections.

In response to these warnings, the State Auditor's Office developed a program of performance audits that focused on improving cyber defenses at Washington local governments that provide critical infrastructure services. Our FY 2025 audits included assessments at 39 local governments, all with responsibilities for drinking water or wastewater. Washington's governor included audits of these systems as part of our state's cybersecurity plan submitted to the National Security Council.

These audits answered the following question:

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

Organizations promoting heightened cybersecurity awareness efforts for critical infrastructure installations

- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- National Security Agency (NSA)
- Environmental Protection Agency (EPA)
- Department of Energy (DOE)
- United States Department of Agriculture (USDA)
- Food and Drug Administration (FDA)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Canadian Centre for Cyber Security (CCCS)
- National Cyber Security Centre, UK (NCSC-UK)

Audit results

While each local government had some good IT security practices in place, we found opportunities to make their IT systems more secure. Those governments that supplied a formal response to our recommendations expressed agreement with the audit results, and said they intended to use them as they continue to improve their cybersecurity posture. Some governments did not provide a formal response.

The responding governments said they have 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. CISA and the Multi-State Information Sharing and Analysis Center (known as MS-ISAC)

Chapter Three: A review of ransomware resiliency identified opportunities to improve IT security at six local governments

Ransomware attacks are of particular concern because they can deny government employees access to systems and data used to deliver essential government services. Such attacks can expose school, health or banking data, and compromise systems used by critical services like fire and rescue, police, courts, and utilities. They can also cost governments thousands – if not millions – of dollars, whether in ransom payments, lost productivity, increased insurance premiums or in replacing affected systems. They can also endanger lives when the compromised systems involve emergency services. To help local governments prevent, detect, respond to and recover from this increasing risk, we performed audits that specifically examined resiliency to ransomware at six local governments. This audit answered the following question:

- Can selected local governments make their IT systems more secure and better align with leading practices that contribute to ransomware attack resiliency?

Audit results

While each selected local government had some good IT security controls and practices in place, we found opportunities to make their IT systems and IT security practices more resilient to ransomware. Governments supplied a formal response to our recommendations that 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 information contained in those systems from ransomware attacks, we recommended the audited local governments:

1. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect them
2. Continue strengthening IT security controls to further align with leading practices as detailed in the recommendations we provided
3. Continue to identify and periodically assess IT security needs and resources, including personnel and technology, to mature and maintain sufficient security

State Auditor's Remarks

The Office of the Washington State Auditor recognizes each local government's willingness to participate in these audits, demonstrating their dedication to making government work better. It is apparent each government's management and staff want to be accountable to Washington's residents 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: Objectives, Scope and Methodology – Cybersecurity Leading Practices

Objectives

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

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

Scope

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

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 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 October 2023 and January 2025 by a third-party vendor on our behalf. Our own auditors and IT security specialists also conducted additional, limited, technical testing of separately

selected 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 the government's IT security practices could better align with leading practices, we interviewed key IT staff, observed their security practices and settings, conducted limited technical analysis of government systems, and as applicable, reviewed local government IT security policies and procedures. This work was completed at the seven selected governments between April 2024 and January 2025.

We used selected controls from the Center for Internet Security's Critical Security Controls (CIS Controls), version 8, as our criteria to assess the governments' IT security programs and identify areas that could be strengthened.

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, when applied together, form a layered defense of best practices – also called "defense-in-depth" – to 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:

1. Implementing the safeguard
2. As applicable, maintaining documentation to support the safeguard, such as policies or procedures

Work on internal controls

These audits assed the design and tested the effectiveness of limited the IT security internal controls at the selected governments. We used a selection of safeguards from the CIS Controls as the internal control framework for the assessment. Based on an initial assessment, we selected around 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: Objectives, Scope and Methodology – Critical Infrastructure

Objectives

To help the selected local governments with critical infrastructure protect their IT systems and secure the data they need to operate, we conducted performance audits designed to identify opportunities to improve IT security. These audits answered the following question:

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

Scope

These audits identified opportunities for 39 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, or drinking water and wastewater services. In this fiscal year, these audits focused primarily on governments providing water and wastewater services because safe drinking water is a prerequisite for protecting public health and all human activity. We also prioritized government selection based on a variety of factors, but primarily on the number of customers they serve. All 39 governments volunteered to participate in the audit.

These audits tested the effectiveness of external IT security controls using penetration testing to assess if there were opportunities to make them more secure. The audits 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. These audits did not assess the documentation associated with these internal controls or the governments' alignment with federal or state special data-handling laws or requirements.

Methodology

To answer the audit objectives, we conducted penetration testing on each local government's internet-facing systems, assessed external-facing firewall configurations, and also conducted interviews with key IT management and staff regarding their IT and IT security processes and controls.

External penetration testing and external firewall reviews

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 February 2024 and May 2025. Our staff assessed external-facing firewall configurations to identify potential areas for additional hardening, which could block or otherwise thwart an attack.

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. After each interview, we gave the government detailed recommendations tailored to its specific IT environment. 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 December 2023 and April 2025 by State Auditor's Office cybersecurity auditors and cybersecurity specialists.

Work on internal controls

These audits reviewed the design and tested the effectiveness of limited IT security internal controls at 39 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.** 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.**
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. 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: Objectives, Scope and Methodology – Ransomware Resiliency

Objectives

To help the selected local governments protect their IT systems and secure the data they need to operate, we conducted performance audits designed to identify opportunities to improve resiliency to ransomware attacks and promote IT security. These audits answered the following question:

- Can selected local governments make their IT systems more secure and better align with leading practices that contribute to ransomware attack resiliency?

Scope

These audits identified opportunities for six local governments to improve their resiliency to ransomware attacks. All six governments volunteered for the audits. We examined five control areas that apply to distinct facets of ransomware prevention, detection and response. These key IT security controls were identified by our IT security subject matter experts based on leading practices set out in the #StopRansomware Guide developed through the Joint Ransomware Task Force (JRTF).

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, nor did it address security safeguards outside the direct scope of ransomware prevention, detection and recovery.

Methodology

To answer the audit objectives, we conducted limited technical testing on the local governments' networks and compared implementation of IT security controls to selected leading practices.

Technical testing

To determine if the local governments could make their IT systems more secure, we tested selected key systems and networks for vulnerabilities in their IT environments. For example, we assessed external security controls that included analyzing email security settings, internet-facing firewall configurations for common misconfigurations, and external server communications protocols. Internal security tests included performing vulnerability scans on IT assets to identify missing patches, out-of-date software or operating system components, and to determine the level of hardening that has been configured on a sample of Windows devices.

Interviews with IT management and staff

To determine whether the government's IT security practices could better align with leading practices concerning ransomware resiliency, we interviewed key IT staff, observed security practices and settings, and conducted limited technical analysis of IT systems.

We used a set of 22 ransomware resiliency leading practice safeguards identified by the State Auditor's Office's cybersecurity specialists as our criteria to assess resiliency to ransomware and to identify areas that could be strengthened. The five control areas these 22 safeguards fall into include:

- General network security
- Preparations to speed recovery from an attack
- Securing internet-facing systems
- Preventing phishing and other social engineering attacks
- Protection from malware

The set of 22 safeguards developed by our Office was primarily based on the #StopRansomware Guide developed through JRTF. This task force is composed of members from Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC). This interagency collaborative effort works to reduce the prevalence and impact of ransomware attacks. The JRTF published #StopRansomware to help organizations reduce the risk of ransomware incidents through best practices to detect, prevent, respond to and recover from ransomware, including step-by-step approaches to address potential attacks.

This work was performed between April 2024 and April 2025 by State Auditor's Office cybersecurity auditors and cybersecurity specialists.

Work on internal controls

These audits assessed the design and tested the effectiveness of limited IT security internal controls at six selected local governments. We used a set of 22 safeguards developed by our Office as the internal control framework for the assessment. We completed our assessment for the purpose of identifying opportunities for the local government to improve its internal IT security controls and protect against ransomware, but not to provide assurance on its 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 was not designed to 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.**
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 evaluated the roles and functions of IT security and made recommendations to align them with leading practices.
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 made recommendations to improve IT security based on the best practices identified by our subject matter experts and cybersecurity specialists.

Appendix D: 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-it-audits/

Our website also features special reports summarizing our cybersecurity audit findings, including:

- *Cybersecurity Special Report 2024: Roundup of fiscal year 2024 audits and other work*
- *Cybersecurity Special Report 2023: Roundup of 2022 audits and other work*
- *Cybersecurity Special Report 2022: Keeping an independent eye on government IT security*

Read our 2024 rollup report on local government cybersecurity audits: *Opportunities to Improve IT Security at Local Governments Fiscal Year 2024*.

Read our 2024 rollup report on state government cybersecurity audits: *Opportunities to Improve State Information Technology Security 2024.*

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.

"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
Pat McCarthy