

# PERFORMANCE AUDIT



Office of the  
Washington  
State Auditor  
Pat McCarthy

## Opportunities to Improve State Information Security – FY 2025

September 8, 2025

Report Number: 1038032

# Table of Contents

About the Audit	3
Audit Results	5
State Auditor's Remarks	6
Recommendations	7
Agency Response	8
Appendix A: Initiative 900 and Auditing Standards	10
Appendix B: Objectives, Scope and Methodology	12
Appendix C: Other Cybersecurity Audit Work	14

## State Auditor's Office contacts

### State Auditor Pat McCarthy

564-999-0801, [Pat.McCarthy@sao.wa.gov](mailto:Pat.McCarthy@sao.wa.gov)

### Scott Frank – Director of Performance and IT Audit

564-999-0809, [Scott.Frank@sao.wa.gov](mailto:Scott.Frank@sao.wa.gov)

### Peg Bodin, CISA – Assistant Director for IT Audit

564-999-0965, [Peggy.Bodin@sao.wa.gov](mailto:Peggy.Bodin@sao.wa.gov)

### Erin Laska – IT Security Audit Manager

564-999-0615, [Erin.Laska@sao.wa.gov](mailto:Erin.Laska@sao.wa.gov)

### Joseph Clark – IT Security Assistant Audit Manager

564-999-0968, [Joseph.Clark@sao.wa.gov](mailto:Joseph.Clark@sao.wa.gov)

### Kathleen Cooper – Director of Communications

564-999-0800, [Kathleen.Cooper@sao.wa.gov](mailto:Kathleen.Cooper@sao.wa.gov)

## To request public records

### Public Records Officer

564-999-0918, [PublicRecords@sao.wa.gov](mailto: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](mailto:Webmaster@sao.wa.gov) for more information.

# About the Audit

## Washington state agencies must protect the IT systems they rely on to deliver critical government services to their residents

People depend on Washington's state agencies for many different services, from public safety and tax collection to social services and transportation systems. These agencies in turn depend on information technology (IT) systems to help them deliver these services. The security of IT systems and related data underpins the stability of government operations, and the safety and well-being of residents. Protecting these systems is critical to maintaining public confidence in the state.

These IT systems also process and store confidential data. Aside from the loss of public confidence, a data breach involving such data can present the agency with considerable tangible costs. These include identifying and repairing damaged systems as well as 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.

## In fiscal year 2025, our audits looked for opportunities to improve the IT security at seven state agencies

To help the selected state agencies 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 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. These point-in-time security assessments identified and assessed vulnerabilities that attackers could exploit on internal or external systems.

## Comparing agencies' IT security programs to leading practices

We compared the seven agencies' IT security practices and as applicable the associated policies and procedures, to selected leading practices to identify any improvements that could make them stronger. We selected the practices from the Center for Internet Security's Critical Security 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 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 (<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. 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 to each agency's IT staff as we completed them. We also gave each agency's management recommendations for its review, response and action. While each agency had some good IT security practices in place, we identified opportunities to make IT systems more secure. 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 (GAGAS), sections 9.61-9.67.

# State Auditor's Remarks

The Office of the Washington State Auditor 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 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.

# Recommendations

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

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

# Agency Response

BOB FERGUSON  
Governor



WILLIAM S. KEHOE  
Director &  
State Chief Information Officer

STATE OF WASHINGTON

## WASHINGTON TECHNOLOGY SOLUTIONS

1500 Jefferson Street SE • Olympia, Washington 98504-1501

August 29, 2025

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

Dear Auditor McCarthy:

On behalf of Washington Technology Solutions (WaTech) and 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 Security, FY 2025."

WaTech and our partner agencies appreciate the SAO's continued leadership in identifying opportunities to strengthen the state's information security posture. Protecting Washington's critical information systems and the confidential data they hold is fundamental to public trust. We recognize and agree with the recommendations in this year's report. State agencies have already taken steps to remediate identified vulnerabilities and assess and mature their security needs and resources to meet evolving threats.

WaTech is driving key initiatives to boost cybersecurity across the state. These efforts include expanding enterprise-wide monitoring for real-time threat detection, strengthening incident response and training for state agencies, modernizing policies to align with national security standards, and collaborating with local governments while leveraging federal grants to build stronger collective defenses.

As the audit highlights, cybersecurity requires continuous attention. WaTech remains committed to working closely with the SAO, the Office of the Governor, the Office of Financial Management, and all state agencies to ensure ongoing improvements. Thank you again for your thoughtful report and partnership.

Sincerely,

William S. Kehoe  
Director and State Chief Information Officer  
Washington Technology Solutions

cc: Shane Esquibel, Chief Operations Officer, Office of the Governor  
Franklin Plaistowe, Deputy Chief Operations Officer, Office of the Governor  
Kenneth Martin, Policy Director, Office of the Governor  
Debbie Driver, Legislative Director, Office of the Governor  
Jesse Jones, 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 SECURITY, FY 2025

---

AUG. 29, 2025

This management response to the State Auditor's Office (SAO) performance audit report received August 12, 2025, 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 recommended the audited agencies:

1. Continue remediating vulnerabilities identified during the security testing, starting with those most significantly affecting them.
  2. Revise IT security policies, procedures and practices to align more closely with leading practices.
  3. 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 to improve recommended by the SAO to help protect agency systems and data. We take our duty to continue improving state government security seriously and will continue to do so. We have already implemented improvements and will continue to remediate any remaining vulnerabilities. We will continue to periodically assess and improve IT security needs.

Washington Technology Solutions will continue using the SAO's findings and observations of this and previous audits to improve the state's security posture across all state organizations.

### Action Steps and Time Frame

- Each audited entity will work with its appropriate governing bodies to address and prioritize vulnerabilities, improvements, and considerations suggested by the SAO during its' fiscal year 2025 performance audit.

# Appendix A: Initiative 900 and Auditing Standards

## Initiative 900 requirements

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Results and Recommendations sections of this report.

I-900 element	Addressed in the audit
1. Identify cost savings	<b>No.</b> The audits did not identify measurable cost savings. However, strengthening IT security could help agencies avoid or mitigate costs associated with a data breach or security incident
2. Identify services that can be reduced or eliminated	<b>No.</b>
3. Identify programs or services that can be transferred to the private sector	<b>No.</b> 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	<b>No.</b>
5. Assess feasibility of pooling information technology systems within the department	<b>No.</b>

I-900 element	Addressed in the audit
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	<b>Yes.</b> 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	<b>No.</b>
8. Analyze departmental performance data, performance measures and self-assessment systems	<b>Yes.</b> 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	<b>Yes.</b> 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 as published in *Government Auditing Standards* (July 2018 revision) issued by the U.S. Government Accountability Office. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## The mission of the Office of the Washington State Auditor

To provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective. The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic [subscription service](#). We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program. For more information about the State Auditor's Office, visit [www.sao.wa.gov](http://www.sao.wa.gov).

# Appendix B: Objectives, Scope and Methodology

## Objectives

To help the selected state agencies 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 agencies make their IT systems more secure, and better align their IT security practices with leading practices?

## Scope

These audits identified opportunities for seven state agencies to improve their IT security. The audits assessed the extent to which these agencies' IT security programs, including their implementation and, as applicable, documentation, aligned with selected CIS Controls. The audit also 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 agencies' alignment with federal or state special data-handling laws or requirements.

## 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 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 May 2024 and May 2025. 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, observed agency security practices and settings, conducted limited technical analysis of agency systems, and, as applicable, reviewed agency IT security policies and procedures. This work was completed at the seven agencies between December 2023 and April 2025.

We used selected controls from the Center for Internet Security Critical Security Controls (CIS Controls), version 8, as our criteria to assess the IT security programs at the seven state agencies to identify areas that could be made stronger.

CIS is a nonprofit organization focused on securing public and private organizations against cyber threats. The CIS Controls, 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 agency against selected safeguards to determine alignment with those safeguards. We did this by assessing the extent to which each agency met each safeguard in two areas:

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

## Work on internal controls

These audits assessed the design and tested the effectiveness of limited the IT security internal controls at seven state agencies. 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 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 agency to improve its internal IT security controls, but not to provide assurance on the agencies' 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. 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/](https://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 state government cybersecurity audits: [\*Opportunities to Improve State Information Technology Security 2024.\*](#)

Read our 2024 rollup report on local government cybersecurity audits: [\*Opportunities to Improve IT Security at Local Governments Fiscal Year 2024.\*](#)

## Earlier state cybersecurity audits

[\*Opportunities to Improve State Information Technology Security 2022\*](#)

[\*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 \(issued 2014\)\*](#)



"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](http://www.sao.wa.gov)

**1-564-999-0950**



Office of the Washington State Auditor  
Pat McCarthy