

JAY INSLEE  
Governor



WILLIAM S. KEHOE  
Director &  
State Chief Information Officer

STATE OF WASHINGTON

WASHINGTON TECHNOLOGY SOLUTIONS

1500 Jefferson Street SE • Olympia, Washington 98504-1501

January 18, 2023

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

Dear Auditor McCarthy:

On behalf of the audited participants, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report "Opportunities to Improve State Information Technology Security – 2022."

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

We must vigilantly continue to strengthen protections of state government systems and data. We appreciate the SAO continuing to identify opportunities to help us do so.

Please thank your team for their collaborative approach throughout this performance audit. We continue to welcome the SAO's observations and recommendations of what to improve.

Sincerely,

A handwritten signature in cursive script, appearing to read "William S. Kehoe".

William S. Kehoe  
Director & State Chief Information Officer

cc: Jamila Thomas, Chief of Staff, Office of the Governor  
Kelly Wicker, Deputy Chief of Staff, Office of the Governor  
Nick Streuli, Executive Director of Policy and Outreach, Office of the Governor  
David Schumacher, Director, Office of Financial Management  
Mandeep Kaundal, Director, Results Washington, Office of the Governor  
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor  
Ralph Johnson, State Chief Information Security Officer, Washington Technology Solutions  
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor

This management response to the State Auditor’s Office (SAO) performance audit report received December 19, 2022, is coordinated by the State’s Chief Information Officer on behalf of the audited entities.

---

**SAO PERFORMANCE AUDIT OBJECTIVES:**

The SAO sought to answer this question:

1. Can selected agencies make their IT systems more secure, and better align their IT security practices with leading practices?

---

**SAO Recommendations to the selected state agencies:** to protect agency IT systems and the information contained in them, we recommend:

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

**STATE RESPONSE:**

We agree with the opportunities for improvement identified by the SAO to help protect agency systems and data. We also recognize our responsibility to continue improving state government security and take that duty seriously. As noted in the report, audited agencies have already implemented improvements and will continue to remediate any remaining vulnerabilities. The agencies will also continue to assess and make improvements to IT security needs – including further alignment with leading practices recommended in the CIS controls where appropriate. These controls are more prescriptive than the OCIO IT security standards 141.10 that agencies are required to follow.

The OCIO will use the SAO’s findings and observations of this and previous audits to work with all state organizations to better improve the state’s security posture.

**Action Steps and Time Frame**

- Each audited entity will continue to work with their appropriate governing bodies to address and prioritize vulnerabilities, improvements and considerations suggested by the SAO during calendar year 2023 and beyond.