

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

December 13, 2021

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 "Continuing Opportunities to Improve State IT Security – 2021."

We appreciate the report recognizing state government auditees' dedication to making government work better.

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
Keith Phillips, Director of Policy, Office of the Governor
David Schumacher, Director, Office of Financial Management
Christine Bezanson, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
Vinod Brahmapuram, 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 CONTINUING OPPORTUNITIES TO IMPROVE STATE IT SECURITY – 2021 **DEC. 13, 2021**

This management response to the State Auditor’s Office (SAO) performance audit report received November 29, 2021, 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 systems and the information within those systems, we recommend the six audited agencies:

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.
3. In addition, we recommend the five agencies whose IT security practices we reviewed further align their IT security programs with leading practices recommended in the CIS controls.

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. 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 work with their appropriate governing bodies to address and prioritize vulnerabilities, improvements and considerations suggested by the SAO during calendar year 2022.