JAY INSLEE
Governor

Rob St. John
Acting Director & State Chief
Information Officer

STATE OF WASHINGTON

WASHINGTON TECHNOLOGY SOLUTIONS

1500 Jefferson Street SE • Olympia, Washington 98504-1501 • (360) 407-8700

March 15, 2018

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

Dear Auditor McCarthy:

On behalf of the audited agencies, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report Continuing Opportunities to Improve State Information Technology Security – 2017.

We appreciate the report's recognition of the significant measures agencies have taken to protect their information technology systems from risk. We agree that opportunities exist to continue to strengthen our security and will continue to do so.

We also appreciate the collaborative approach your staff exercised throughout this performance audit to protect the IT security of our state. Please extend our thanks to them.

Sincerely,

Rob St. John
Acting Director and State Chief Information Officer

cc: David Postman, 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
Inger Brinck, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor

OFFICIAL STATE CABINET AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON CONTINUING OPPORTUNITIES TO IMPROVE STATE IT SECURITY – 2017 MAR. 15, 2018

This management response to the State Auditor's Office (SAO) performance audit report received Feb. 22, 2018, is provided by the acting Director of Washington Technology Solutions and State Chief Information Officer on behalf of the audited agencies.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO sought to determine if there were opportunities to strengthen IT security controls at three state agencies through these questions:

1. Are selected state agencies adequately protecting their confidential information from external and internal threats?
2. Are their security practices aligned with select critical security controls and compliant with related state IT security standards?

SAO Issue 1: Opportunities exist to strengthen IT security.

SAO Recommendations 1-3: The three audited agencies should:

- Continue remediating issues identified during the security testing.
- Continue remediating gaps identified between agency practices or documented policies and procedures and the state's IT security standards and industry leading practices.
- Continue periodically assessing 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 to strengthen IT security by the SAO. The audited agencies will continue to work diligently to remediate the issues identified during testing and the gaps identified between agency practices or documented policies and procedures and the state's IT security standards. Agencies are committed to ongoing assessment of IT security needs.

Action Steps and Time Frame

- Each audited agency will establish a plan to address the gaps and improvements identified. These plans will be monitored over time by the SAO and the audited agency security staff. *By May 31, 2018.*

SAO Recommendation 4: To the state's Office of Cyber Security (OCS): Continue to conduct outreach to state agencies to determine how additional clarity or guidance could help agencies

identify detailed controls to incorporate into their policies and procedures, and help them align agency practices with the state IT security standards.

STATE RESPONSE:
The state Office of Cyber Security will continue to encourage agencies to participate in OCS provided monthly technical and policy training sessions and weekly open office hours to address security questions and/or issues.

Action Steps and Time Frame

- OCS will send monthly training notifications to a broader audience. *By May, 31 2018.*

SAO Recommendation 5: To the state's Office of Cyber Security: Continue to develop and provide that additional clarity or guidance to state agencies.

STATE RESPONSE:
The state Office of Cyber Security will continue to encourage agencies to participate in OCS provided monthly technical and policy training sessions and weekly open office hours to address security questions and/or issues.

Action Steps and Time Frame

- OCS will send monthly training notifications to a broader audience. *By May 31, 2018.*
