OFFICIAL STATE CABINET AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON CONTINUING OPPORTUNITIES TO IMPROVE STATE IT SECURITY – 2016 NOV. 1, 2016

This management response to the State Auditor's Office (SAO) performance audit report received Oct. 11, 2016, is provided by the state's Chief Information Officer on behalf of Washington Technology Solutions (WaTech) and 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 these state agencies adequately protecting their confidential information from external and internal threats?
2. Are their security programs aligned with select IT security leading practices?

SAO Issue 1: Opportunities exist to strengthen IT security.

SAO Recommendation 1: The audited agencies should continue remediating issues identified during security assessment testing and gaps identified between agency practices or documented policies and procedures and the leading practices. They should continue to assess agency's IT security needs and resources periodically, including personnel and technology, to mature and maintain sufficient security.

STATE RESPONSE:
We agree with the opportunities for improvement identified by the SAO. Agencies will continue to work diligently to remediate the issues identified between agency practices or documented policies and procedures and the leading practices. Agencies have an ongoing commitment to assess IT security needs.

Action Steps and Time Frame

- Each agency will establish a plan for the gaps and improvements identified by the end of the year. These plans will be monitored by the SAO and WaTech. *By Dec. 31, 2016.*

SAO Recommendation 2: To WaTech, to help ensure agencies can effectively plan and budget to make full use of WaTech's services:

- Solicit input from state agencies when procuring new services
- Provide details about new services to state agencies as early as possible. Service specifications should be set out in "terms of service" or similar document; key specifications to consider covering include limitations roles and responsibilities, performance measures, and security of the service.

STATE RESPONSE:
The State's Chief Information Officer (CIO) agrees that agencies should be aware of and involved in the exploration and needs of WaTech services that can be leveraged by agencies to fulfill their missions in government. A full understanding of WaTech's services can inform agencies in the development of their technology strategic plans and budgets. Terms of Service or service level agreements should provide clarity in roles and responsibilities, performance measures, security, and limitations when known.

WaTech will review and update Terms of Service to include more clarity in roles and responsibilities, performance, security and known limitations. This effort is already underway and will be ongoing as new Terms of Service and Service Level Agreements are entered.

WaTech implemented the *Service Catalog Process* to maintain the WaTech service catalog, or list of current services, effective December 2015. The planning for new WaTech services includes review with customers seeking input on those services. WaTech seeks input from customers through multiple methods including the Watech Advisory Council, the CIO Forum, Quarterly Customer meetings and through interactions with customers on an individual basis. WaTech publishes updates to the Service Catalog on the WaTech website and on the WaTech Strategic Roadmap.

Action Steps and Time Frame

- Update the Terms of Service to include more clarity in roles and responsibilities, performance, security and known limitations. *By September 30, 2017.*
- Implement a Service Catalog Process that includes a Customer Advisory Council. *Complete.*

SAO Recommendation 3: To WaTech's Cyber Security Office:

- Conduct outreach to state agencies to determine how additional clarity or guidance could help align practices with the state IT security standards and leading practices
- Develop and provide that additional clarity or guidance to state agencies

STATE RESPONSE:
The State Office of Cyber Security agrees that agencies would benefit from additional clarity and guidance on how agency security controls and procedures could better align with state IT security standards leading best practices. Proper interpretation and application of effective IT security standards and controls has become increasingly important as the IT security threat landscape continues to change and agencies move more critical business applications to the cloud.

- The State Office of Cyber Security has already begun taking action to provide agencies with additional information on emerging IT security threats, guidance on how state IT security standards and best practices can most effectively be applied and training resources to help them protect their most critical IT assets:

    - Monthly Workshops: Every month, the State Office of Cyber Security hosts IT Security workshops. In these sessions, IT security industry experts and Office of Cyber Security

staff members provide agencies with information on new and emerging threats, technical implementations and interpretation of the state's IT security standards. These workshops also serve as a forum where agency IT security professionals can raise questions, share their successes and learn from one another. These workshops commenced in March, 2016.

- Weekly "Office Hours": The State Office of Cyber Security has set aside several hours per week to provide agencies with the opportunity to drop by and interact with staff to discuss any questions they may have regarding IT Security standards compliance, implementation of best practices, threat detection and analysis and other IT security-related questions. The Office Hours program was implemented in September 2016. Employee IT Security Awareness Training: In an effort to continually raise the state's overall security posture, the State Office of Cyber Security is in the process of contracting with a second firm to provide online employee IT security awareness training. As a result, agencies will have the option of using one of two curriculums to satisfy annual training requirements for their employees. This training, made available at no cost to agencies, allows all state employees to receive up-to-date instruction on what they can do to protect their work environment from exposure to commonly used threat tactics. The contracted is expected to be executed, and training in place, by December 31, 2016.

Action Steps and Time Frame

- Establish monthly workshops to provide agencies with information on new and emerging threats, technical implementations and interpretation of the state's IT security standards. *Complete.*
- Establish weekly Office Hours" for agencies. *Complete.*
- Contract with a second firm to provide online employee IT security awareness training. *By December 31, 2016.*