Cabinet and Governor Appointed Agencies' Performance Audit Action Item(s) & Status

Continuing Opportunities to Improve State IT Security – 2018

(See also cabinet agency response for full context to Washington State Auditor's Office (SAO) report, December, 2018)

Three state agencies were included for this performance audit. Information also was provided by Washington Technology Solutions (WaTech).

SAO Recommendations (Rec) to the three audited agencies:

1. Continue remediating issues identified during security testing
2. Continue remediating gaps between agency IT security implementation or written policies and the procedures and the state's IT security standards
3. Consider also further aligning agency IT security controls with leading practices recommended in Critical Security Controls #1 through #5 and #11
4. Continue periodically assessing IT needs and resources, including personnel and technology, to develop and maintain sufficient IT security

SAO Recommendations (Rec) to the Office of Cyber Security (OCS) within WaTech:

5. Continue to reach out to state agencies to identify what information would help agencies:
    a. Incorporate detailed controls into their policies and procedures
    b. Align agency practices with the state IT security standards
6. Continue to develop and provide that additional clarity or guidance to state agencies
7. Continue to assess resources to better assist agencies in developing and implementing their IT security programs

The table below shows the current status of action items the agency initiated to address issues identified in the performance audit report. Please see the *cabinet agency response* for additional context and any additional steps already taken.

For an explanation of the columns below, see the legend.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources?	Budget Impact?	Legislation Required?	Notes
Rec. 1-4	Complete	Each audited agency will establish a timeline to address the gaps, improvements and considerations identified	1-3	3/19	Yes	No	No	
Rec. 5-7	Complete	OCS will survey state agencies and analyze the information collected to focus its education efforts	WaTech	~~3/19~~ complete	Yes	No	No	**July 2019:** The new state Chief Information Security Officer (CISO), has worked with federal partners to allow Washington state and local government agencies to participate in the Nationwide Cybersecurity Review (NCSR) survey. This is a comprehensive, nationally-recognized survey that measures

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources?	Budget Impact?	Legislation Required?	Notes
								agency IT security gaps and capabilities. In addition to providing results at the agency level, this online survey will allow OCS to conduct a roll-up of all agency results, providing a high-level view of state cyber maturity. The result of the initial survey will be used as a baseline to measure security maturity going forward. The window for participation in this nationally-administered survey opens in October 2019. **August 2020:** The new State Chief Information Security Officer (CISO) has re-energized the CISO council in addition to the weekly calls for the outreach required to identify and help agencies with information to ensure their continued success. **August 2021**: This is ongoing work within OCS.
Rec. 5-7	Complete	OCS will use the survey information during its ongoing outreach in order to help agencies incorporate detailed controls into their policies and procedures, and align agency practices with the state IT security standards	WaTech	complete	Yes	No	No	**July 2019:** The results of the NCSR survey (above) will provide OCS with actionable data to be used to help OCS focus its education efforts and help agencies incorporate detailed controls into their policies and procedures. **August 2020:** To align agency practices with State IT security standards and to ensure the necessary clarity, the new State Chief Information Security Officer (CISO) has developed an operating model that provides the necessary guidance to state agencies. This operating model has received positive feedback from agencies and is currently in the process of implementation. **August 2021**: This is ongoing work within OCS.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources?	Budget Impact?	Legislation Required?	Notes
Rec. 5-7	Complete	OCS will prepare explanatory handouts and continue to develop and provide that additional clarity or guidance to state agencies	WaTech	Complete	Yes	No	No	**July 2019:** This is an ongoing effort. In addition to continuing to provide agencies with needed clarity and guidance, OCS will be enhancing its National Cyber Security Awareness month "Hacktober" activities to further educate and engage agencies to provide clarity and guidance. **August 2020:** The State Chief Information Security Officer conducted multiple presentations and is also creating an agency engagement plan and organization transformation plan as part of the security strategy to meet this objective. **August 2021**: This is ongoing work within OCS.
Rec. 5-7	Complete	OCS will continue to assess resources to better assist agencies in developing and implementing their IT security programs	WaTech	Complete	Yes	No	No	**July 2019:** This is an on-going effort. The state CISO is currently in the process of chartering an agency CISO council to facilitate the exchange of IT security information and best practices with the goal of improving the overall security posture of the state. **August 2020:** With appointment of the state CISO, Vinod Brahmapuram, in October 2019, OCS has taken significant steps to buildout the CISO Council to develop cohesion between OCS and state agency CISOs. This has led to a much better understanding of what agencies need and how OCS can help them meet their security program objectives. The State CISO has also developed an operational plan to develop the essential resources to better assist agencies in

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources?	Budget Impact?	Legislation Required?	Notes
								developing and implementing their IT security program. **August 2021**: This is ongoing work within OCS.