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

Opportunities to Improve State IT Security

(See also cabinet agency response for full context to Washington State Auditor's Office (SAO) report, December 2014)

Washington Technology Solutions (WaTech) will work with audited agencies to complete the action plan prepared in response to the performance audit. Note: At the time of the performance audit, the State Auditor's Office worked with the Office of the Chief Information Officer (OCIO) and Consolidated Technology Services (CTS) to conduct the audit. These agencies merged into WaTech on July 1, 2015.

SAO Findings Summary:

1. Opportunities exist for Washington to further protect the confidential information entrusted to the state by improving IT security.
2. While the state's IT security standards align closely with leading practices, improvements could be made.
3. Selected agencies are not in full compliance with state IT security standards.
4. Application security testing identified security issues.
5. Agencies reported several barriers to fully complying with state IT security standards.
6. The state's process to monitor agency IT security compliance could be improved.

SAO Recommendations (Rec):

1. The audited agencies should continue remediating gaps identified where agency practices or documented policies are not in full compliance with the state's IT security standards, and weaknesses identified through our application security testing.
2. The audited agencies provide accurate and complete information on agency compliance with, and deviations from, the state's IT security standards in the agency's annual verification letter to the OCIO.
3. The state's Chief Information Officer revise the state's IT security standards to more closely align with leading practices, and clarify those where our review found multiple agencies did not comply.
4. The state's Chief Information Officer evaluate and revise the current process used for agencies to annually report the status of their compliance with, and deviations from, the state's IT security standards to ensure the process provides meaningful and accurate information. While doing so, evaluate what is needed to help agencies understand how to technically comply with the standards and to monitor annual agency compliance.
5. The state's Chief Information Officer continue to collaborate with the state's Chief Information Security Officer (CISO) to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.
6. The state's CISO continue to collaborate with the OCIO to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

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
1	Complete	Agencies will continue to work diligently to remediate gaps and improve both practices and documentation.	WaTech	12/15	Yes	No	No	**July 2016:** Agencies have remediated gaps identified in the performance audit, and have improved practices and documentation as a result.
2	Complete	Agencies will provide complete and accurate IT security compliance information to the OCIO in their annual verification letters by the next annual reporting date.	WaTech	Ongoing to 8/20	Yes	No	No	**July 2018:** This is a continual work in progress. WaTech did see improvement in the quality of agencies' last annual attestations, but does not have the staffing resources to independently attest that they are truly "complete and accurate". To help address this, WaTech has added an additional FTE to review agency attestations, follow-up on mitigation status of non-compliant conditions identified, and help agencies better identify, and report on, those conditions needing improvement. **July 2019**: The office continues to closely monitor agencies for compliance to OCIO Standard 141.10. However, over time, it has become clear that, in addition to maintaining compliance to published standards, agencies must take a more risk-based approach to IT security to appropriately address evolving threats before they can be codified in a published standard. Therefore, in 2019, in lieu of providing annual compliance information, agencies will be asked to complete a Nationwide Cybersecurity Review survey. The results of this survey will provide insight on the level of maturity and risk awareness at both the agency level and

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact?	Legislation Required?	Notes
								the state enterprise as a whole. This information will be used to target the state's largest risks, and will be used as a baseline to measure agency risk awareness and security maturity moving forward. **August 2020:** In lieu of providing compliance information, WaTech continues to require agencies to complete a Nationwide Cybersecurity Review Survey in 2020 as was done in 2019. This approach has proved beneficial to meet the intended objective of this issue especially since this survey provides actionable feedback and metrics to the participating agencies using a nationally approved standard for measurement.
3	Complete	The OCIO will incorporate the additional national best practices identified in the report into the OCIO standards and clarify those sections of the standards where it was found that multiple agencies did not comply.	WaTech	On-going to 8/20	Yes	No	No	**July 2018:** Several of these areas were addressed in the latest revision of the OCIO IT Security Standards adopted by the Technology Services Board in November 2017. WaTech will continue to iteratively address these areas in subsequent revisions to the Standards. **July 2019:** National best practices have continued to evolve and coalesce since the time this audit report was published. The nationally recognized measure of cybersecurity maturity and readiness for organizations is now the Cyber Security Framework (CSF), which incorporates the national best practices identified in this audit. The office will intentionally be encouraging agencies to adopt the CSF,

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact?	Legislation Required?	Notes
								which will be used to augment the OCIO standards to reduce risk. **August 2020**: WaTech has incorporated best practices identified in this 2014 performance audit into the state's existing security standards to the degree they conform to the state's IT security architecture. To address existing and emerging threats and risks going forward, WaTech, with guidance from the state IT security community, intends to adopt new standards. As such, further incorporation of best practices into the existing standards will discontinue, and this 2014 recommendation is considered "Complete".
4	Complete	Beginning in January 2015, the OCIO will work with agencies to better understand how the reporting process can be improved to solicit more accurate, meaningful information, and how they might better monitor compliance to the standards. Also, realizing that agencies often rely on the results of required 3- year independent audits to determine their compliance status, the OCIO will review the audit standard currently used by agencies to determine if these should be enhanced to provide more in-	WaTech	~~6/16~~ ~~3/17~~ 12/17	No	Yes	No	**July 2018:** Since the completion of the "Opportunities to Improve State IT Security" performance audit in December 2014, WaTech, has worked with the State Auditor's Office to understand how required 3-year security audits could provide better, more actionable feedback to both audited agencies and the WaTech compliance team. These auditing standards have been revised, and SAO now provides agencies with auditing options at various levels of detail to provide a better assessment of their compliance status. The ability of WaTech to responsibly monitor and enforce the expected increase in more accurate compliance information has been

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact?	Legislation Required?	Notes
		depth, operational information that can be used by agencies to enhance their security posture and provide more accurate compliance information to the OCIO.						addressed by the addition of a FTE to perform these duties (see #2 above).
5	Complete	The state's CISO, though a member of Consolidated Technology Services, currently reports to the CIO through a dotted-line relationship. The CIO and CISO meet on a regularly scheduled basis, and the CISO is in contact with OCIO staff on a near-daily basis. Also, as mentioned in the auditor's report, legislation is being drafted to merge the OCIO, CTS and parts of DES. This will strengthen the reporting relationship between the CIO and CISO, and bring greater cohesion between the policy and operational aspects of IT security.	WaTech	07/01 /2015	Yes	No	No	**October 2015:** The passage of ESSB 5315 required the consolidation of the Office of the Chief Information Officer with the Consolidated Technology Services agency (WaTech). As a result of this, the IT security policy and standards functions have been moved under the state Chief Information Security Officer, strengthening the reporting relationship between the CIO and CISO. This has resulted in greater cohesion between the policy and operational aspects of IT security.
6	Complete	The CISO and CIO meet on a regularly scheduled basis, and the CISO is in contact with OCIO staff on a near-daily basis. As the OCIO incorporates the additional national best practices identified in the report into the OCIO IT standards, the CISO with work with the CIO to	WaTech	07/01 /2015	Yes	No	No	**October 2015:** Please see note for Issue 5 above. The passage of ESSB 5315 has resulted in closer, more frequent contact with, and discussion between, the state CIO and state CISO. This has allowed the CISO to work more closely with the CIO to provide guidance on how agencies can consistently implement the security controls identified in the security standards.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact?	Legislation Required?	Notes
		provide guidance on how agencies can consistently implement the security controls identified in the updated security standards.						