Official State Agency Response to the Performance Audit on Opportunities to Improve State IT Security Dec. 12, 2014

This management response to the State Auditor's Office (SAO) performance audit report received Dec. 1, 2014, is provided by the Office of the Chief Information Officer (OCIO) on behalf of Consolidated Technology Services (CTS) and the audited agencies.

SAO Performance Audit Objectives:

The SAO sought to answer these questions:

1. Do the state's IT security standards align with leading practices?
2. Are selected state agencies in compliance with the state's IT security standards?
3. Are those agencies adequately protecting confidential information?

SAO Issue 1: Opportunities exist for Washington to further protect the confidential information entrusted to the state by improving IT security.

SAO Issue 2: While the state's IT security standards align closely with leading practices, improvements could be made.

SAO Issue 3: Selected agencies are not in full compliance with state IT security standards.

SAO Issue 4: Application security testing identified security issues.

SAO Issue 5: Agencies reported several barriers to fully complying with state IT security standards.

SAO Issue 6: The state's process to monitor agency IT security compliance could be improved.

SAO Recommendation 1: The five 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.

STATE RESPONSE:
We agree with the opportunities for improvement identified by the SAO.

Action Steps and Time Frame

- Agencies will continue to work diligently to remediate gaps and improve both practices and documentation. Ongoing. .

SAO Recommendation 2: The five 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 Office of the Chief Information Officer.

STATE RESPONSE:

The selected agencies concur with the SAO recommendation to provide the OCIO complete and accurate information in their annual verification letters.

Action Steps and Time Frame

- Agencies will provide complete and accurate IT security compliance information to the OCIO in their annual verification letters by the next annual reporting date, which is August 31, 2015.

SAO Recommendation 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.

STATE RESPONSE:
While we recognize that the report found no significant gaps in the state's IT standards, the OCIO is committed to continually updating these standards to ensure they are consistent with national standards and address emerging cyber threats. The standards have been updated several times in the past two years to provide relevance and clarity, and we agree that further updates are necessary to more completely align the standards with national best practices and clarify the intent and purpose for agencies.

Action Steps and Time Frame

- 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 by June 30, 2015.

SAO Recommendation 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.

STATE RESPONSE:
The OCIO agrees with the opportunities for improvement identified by the SAO

Action Steps and Time Frame

- 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-depth, operational information that can be used by agencies to enhance their security posture and provide more accurate compliance information to the OCIO.

SAO Recommendation 5: The state's Chief Information Officer continue to collaborate with the state's Chief Information Security Officer 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.

STATE RESPONSE:
The state's Chief Information Officer (CIO) agrees that continued input from, and collaboration with, the state's Chief Information Security Officer (CISO) is critical in making sure OCIO security policies and standards address real-world, operational security concerns. The importance of this relationship is well understood and must continually be strengthened in order to effectively combat the continually increasing number and complexity of cyber threats.

Action Steps and Time Frame

- 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.

SAO Recommendation 6: The state's Chief Information Security Officer continue to collaborate with the Office of the Chief Information Officer 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.

STATE RESPONSE:
The state's Chief Information Security Officer (CISO) agrees that close collaboration with the state's Chief Information Officer (CIO) is critical to ensuring OCIO security policies and standards address real-world, operational security risks. This relationship is critical to providing consistent implementation strategies across agencies as the threat landscape changes.

Action Steps and Time Frame

- 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 provide guidance on how agencies can consistently implement the security controls identified in the updated security standards by December 2015.