JAY INSLEE
Governor

STATE OF WASHINGTON
WASHINGTON TECHNOLOGY SOLUTIONS
1500 Jefferson Street SE • Olympia, Washington 98504-1501

December 10, 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 and the Department of Enterprise Services (DES), thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report, "Contract Assurances for Vendor-Hosted State Information Technology Applications."

We appreciate the recommendations provided by the SAO and agree there are opportunities to improve and learn from. The SAO's recommendations will help DES and the Office of the Chief Information Officer (OCIO) improve their processes and tools, which will more broadly help state agencies, improve the security of sensitive information entrusted to the state.

In general, we agree the recommendations to the agencies in the audit are good practices for all state agencies. However, we caution that the results the SAO identified through auditing five agencies and seven contracts should not be broadly construed as results for all state agencies. For example, in one specific case only one contract was reviewed for an agency where the vendor was a sole provider of a required service where the vendor did not comply with all requirements. Basing results broadly on such a narrow scope of review may not be a fair representation of whether an agency complies with IT security requirements.

Some of the audited agencies have already made improvements and more are underway. Steps to be taken to address SAO's recommendations follows.

Please thank your team for their important work on this performance audit.

Sincerely,

James Weaver
Director & State Chief Information Officer

cc: David Postman, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Drew Shirk, Executive Director of Legislative Affairs, Office of the Governor
Keith Phillips, Director of Policy, Office of the Governor
Inger Brinck, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
John Cooper, Senior Performance Project Manager, Results Washington, Office of the Governor
Scott Bream, Acting Chief Information Security Officer, Washington Technology Solutions
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor

OFFICIAL STATE CABINET AGENCY RESPONSE TO PERFORMANCE AUDIT ON CONTRACT ASSURANCES FOR VENDOR-HOSTED STATE INFORMATION TECHNOLOGY APPLICATIONS – DECEMBER 10, 2018

This management response to the State Auditor's Office (SAO) performance audit report received November 16, 2018, is provided by the Office of the Chief Information Officer (OCIO) on behalf of the audited agencies and the Department of Enterprise Services.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO assessed whether:

1. Selected IT contracts have included appropriate provisions to address the state's IT security requirements?
2. Selected state agencies follow leading practices to ensure vendors comply with the IT security requirements in their contracts?

The SAO also examined:

3. What contractual provisions selected state agencies have included in vendor contracts to protect the state in case of a data breach?

SAO Recommendations 1-4 to the Department of Enterprise Services (DES):

1. Create recommended contract draft language, in cooperation with OCIO that agencies can use to satisfy basic state IT security requirements when developing new contracts. When completed, share the recommended language with the Office of the Attorney General and agencies' staff responsible for contract monitoring.
2. Finalize policies and procedures to help agencies monitor IT contracts effectively and efficiently.
3. As an agency responsible for contracting policies, consider creating a forum for agency IT and contracting professionals and OCIO staff to share leading practices, and discuss challenges related to ensuring IT security over vendor-hosted applications.
4. Work with the Office of the Attorney General and OCIO to help develop recommended indemnification and notification language. Among other things, such language should clearly define a security breach, timelines for reporting a security breach, and the responsibility of each party in the event of a security breach. When completed, share the recommended language with the state agency procurement officers.

STATE RESPONSE: The Department of Enterprise Services (DES) recognizes the value of the Auditor's recommendations as they pertain to DES and fully supports working with the Office of the Chief Information Officer and the Office of the Attorney General to implement the recommendations.

DES offers a basic contract management training and is in the process of developing an advanced contract monitoring training, which will include procedures. An enterprise contract management and monitoring policy will be also be adopted.

DES will also consider creating a forum for agency IT contracting professionals and OCIO staff to share leading practices and to discuss the challenges related to ensuring IT security over vendor-hosted applications.

Action Steps and Time Frame

- Work with the OCIO and the Attorney General's Office (AGO) to draft recommended contract language for agencies to address basic state IT security requirements for new contracts. This will include indemnification and notification language. *By July 1, 2019.*
- Develop an advanced contract management training, to include procedures. *By July 1, 2019.*
- Adopt an enterprise contract management and monitoring policy. *By December 31, 2019.*
- Consider creating a forum for agency IT contracting professionals and OCIO staff to share leading practices and discuss challenges related to ensuring IT security over vendor-hosted applications. *By December 31, 2019.*

SAO Recommendations 5-8 to the Office of the Chief Information Officer (OCIO):

5. Continue to clarify state IT security standards to help agencies determine how to ensure vendor compliance both before and after the application is deployed. That way agencies can gain assurance that vendors hosting applications are securely processing and storing confidential state data.
6. Determine if additional nationally recognized IT security frameworks or federal IT security standards could substitute for all or part of the state's IT security standards in IT vendor contracts.
7. Clarify expectations for the IT risk assessment that agencies must submit during the security design review process, by providing additional written guidance and tools.
8. Provide uniform guidance on how agencies should interpret the term "immediately" in RCW 19.255.010(2) so agencies can include consistent notification timeline requirements in contracts with their vendors.

STATE RESPONSE: The Office of Cyber Security (OCS) will continue to encourage agencies to participate in OCS monthly technical and policy training sessions, and weekly open office hours to address security issues. This includes education for agencies on steps they can take to ensure vendor compliance both before and after new systems are deployed.

Existing OCIO security standards are tailored to address Washington State's specific IT environment and are closely aligned with Federal IT standards. However, OCIO will investigate to determine where Federal standards could be used explicitly to substitute for part of the state's IT security standards in vendor contracts in order to establish "common language" and frame of reference for vendors who have already achieved compliance with Federal standards. The OCIO will also investigate risk assessment tools agencies can use to better understand their vulnerabilities, and work with agencies to develop these tools.

The OCS will work with DES contracts and state agencies to develop guidance and consensus on how the term "immediately" should be interpreted in order to provide consistent notification timeline requirements in contracts with vendors.

Action Steps and Time Frame

- Continue to educate and clarify for agencies steps they can take to ensure vendor compliance. *Ongoing.*
- Investigate where Federal standards could be used to explicitly substitute for part of the state's IT security standards in vendor contracts to establish "common language" and frame of reference for vendors who are compliant with Federal standards. *By December 31, 2019.*
- Investigate risk assessment tools agencies can use to better understand their vulnerabilities and work with agencies to develop these tools. *By September 30, 2019.*
- Work with DES contracts and state agencies to develop guidance on how the term "immediately" should be interpreted in order to provide consistent notification timeline requirements in contracts with vendors. *By July 1, 2019.*

SAO Recommendations 9-11 to state agencies:

9. Continue to work to ensure the security of confidential data in vendor hosted applications.
    a. Conducting a risk assessment to identify appropriate state and agency IT security requirements for each vendor-hosted application and require vendors to comply with them. If certain security requirements do not apply to a vendor-hosted application, the agency should confirm with the OCIO that those standards may be omitted by submitting a waiver request to the state Chief Information Security Officer (CISO).
    b. Including the requirement for compliance with appropriate state and agency IT security requirements in the solicitation process so all potential vendors are fully aware of the requirement from the beginning of the procurement process and are able to respond accordingly.
    c. If vendors are unable to comply with one or more IT security requirements, agencies should work with the vendor to identify controls that are commensurate with the requirements. Agencies should then submit a waiver request to the state CISO identifying the specific section of OCIO 141.10 that cannot be met, along with any information relating to compensating controls.
    d. In cases where agencies' vendors comply with alternative IT security frameworks, agencies should demonstrate compliance by mapping comparable contractor controls to all appropriate IT security standards and controls, and add supplemental controls to close any gaps between state standards and other IT security frameworks in place.
    e. Requesting a security design review in accordance with criteria outlined in OCIO 141.10 to help ensure vendors secure state data and assets appropriately and comply with state IT security standards before implementing vendor-hosted applications.
10. Improve the monitoring of vendors by following leading practices on contract monitoring. Specifically:
    a. Using results of the conducted risk assessment, develop appropriate contractual monitoring criteria, including details outlining how, and how often, the vendor should demonstrate compliance.
    b. Verify vendor compliance with IT security requirements stated in the contract, in accordance with contractual timelines and using the tools and processes detailed in the contract.
    c. Develop and formalize communication protocols with their vendors that include:
        - Clear roles and responsibilities for agency and vendor staff as they relate to IT security.

- Clear channels of communication between the agency and the vendor as well as types and frequency of communication regarding IT security in particular.

11. To protect the state in the event of a security breach, we recommend state agencies:
    a. Continue working with the DES Office of Risk Management and Assistant Attorneys General when developing contracts to ensure robust indemnification and notification language and to consider when cyber liability insurance might be appropriate.
    b. Ensure the data breach notification timeline in the current and future contracts aligns with state laws and policies.

STATE RESPONSE: We appreciate and agree with the recommendations provided by the SAO. While we are unable to modify the conditions of our current contracts to address all of the recommendations, we plan to address these in contract amendments and operational processes as appropriate. Going forward we plan to take the following actions to improve future contracts.

Action Steps and Time Frame
For future contracts, the audited agencies plan to take the following actions by the designated date:

- Develop a process for conducting risk assessments, to include state and agency IT security requirements (agencies 1-5). *By March 31, 2020.*
- Include in RFPs for vendor-hosted applications the requirement for compliance with applicable agency, state, and federal IT security requirements (agencies 2, 3, 4 and 5). *By July 1, 2019*
- Develop a process to work with vendors unable to comply with IT security requirements to submit a waiver request to the state's Chief Information Security Officer (agencies 1-5). *By March 31, 2020.*
- Develop a process or continue to work with vendors who are complying with alternative IT security frameworks to demonstrate full compliance with the required IT security standards (agencies 1-5). *By March 31, 2020.*
- Continue to or request a security design review in accordance with criteria outlined in the state's IT standards OCIO 141.10 (agency 3, 4, and 5). *By March 30, 2020.*
- Use the results of risk assessments conducted to develop appropriate contractual monitoring criteria (agencies 1-5). *By May 1, 2020.*
- Verify vendor compliance with IT security requirements using contractual timelines, tools and processes (agencies 1, 3 and 5). *By July 1, 2019.*
- Develop communication plans for contracts that identify roles and responsibilities of agency and vendor representatives, as well as how and when they communicate (agencies 3 and 5). *By May 1, 2020.*
- Continue to or develop a process to work with the DES Office of Risk Management and the AGO when developing contracts and consider cyber liability insurance where appropriate (agencies 1-5). *By March 31, 2020.*
- Work with DES and OCIO to develop guidance on how the term "immediately" should be interpreted and ensure data breach notification timelines are included in all future contracts that align with state laws and policies (agencies 1-5). *By July 1, 2019.*
- Work with DES and OCIO to develop guidance to follow when vendors don't comply with IT security requirements, especially in circumstances where a vendor is the sole provider of a required service or where purchase of the product requires use of a click-through website that does not allow for review and acceptance of IT security requirements (agency 3 and 5). *By March 31, 2020.*