STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION
Tony Evers, Governor
Joel Brennan, Secretary

January 15, 2021

State Senator Robert Cowles
Co-chair, Joint Legislative Audit Committee
118 South, State Capitol
P.O. Box 7882
Madison, WI 53707-7882

State Representative Samantha Kerkman
Co-chair, Joint Legislative Audit Committee
315 North, State Capitol
P.O. Box 8952
Madison, Wisconsin 53708-8952

Dear Co-Chairpersons Cowles and Kerkman:

The Department of Administration (DOA) herein submits to the Joint Legislative Audit Committee an update on the status of its efforts to implement recommendations related to concerns identified by the Legislative Audit Bureau (LAB) in Audit Report 20-11 "IT Needs Assessment, Procurement, and Security". We thank the LAB for the opportunity to act on these recommendations and their work in highlighting these important issues.

In 2019, DOA conducted a comprehensive review of its statutory responsibilities to identify areas for improvement as the LAB was conducting its audit. Having completed our internal review, and with the benefit of the LAB Audit Report, we are currently working to better comply with our statutory duties, which includes implementing changes to enhance statutory reporting, monitoring, tracking, and other obligations. As I noted in my August 28, 2020 response letter, DOA has already implemented changes to comply with statutory requirements for annual and statewide IT strategic planning, semiannual large and high-risk project reporting, and other required reports. DOA also continues to work with executive branch agencies to ensure their compliance with statutory and policy requirements, including by providing additional oversight of IT projects and more information and resources to increase efficiency and effectiveness in completing them. While all of this work is ongoing, we have made significant progress in addressing LAB's recommendations, which is discussed in greater detail in the attached report.

Through our work to respond to LAB's recommendations, it became clear that the recommendations reflect common themes and many are interdependent with each other. To ensure DOA is accomplishing our statutory obligations while producing the greatest business value, DOA is also working to establish a comprehensive roadmap of pertinent statutory responsibilities that will guide decision-making and resource allocation.

We believe that our responses to the report's recommendations will help us continue optimizing our management and oversight of executive branch IT projects and initiatives.

Sincerely,

Joel Brennan

Joel T. Brennan
Secretary

Attachment

DOA RESPONSE TO LAB Report 20-11 RECOMMENDATIONS

January 15, 2021

SUMMARY

In Audit Report 20-11 "IT Needs Assessment, Procurement, and Security," the Legislative Audit Bureau (LAB) recommended changes to the way the Department of Administration (DOA) oversees IT projects across state agencies in three areas: Statutory Reporting, Procurement, and Cloud Services.

DOA is committed to complying with statutory requirements and has already undertaken several measures to meet the LAB's recommendations.

- DOA established a process to review IT strategic plans from agencies in line with statutory requirements found at s. 16.971(2)(L), s. 16.971(2)(Lm), and s. 16.976, and has communicated to agencies that DOA will withhold approval of agency plans until all required information is included.
- DOA updated its processes to ensure that required reports are submitted to the Joint Committee on Information Policy and Technology within statutory deadlines.
- DOA is currently updating its policies to reflect current business practices for reviewing large, high-risk IT projects with agency leaders, including IT directors.
- DOA is analyzing the scope of certain requirements to establish procurement processes that satisfy statutory mandates.

Given the commonality and interdependency of many of these recommendations, DOA is working on a comprehensive roadmap of the interaction among these recommendations, which will guide DOA and executive branch agencies in complying with statutory requirements.

DOA previously responded to LAB's Security Recommendations in November 2020. Work on the IT Security Policy Handbook and related standards to address concerns are ongoing. DOA's report on these recommendations was submitted to the Joint Legislative Audit Committee on November 13, 2020.

Specific responses to each LAB recommendation are outlined below.

STATUTORY REPORTING

RECOMMENDATION:

Consistently require state agencies to include all statutorily required information about all of their projects in their annual information technology strategic plans. (20-11, p. 19)

DOA RESPONSE:

DOA has established a two-month period from March 1 to May 1 in DOA's annual agency IT strategic planning process to review all submitted IT strategic plans to ensure that agencies include all statutorily required information. DOA also implemented other changes to the annual agency IT strategic planning process to help ensure that all statutorily required information is received from agencies. As part of this process, DOA has communicated to agencies that information technology strategic plans that do not include all statutorily required information or do not include all required projects will not be approved.

RECOMMENDATION:

Comply with statutes by submitting the statewide information technology strategic plan to the Joint Committee on Information Policy and Technology every two years. (20-11, p. 19)

DOA RESPONSE:

As required under s. 16.971(2)(m), DOA submitted the statewide IT Strategic Plan to the Governor and the Joint Committee on Information Policy and Technology on September 15, 2020. We are evaluating the development of a policy to standardize statutory reporting across DOA to ensure compliance with statutory reporting requirements.

RECOMMENDATION:

Comply with its policies by ensuring that the interagency committee conducts technical reviews of all large, high-risk information technology projects. (20-11, p. 20)

DOA RESPONSE:

Due to improvements to the State's IT governance structure that have occurred since the referenced policy was enacted, DOA will be updating this policy to align with current business practices. IT project technical reviews now occur within Enterprise IT, which is comprised of executive branch agency IT directors, rather than the interagency committee. Larger IT projects may also be reviewed with the Administrative Officers' Council and the Deputy Secretaries' Group.

RECOMMENDATION:

Ensure that state agencies consistently provide it with complete and accurate information about ongoing large, high-risk information technology projects. (20-11 p. 24)

DOA RESPONSE:

DOA communicated to agencies their responsibility to provide complete and accurate information to DOA in an email from DOA to agencies on January 5, 2021. DOA will continue to reinforce the importance of providing complete and accurate information to agency leaders on an ongoing basis throughout the statutory reporting process. DOA is working to increase communication and collaboration with agencies through the development of a roadmap that aligns statutory reporting requirements to provide the greatest value to both DOA and agencies.

RECOMMENDATION:

Comply with statutes by consistently submitting semiannual reports about large, high-risk information technology projects to the Joint Committee on Information Policy and Technology. (20-11 P. 24)

DOA RESPONSE:

As required under s. 16.973(16), DOA submitted semiannual reports to the Joint Committee on Information Policy and Technology on February 29, 2020, and August 31, 2020, which is within statutory requirements. DOA is evaluating the development of a policy to standardize statutory reporting across DOA to ensure compliance with statutory reporting requirements.

RECOMMENDATION:

Ensure that the submitted semiannual reports contain all statutorily required information about each project. (20-11 P. 24)

DOA RESPONSE:

DOA has incorporated a one-week period within the semiannual reporting process to review all semiannual reports received from agencies to ensure they contain all statutorily required information and to revise reports that are missing statutorily required information prior to submission to the Joint Committee on Information Policy and Technology. This additional review period will help ensure semiannual reports contain all statutorily required information about each project and that all projects are included.

RECOMMENDATION:

Consistently comply with statutory requirements pertaining to its oversight of information technology projects. (20-11 P. 41)

DOA RESPONSE:

In 2019, DOA conducted a review of State statutes relevant to its IT oversight to evaluate its statutory responsibilities and identify areas where compliance with statutory requirements could be better formalized or strengthened. As a result of that review, DOA has already completed updates to several reporting requirements, including agency and statewide IT strategic planning processes, semiannual large and high-risk project reporting processes, the biennial TEACH program report, the annual report on master leases for IT projects, and the annual self-funded portal report. While DOA has completed updates to these items, work is continuing to ensure DOA meets its statutory obligations with respect to IT oversight.

RECOMMENDATION:

Ensure that state agencies consistently comply with statutory and policy requirements pertaining to information technology projects and information technology security. (20-11 P. 41)

DOA RESPONSE:

DOA is working with agencies to increase compliance with statutory requirements by communicating specific agency responsibilities to agency leaders and engaging in proactive oversight of agencies through regular communication and collaboration to ensure their compliance with statutory responsibilities. DOA has already made updates to agency and statewide strategic IT planning processes and the semiannual large and high-risk reporting process and is working to update its processes for other statutory requirements.

PROCUREMENT

RECOMMENDATION:

Comply with statutes by consistently reviewing and approving all information technology contracts for other state agencies. (20-11 P. 21)

DOA RESPONSE:

We appreciate that LAB highlighted this as an area where the legislature should consider making changes, because DOA's oversight resources are best directed at large, high-risk IT contracts rather than every IT contract. This is particularly true given the ever-expanding role of IT across the enterprise.

Absent legislative intervention, DOA is currently analyzing the scope of this requirement in order to ascertain the point at which the required review should occur, as well as the level of review and approval required by statute. For example, not every purchase order or amendment under a contract will need separate approval, though under the current statutory language, every contract must be reviewed and approved at some level. DOA is evaluating how it would best implement the proper internal controls to fulfill these requirements in their current form, while minimally impacting necessary agency operations. DOA plans to complete this analysis by June 30, 2021.

RECOMMENDATION:

Ensure that state agencies comply with statutes by including in contracts for large, high-risk information technology projects a stipulation that it must approve any order or amendment that would change the contract scope and increase the contract price. (20-11, P. 22)

DOA RESPONSE:

As referenced above, this requirement acknowledges that in some instances the legislature has already rightfully directed DOA's oversight resources to large, high-risk IT projects. Currently, the State Procurement Manual, PRO-508, includes a requirement that agencies include a stipulation in certain IT contracts that DOA must approve any order or amendment that would change the contract scope and increase the contract price. Specifically PRO-508 states, "For high risk IT contracts, as defined by the Division under the authority of s. 16.973(10) or for contracts at the large IT procurement threshold, agencies will include a stipulation requiring the vendor to submit to the department for approval any order or amendment that would change the scope of the contract and have the effect of increasing the contract price."

In addition to the Procurement Manual stipulation, the work to identify the scope of DOA's IT oversight responsibility discussed in response to the previous recommendation will also impact DOA's ability to ensure that all relevant orders or amendments are also approved by DOA.

CLOUD SERVICES

RECOMMENDATION:

Require state agencies, including itself, that contract with firms that provide cloud computing services to take various appropriate actions to safeguard the State's data. (20-11 p. 33)

DOA RESPONSE:

DOA has established a cross-agency workgroup to update DOA and agency policies, including codification of appropriate actions to safeguard the State's data. DOA plans to complete this work by June 30, 2021. Additional changes to enhance safeguards for cloud computing services are detailed in the answers below.

RECOMMENDATION:

Modify its policies for acquiring cloud computing services from firms, including by specifying the entities to which the policies apply and requiring state agencies to evaluate in writing the advantages and disadvantages of contracting with such firms. (20-11 p. 26)

DOA RESPONSE:

DOA has established a cross-agency workgroup to update DOA and agency policies and to develop enterprise-wide policies governing the review of proposed contracts for cloud computing services, including developing criteria for agencies to determine which entities are considered cloud computing services and integrating requirements for cloud computing contracts that safeguard the State's data such as security assessments, submission of annual data security audits, storage of all data within the United States, background checks for all employees and subcontractors, limitations on employee access to data, payment of monetary penalties or assumption of responsibility for the effects of security breaches or unauthorized disclosures of data, and notification of security breaches or unauthorized disclosures of data.

RECOMMENDATION:

Help state agencies to develop appropriate policies for contracting with firms that provide cloud computing services. (20-11 p. 42)

DOA RESPONSE:

As previously noted, DOA has established a cross-agency workgroup to update DOA and agency policies to address the LAB's recommendations, including requirements for cloud computing contracts that safeguard the State's data such as security assessments, submission of annual data security audits, storage of all data within the United States, background checks for all employees and subcontractors, limitations on employee access to data, payment of monetary penalties or assumption of responsibility for the effects of security breaches or unauthorized disclosures of data, and notification of security breaches or unauthorized disclosures of data.