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

August 16, 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 (Committee) an update on the status of its efforts to implement recommendations related to Finding 2019-001, Finding 2019-002, and Finding 2019-003, identified by the Legislative Audit Bureau (LAB) in Audit Report 19-30, December 2019, "State of Wisconsin FY 2018-19 Financial Statements". The update was to be provided to the Committee on August 16, 2021. Enclosed is a detailed report to the Committee regarding the actions undertaken by DOA in response to each recommendation.

In the intervening months, all of the LAB's recommendations in Report 20-30 have either been addressed or are in the process of being addressed. In April 2021, DOA reported to the Committee on the progress it made concerning recommendations 2019-001, 2019-002, and 2019-003.
We thank the LAB for the opportunity to act on these recommendations and their work in highlighting these important issues.

Respectfully,

Joel Brennan

Joel T. Brennan
Secretary

DOA RESPONSE TO LAB Report 20-30 RECOMMENDATIONS

August 16, 2021

SUMMARY

In Audit Report 20-30 "State of Wisconsin FY 2019-20 Financial Statements," the Legislative Audit Bureau (LAB) conducted a financial audit of the State by auditing its financial statements in accordance with applicable government auditing standards, issuing LAB auditor's opinions, reviewing internal controls, and making recommendations for improvements. The Department of Administration (DOA) provided an update to LAB and the Joint Legislative Audit Committee (JLAC) on April 15, 2021 as recommend regarding clearing appropriations.

Audit Report 20-30 recommended that DOA take steps to fully complete projects or update project plans to implement the written procedures, practices, and settings of the Division of Enterprise Technology (DET) to enforce policies and standards. Report 20-30 recommended DOA evaluate the adequacy of agency monitoring and compliance with the State of Wisconsin IT Security Policy Handbook and related standards; set specific completion dates for the actions identified in its DET's risk assessment plan related to vulnerability management and penetration testing; and identify areas not included within the scope of the current risk assessment plan or other methods of assessing risks that would assist in the overall management of risk, and update the risk assessment plan for consideration of these areas or methods.

Audit Report 20-30 recommended that DOA develop and provide training to assist state agencies in understanding their responsibilities for preparing financial information for inclusion in the Comprehensive Annual Financial Report (CAFR); determine which state agencies consistently have delays in meeting established timelines, work with those agencies to address areas that cause delays in reporting, and identify solutions to improve the efficiency and timeliness of the process for preparing the financial statements; and work with state agencies to plan for the implementation of new accounting standards and ensure DOA completes all planning, review, and assessment processes before the close of the affected financial reporting period.

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

BACKGROUND

Under s. 16.97, Wis. Stats., DOA is responsible for the State's IT services, including ensuring that all state data processing facilities develop proper privacy and security procedures and safeguards. As a part of DOA, DET operates data centers to provide a variety of services to state agencies, including managing the mainframe for all agencies; managing servers for DOA and other executive branch agencies; and maintaining DOA-related systems.

In addition, DET performs programming and security functions, including maintaining the infrastructure for STAR, which is the State's enterprise resource planning system that includes accounting, payroll, and purchasing systems used by most state agencies.

As defined by DET, IT policies are formal, brief, high-level statements or plans that reflect an agency's general beliefs, goals, rules, and objectives for a specific subject area. Standards are mandatory actions or rules designed to support policies. Procedures are a documented series of steps that align with policies and standards. DET's policies and standards are set forth in the State of Wisconsin IT Security Policy Handbook, which became effective in October 2018 and includes the related standards by reference.

State Controller's Office/Financial Background:
The DOA State Controller's Office (SCO) has primary responsibility for completing the State of Wisconsin CAFR, which are the State's GAAP-based financial statements. Although, SCO completes many of the required entries centrally, there is certain information that is only available to agencies, therefore SCO has to rely on agencies to complete portions of the CAFR. Agencies complete this by sending in submissions, which are reviewed by SCO. SCO provides guidance to state agencies on the preparation of financial information through the State of Wisconsin Uniform GAAP Conversion Policies and Procedures Manual (GAAP Manual), which is maintained by SCO. SCO also provides trainings to agencies as issues are identified. Each July, SCO establishes a timeline for state agencies to follow when preparing and submitting financial information. Timelines for state agencies are generally similar from year to year. When state agencies do not adhere to the timeline, SCO is challenged to compile the CAFR in a timely manner.

FINDING 2020-001 (IMPLEMENTATION OF IT PROCEDURES BY DOA DET)

RECOMMENDATION:

Take steps to fully complete projects or update project plans to implement the written procedures, practices, and settings of the Division of Enterprise Technology to enforce policies and standards. (20-30, p. 23)

DOA RESPONSE:

As previously shared with LAB, DOA created a project to evaluate gaps, and codify and update policies, standards, procedures, and settings. This project is now complete - DET policies and standards are available to DOA and agency employees and DET procedures are available to DET employees.

FINDING 2020-002 (DOA INFORMATION TECHNOLOGY OVERSIGHT RESPONSIBILITIES)

RECOMMENDATION:

Evaluate, by December 18, 2020, the adequacy of executive branch agency monitoring provided through the dashboard in assessing the progress of executive branch agency compliance with the State of Wisconsin IT Security Policy Handbook and related standards and implement additional methods for monitoring as needed. (20-30 p.37)

DOA RESPONSE:

The Division of Enterprise Technology (DET) evaluated the adequacy of utilizing a dashboard for monitoring agency progress in attaining compliance for executive branch agency policies, standards, and procedures. DET completed the evaluation and the project. Through the project, DET made changes to the monitoring dashboard to comply with the most recently released revision to NIST Special Publication 800-53, which NIST released in September 2020. In addition to the monitoring dashboard, DET will be closely reviewing all quarterly updates received from agencies and confirming that policies, standards, and procedures meet requirements. We will continue to refine our methodology for monitoring and improving agency compliance with these requirements.

RECOMMENDATION:

Establish a timeline for anticipated agency compliance with the State of Wisconsin IT Security Policy Handbook and related standards, assess agency progress in achieving compliance, and take actions to assist agencies not achieving compliance in a timely manner. (20-30 p.37)

DOA RESPONSE:

DET worked with executive branch agencies to establish goals and timelines for agency compliance with the Executive Branch Agency IT Security Policy Handbook and related standards.

Utilizing the updated monitoring dashboard, DET sent a security policy, standard, and procedure template to agencies for completion. Once received from agencies, these templates will be summarized in an anonymized dashboard available to all agencies to gauge enterprise compliance. After agency responses have been received, the DET CISO will work with agencies to establish agency timelines for compliance with DET security policies, standards, and procedures.

DET security staff will also use agency responses to identify gaps in compliance and will require quarterly updates from agencies to show progress towards full compliance. Moving forward, DET will conduct annual reviews of agency compliance of policies, standards, and procedures and will regularly communicate updates, especially those that directly impact agencies. DET will also work closely with agency CISOs to identify areas for further improvement.

RECOMMENDATION:

Set specific completion dates for the actions identified in its Division of Enterprise Technology's risk assessment plan related to vulnerability management and penetration testing, complete the actions by the dates established, and update the plan to specify the frequency of and processes for ongoing or periodic assessments and related actions. (20-30 p.37)

DOA RESPONSE:

DET worked with executive branch agencies to establish a process to enhance enterprise capabilities for vulnerability management, penetration testing, and risk assessments.

DET is now working to implement its vulnerability management plan, which includes tools, penetration testing, risk assessments, and associated policies, standards, and procedures. Once the plan is finalized, DET will be working with agencies to identify timelines and actions that must be taken.

RECOMMENDATION:

Identify, by December 18, 2020, areas not included within the scope of the current risk assessment plan or other methods of assessing risks that would assist in the overall management of risk, and update the risk assessment plan for consideration of these areas or methods. (20-30 p.37)

DOA RESPONSE:

DET worked with executive branch agencies to evaluate areas not included within the current risk assessment plan and possible methods of assessing risks that would assist in the overall management of risk and updated the risk assessment plan for consideration of these areas or methods as needed.

This evaluation was completed, and initial updates were made. Additional updates will be made once the updated vulnerability management plan is finalized.

FINANCIAL REPORTING PROCESS

RECOMMENDATION:

Continue developing and providing training to assist state agencies in understanding their responsibilities for preparing financial information for inclusion in the CAFR. (20-30 p.16)

DOA RESPONSE:

Each year, the SCO reviews each agency's prior year submission and looks for areas where training may be needed. If the SCO identifies issues relevant to multiple agencies, group trainings are provided. Conversely, if an issue is specific to an individual agency, SCO works with the agency individually to ensure they understand their responsibilities and financial reporting information. Also, when agencies have turnover and hire new accountants with GAAP responsibilities, SCO reaches out to inquire on their level of experience and questions they may have. During FY 2021, SCO reviewed agency submissions that had issues in the prior year and worked directly with those agencies. SCO scheduled initial meetings to inquire with agencies what caused the issues and then scheduled follow up meetings to provide training and guidance to prevent similar issues in the future.

RECOMMENDATION:

Determine which state agencies consistently have delays in meeting established timelines, work with those agencies to address areas that cause delays in reporting, and identify solutions to improve the efficiency and timeliness of the process for preparing the financial statements. (20-30 p.16)

DOA RESPONSE:

SCO tracks agency submission dates and compares them to the established due dates. Each year SCO identifies agencies that consistently do not meet their due dates and reaches out to the agencies to discuss issues causing the delays. Based on LAB's recommendation in report 20-30, SCO spent even more time and follow-up with agencies in FY 2021 to ensure they understand their submissions along with identifying solutions to improve efficiencies. SCO

scheduled initial meetings to inquire with agencies regarding what was causing them issues and then scheduled multiple follow-up meetings to provide training and guidance.

RECOMMENDATION:

Work with state agencies to plan for the implementation of new accounting standards and ensure DOA completes all planning, review, and assessment processes before the close of the affected financial reporting period. (20-30 p.16)

DOA RESPONSE:

Each year SCO reviews new GASB standards effective for current and future years. As part of the process of implementing the standard, SCO determines which agencies could be affected by the new standards by sending out surveys to agencies for which the results determine if the new standards affect them. SCO also presents and discusses new standards at Financial Leadership Council meetings, which are attended by agency financial managers. For larger more complex standards, SCO consults with the affected agencies and then drafts accounting issue papers, which are provided to LAB for review and their feedback.