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 (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 by April 1, 2020. We apologize for the delay. 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 19-30 have either been addressed or are in the process of being addressed. In November 2020, DOA reported to the Committee on the progress it made concerning recommendations 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 19-30 RECOMMENDATIONS

January 15, 2021

SUMMARY

In Audit Report 19-30 "State of Wisconsin FY 2018-19 Financial Statements" (Report), the Legislative Audit Bureau (LAB) identified three findings related to the security and management of STAR, cybersecurity procedures, and IT oversight responsibilities. Though DOA did not meet the original deadline for providing an update on these recommendations, many of the recommendations were implemented within the timeline established by the Report.

Outlined below are responses to LAB Findings 2019-001, 2019-002, and 2019-003.

2019-001: STAR SECURITY CONCERNS

RECOMMENDATION:

Take corrective actions by June 30, 2020, to address the specific recommendations included in the confidential interim memorandum provided during the audit.

DOA RESPONSE:

DOA agreed with LAB's findings and recommendations and by June 30, 2020, took the corrective actions described in its confidential corrective action plan. These corrective measures included reducing access in several areas and implementing new procedures to ensure data stored and processed in STAR is protected from accidental or intentional misuse or destruction. STAR also established internal controls to prevent inappropriate or inadvertent access to STAR and its related databases, and to provide STAR staff with a consistent methodology for performing their work.

The actions undertaken by DOA resolved a majority of the findings included in 2019-001 and, as such, it was no longer reportable in Report 20-30, "State of Wisconsin FY 2019-20 Financial Statements". Plans to implement corrective actions for three remaining items were submitted to LAB on October 15, 2020, as part of a new confidential corrective action plan.

2019-002: IMPLEMENTATION OF IT PROCEDURES BY DET

RECOMMENDATION:

Take steps to fully complete or update and implement the written procedures, practices, and settings of the Division of Enterprise Technology (DET) to enforce its policies and standards, and take corrective action to address the specific concerns communicated during the audit.

DOA RESPONSE:

DOA agreed with LAB's findings and recommendations and took corrective action to address specific concerns identified in the audit. DOA identified 23 projects to address specific items related to the completion, update, and implementation of written procedures, practices, and settings. DOA utilized DET's project prioritization process to track progress through a comprehensive dashboard. The status of the 23 projects as of January 14, 2021, is as follows:

Project Status:	Count
Completed	7
In Progress	15
Approved to Start	0
Pending Prioritization/Release	1
Total	23

These projects will ensure DOA can maintain a secure environment by developing, approving, and following appropriate policies, standards, and procedures. These projects also include updates of technical configurations that enforce controls for a computer or group of computers.

Initiation and scheduling of the one pending project are based upon priority and availability of required resources. DOA anticipates completing projects by June 30, 2021.

2019-003: IT OVERSIGHT RESPONSIBILITIES

RECOMMENDATION:

Develop and implement, by March 31, 2020, a plan for monitoring the progress of executive branch agencies in becoming compliant with the State of Wisconsin *IT Security Policy Handbook* and related standards.

DOA RESPONSE:

DOA agreed with LAB's finding and recommendation and developed and implemented a plan and dashboard for use by executive branch agencies to establish an ongoing process to track compliance with the State of Wisconsin *IT Security Policy Handbook* and related standards. DOA received the first set of responses from agencies by June 30, 2020. These responses established a baseline for executive branch agencies. Through this monitoring, DOA is actively working with agencies to identify non-compliance and rectify it promptly.

The auditors reviewed DOA's efforts as part of Report 20-30 and recommended it review the adequacy of the dashboard and implement additional methods for monitoring, as needed. DET has done this by working with executive branch agencies and is in the process of implementing refinements to its dashboard and processes.

DOA reported on this finding and recommendation in the November 13, 2020 response.

RECOMMENDATION:

Complete its corrective action plan to fully address recommendations from prior year LAB Finding 2018-004 within the timeline provided in its June 2019 communication to LAB on the status of corrective actions taken.

DOA RESPONSE:

DOA agreed with LAB's finding and recommendation and worked with executive branch agencies to complete the Enterprise Risk Assessment plan in April 2020. During the development of the plan and timeline, DET identified the need to standardize the toolset for conducting vulnerability assessments to enable DET the ability to monitor vulnerabilities across the agencies. As a result, DET worked with executive branch agencies and the State Bureau of Procurement to evaluate vulnerability management tools and, in November 2020, selected a tool that will be implemented by the majority of agencies. Implementation of a uniform tool will readily allow the use of standard criteria for vulnerability assessments, which will report up to DOA for oversight.

RECOMMENDATION:

Develop and implement by June 30, 2020, a process to regularly identify, assess, and address risks for the State's IT environment, including vulnerability assessments, penetration testing, and comprehensive risk assessments that assess risk across the IT environment and include ongoing monitoring of agency compliance with the State of Wisconsin IT Security Policy Handbook and related standards.

DOA RESPONSE:

DOA agreed with the findings and recommendations and, as noted above, worked with executive branch agencies to establish an ongoing process to monitor compliance with the IT Security Policy Handbook by June 30, 2020.

The auditors reviewed DOA's efforts in this area as part of its completion of the "IT Needs Assessment, Procurement, and Security" performance evaluation, Report 20-11, and on November 13, 2020, DOA reported that many of the measures taken to respond to this recommendation were already completed or in progress. Also in its November 13, 2020, response, DOA noted that it received detailed responses to specific cybersecurity concerns from executive branch agencies and anticipated completion dates related to each of the concerns.

DOA continues to work closely with executive branch agencies to establish an ongoing process to regularly complete vulnerability assessments, after which it will plan for conducting penetration testing and continue ongoing risk assessments. DOA anticipates rolling out the plan for this process by June 30, 2021.