STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION
Tony Evers, Governor
Kathy Blumenfeld, Secretary-designee

April 1, 2022

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, WI 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 2021-001, identified by the Legislative Audit Bureau (LAB) in Audit Report 21-23, December 2021, "State of Wisconsin FY 2020-21 Financial Statements." The update was to be provided to the Committee April 1, 2022. Enclosed is a detailed report to the Committee regarding 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 is a repeated finding. In August 2021, DOA reported to the Committee on the progress it made concerning the recommendations 2020-001 and 2020-002.

We thank the LAB for the opportunity to act on these recommendations and their work in highlighting these important issues.

Respectfully,

DocuSigned by:
Kathy Blumenfeld
B66780F542464DA...

Kathy Blumenfeld
Secretary-designee

DOA RESPONSE TO LAB REPORT 21-23 RECOMMENDATIONS

April 1, 2022

SUMMARY

In audit report 21-23 "State of Wisconsin FY 2020-21 Financial Statements," the Legislative Audit Bureau (LAB) identified the Wisconsin statutes that require DOA to provide oversight and monitoring of executive branch agency IT operations and made recommendations in Finding 2021-001.

Wisconsin Statutes give DOA responsibility for the State's IT services. Under s. 16.971 (2), Wis. Stats., DOA shall work with executive branch agencies to establish IT policies, procedures, and planning processes, and monitor adherence to these policies, procedures, and processes. Further, s. 16.971 (2), Wis. Stats., requires DOA to provide oversight and monitoring of executive branch agency IT operations, which includes ensuring:

- management reviews of IT organizations are conducted;
- all executive branch agencies develop and operate with clear guidelines and standards in the areas of IT systems development and employ good management practices and cost-benefit justifications; and
- all state data-processing facilities develop proper privacy and security procedures and safeguards.

Finally, s. 16.973 (3), Wis. Stats., states that DOA shall facilitate the implementation of statewide initiatives, including the development and maintenance of policies and programs to protect the privacy of individuals who are the subjects of information contained in the agency databases.

Outlined below are responses to finding 2021-001. Please note that this is a repeated finding from report 20-30.

FINDING 2021-001: DEPARTMENT OF ADMINISTRATION INFORMATION TECHNOLOGY OVERSITE AND MONITORING RESPONSIBILITIES

RECOMMENDATION:
Complete collection of information to develop the dashboard and analyze executive branch agency adherence to the State of Wisconsin IT Security Policy Handbook and related standards by December 30, 2021.

DOA RESPONSE:
DOA agreed with LAB's findings and recommendations. The Division of Enterprise Technology (DET) worked with executive branch agencies and completed collecting information from executive branch agencies via the Agency IT Policies, Standards and Procedures (PSP) dashboard template on September 15, 2021.

From the data collected, DET created an anonymized PSP Dashboard summary, which provides a statewide view of overall executive branch agency compliance with the IT Security Policy Handbook and related standards. The PSP Dashboard was published on October 7, 2021 and shared with executive branch agency security officers and IT Directors on October 12, 2021.

DET completed analysis of individual executive branch agency PSP responses to assess adherence to the State of Wisconsin IT Security Policy Handbook and related standards on December 30, 2021. Documentation of the analysis will be provided to LAB during the upcoming FY22 audit.

RECOMMENDATION:
Respond to the analyses by working with executive branch agencies that are not adhering to the State of Wisconsin IT Security Policy Handbook and related standards to bring them into compliance by September 30, 2022.

DOA RESPONSE:
DOA agreed with LAB's finding and recommendations. DET is working with executive branch agencies that are not in compliance with the State of Wisconsin IT Security Handbook and related standards. DET is in the process of meeting with each non-compliant agency to review the policies and standards that are out of compliance. DET will assist agencies develop a plan to become compliant by September 30, 2022.

DET is using the established Policy, Standards and Procedures (PSP) template and operational procedures (please refer to the response below) to measure adherence with the State of Wisconsin IT Security Policy Handbook and related standards.

RECOMMENDATION:
Review and update the monitoring program, including establishing specific ongoing monitoring processes that DOA will perform to be assured that executive branch agencies continue to adhere to the State of Wisconsin IT Security Policy Handbook and related standards by December 30, 2022.

DOA RESPONSE:
DOA agreed with LAB's finding and recommendations. On October 12, 2021, DET created and published the PSP Dashboard and Operational Procedures which establishes specific ongoing monitoring processes that DOA will perform to assure that executive branch agencies continue to adhere to the State of Wisconsin IT Security Policy and related standards. This process will be reviewed and updated annually.

Copies of the published dashboard and operational procedures were provided to LAB.

RECOMMENDATION:
Work with the executive branch agencies by January 31, 2022, to develop the timeline for purchase, implementation, and configuration of the vulnerability management tool.

DOA RESPONSE:

DOA agreed with LAB's finding and recommendations. DET worked with executive branch agencies, by January 31, 2022, to gather their plans for vulnerability management tool purchase, implementation, and configuration. The agency plans will be shared with LAB during the upcoming FY22 audit.

In addition, DET continues to work with the agencies to assist them with technical questions regarding their implementation and configuration of the tool after purchase. The tool will aid in meeting DOA's responsibility to monitor executive branch agency IT operations.

RECOMMENDATION:
Establish detailed plans by June 30, 2022, for how DOA will perform ongoing vulnerability assessments with the new vulnerability management tool, respond to those assessments, and make changes to further strengthen the State's IT environment.

DOA RESPONSE:
DOA agrees with LAB's finding and recommendation. Part of DOA's vulnerability management implementation project includes working with the executive branch agencies to:

- Ensure agencies are adhering to the State of Wisconsin IT Security Risk Assessment Policy and related standard by receiving agency vulnerability management report results
- Define the types of vulnerability assessments performed and frequency
- Define a schedule for vulnerability assessments
- Review of vulnerability results
- Process to remediate vulnerabilities (e.g., missing patches)
- Verify vulnerabilities have been remediated

DOA's vulnerability management implementation project is currently on track to be completed May 31, 2022.

RECOMMENDATION:
Review and continue to update its risk management program including considering the risks related to approved policy exceptions and remediating known vulnerabilities.

DOA RESPONSE:
DOA agrees with LAB's finding and recommendations. After completion of DOA's vulnerability management implementation, by June 30, 2022, DET will review and update its risk management program and associated risk assessment plan to include consideration of risks related to approved policy exceptions and using the new vulnerability management tool, will remediate known vulnerabilities.

DET will also work with the executive branch agencies to update their risk assessment plans, to ensure that agencies are adhering to the Risk Assessment Policy and related standard.