WISCONSIN
DEPARTMENT OF
ADMINISTRATION
DOA.WI.GOV

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

March 31, 2023

State Senator Eric Wimberger
Co-Chair, Joint Legislative Audit Committee
104 South, State Capitol
P.O. Box 7882
Madison, WI 53707-7882

State Representative Robert Wittke
Co-Chair, Joint Legislative Audit Committee
18 West, State Capitol
P.O. Box 8953
Madison, WI 53708-8953

Dear Co-Chairpersons Wimberger and Wittke:

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 Findings 2022-002, 2022-003 and 2022-004 identified by the Legislative Audit Bureau (LAB) in Audit Report 22-26, December 2022, “State of Wisconsin FY 2021-22 Financial Statements.” The update was to be provided to the Committee March 31, 2023. 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 Audit Report 21-23 have either been addressed or is repeated in Finding 2022-004 identified by the LAB in Audit Report 22-26 and are in the process of being addressed. In April 2022, DOA reported to the Committee on the progress it made concerning the recommendations 2021-001.

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

Respectfully,

Kathy Blumenfeld

Kathy Blumenfeld
Secretary

DOA RESPONSE TO LAB REPORT 22-26 RECOMMENDATIONS

March 31, 2023

SUMMARY

In audit report 22-26 "State of Wisconsin FY 2021-22 Financial Statements," the Legislative Audit Bureau (LAB) identified the Wisconsin statutes that require DOA to: Provide the State's information technology (IT) services, including ensuring that all state data processing facilities develop proper privacy and security procedures and safeguards and provide oversight and monitoring of executive branch agency IT operations. LAB made recommendations in Finding 2022-002, 2022-003 and 2022-004.

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 findings 2022-002, 2022-003 and 2022-004. Please note that findings 2022-002 and 2022-004 are repeated findings from report 21-23.

FINDING 2022-002: DEPARTMENT OF ADMINISTRATION/DIVISION OF ENTERPRISE TECHNOLOGY INFORMATION SECURITY ACCESS REVIEW PROCESS

RECOMMENDATION:
Develop and complete a process by June 30, 2023, to perform access reviews in accordance with the State of Wisconsin IT Security Policy Handbook, including updating access based on the review and retaining documentation of the review and the updates made to access.

DOA RESPONSE:
DOA agreed with LAB's findings and recommendation. The Division of Enterprise Technology (DET) developed a process to perform access reviews in accordance with the State of Wisconsin IT Security Policy Handbook. The process includes steps for updating access based on the reviews. The process document was completed on March 31, 2023 and the access review process will be provided to LAB during the upcoming FY23 audit.

DET is currently working on the implementation of an Active Directory audit tool to aid in the access review of privileged accounts by June 30, 2023. Implementation of the audit tool has encountered several challenges and DET is in the process of acquiring additional technical assistance to complete the installation and configuration of the tool. After implementation of the audit tool, privileged account access reviews will be conducted following the access review process. Completed access reviews of both privileged and Individual account access reviews are expected to be completed by December 30, 2023.

DET will provide audit tool implementation and access review progress reports to LAB during the upcoming FY23 audit.

FINDING 2022-003: DEPARTMENT OF ADMINISTRATION/DIVISION OF ENTERPRISE TECHNOLOGY INFORMATION SECURITY POLICY EXCEPTION PROCESS

RECOMMENDATION:
Complete by January 31, 2023, a review of its existing IT security exception process and make revisions to the process, including developing a procedure for escalating noncompliance with established policies to senior management within the Department of Administration and within the particular executive branch agency.

DOA RESPONSE:
DOA agreed with LAB's findings and recommendation. The Division of Enterprise Technology (DET) completed a review of its existing IT security exception process and made revisions to the process including developing a procedure for escalating noncompliance with established policies to senior management within the Department of Administration and with the particular executive branch agency.

The revised IT security exception form and procedure was published to the DET Customer Center website on January 30, 2023. Prior to publishing the revisions, DET shared the changes to the form and procedure both verbally and in writing with agency security officers and agency IT Directors.

Documentation of the revised IT security exception process and agency communications will be provided to LAB during the upcoming FY23 audit.

RECOMMENDATION:
Develop an exception process training program and communicate the relevant training program and exception process procedures and responsibilities to its staff and executive branch agency staff by January 31, 2023.

DOA RESPONSE:

DOA agreed with LAB's findings and recommendation. The Division of Enterprise Technology (DET) created an IT Security Exception training PowerPoint presentation that was presented to agency security officers on January 17, 2023, and to agency IT Directors on January 25, 2023. In addition, by agency request, the PowerPoint Training was recorded and published to the DET Customer Center website on March 13, 2023. Finally, DET has been conducting coaching sessions with the agencies on the steps and activities in preparing exception requests.

Documentation of the IT security exception training and agency communications will be provided to LAB during the upcoming FY23 audit.

RECOMMENDATION:
Complete and document its review and assessment of processes and configurations that do not comply with established policies, complete approvals of exceptions when changes to processes cannot be made timely, maintain documentation of discussions and meetings with agency staff as the review and assessment of exceptions are completed, and complete this review and approval of exceptions by March 31, 2023.

DOA RESPONSE:
DOA agreed with LAB's findings and recommendation. DET completed and documented a review of agency policies, standards and procedures that are not in compliance on December 15, 2022. DET completed its review of configurations that do not comply with established policies on March 3,2023.

DET worked with agency staff to complete approvals of exceptions when changes to processes could not be made by March 31, 2023 and maintained documentation of discussions and meetings with agency staff as the review and assessment of exceptions were completed.

Documentation of the agency discussions and approved IT security exceptions will be provided to LAB during the upcoming FY23 audit.

FINDING 2022-004: DEPARTMENT OF ADMINISTRATION INFORMATION TECHNOLOGY OVERSIGHT AND MONITORING RESPONSIBILITIES

RECOMMENDATION:
The Wisconsin Department of Administration, Division of Enterprise Technology comply with its statutory responsibilities to provide oversight and monitoring of executive branch agency adherence to the State's IT policies by using its statutory authority to ensure executive branch agencies conform with the State's IT policies and standards or obtain an approved exception by March 31, 2023.

DOA RESPONSE:
DOA agreed with LAB's findings and recommendation. The Division of Enterprise Technology (DET) worked with executive branch agencies and completed collecting revised information from executive branch

agencies via the Agency IT Policies, Standards and Procedures (PSP) dashboard template on December 15, 2022.

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 January 4, 2023. DET met with each executive branch agency to review demonstrated compliance with the States IT policies and standards or to obtain an approved exception following the IT Security Exception process. Approved exceptions where needed were obtained by March 31, 2023.

Documentation of the analysis, agency meetings and approved exceptions will be provided to LAB during the upcoming FY23 audit.

RECOMMENDATION:
Develop and communicate to executive branch agencies by March 31, 2023, a monitoring plan to review the effectiveness of agency-reported information in the dashboard, including how the Department of Administration will report results to the agency and expected timelines for agencies to correct the noncompliance with the State's IT policies and standards or obtain an approved exception.

DOA RESPONSE:
DOA agrees with LAB's finding and recommendation. DET is working with agency Chief Information Security Officers (CISOs) to develop a monitoring plan to periodically review the effectiveness of agency-reported information in the IT Policies, Standards and Procedures (PSP) dashboard and has captured response, ideas, and feedback from the CISOs on the recommendation. DET would like to further discuss the recommendation as part of the upcoming FY23 audit to ensure a clear understanding of the scope and depth of the recommendation as to meet expectations and to effectively enable us to respond to agency feedback. DET is expecting to utilize the established IT Policy, Standards and Procedures (PSP) template and operational procedures to measure adherence with the State of Wisconsin IT Security Policy Handbook and related standards, but feel the clarifying conversations with LAB are necessary to ensure adherence to the recommendation.

DET has been working with noncompliant agencies to obtain approved IT security exceptions by March 31, 2023. Documentation of the approved exceptions will be provided to LAB during the upcoming FY23 audit.

RECOMMENDATION:
Establish detailed plans by June 30, 2023, for how it 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 agreed with LAB's finding and recommendation. DET has enhanced its ongoing vulnerability assessment schedule to include quarterly compliance assessments beginning in April 2023. In addition to

the monthly patch audit performed, the compliance assessment will check the configuration settings of DET managed systems to ensure that the settings have not been misconfigured and are also in compliance with federal and state standards.

In addition, DET's detailed plans will include 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 agency vulnerability assessments performed and frequency.
- Review of agency vulnerability results.
- Process to remediate vulnerabilities (e.g., missing patches).
- Verify vulnerabilities have been remediated.

DOA's detailed vulnerability assessment plan is currently on track to be completed June 30, 2023. DET will provide LAB a status update during the upcoming FY23 audit.

RECOMMENDATION:
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 recommendation. After completion of DOA's detailed vulnerability management plan, by June 30, 2023, 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.