



STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary

VIA EMAIL

March 1, 2024

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

RE: Report 23-26

Dear Joint Legislative Audit Committee Co-Chairs Wimberger and Wittke:

The enclosed memo serves as the Department of Administration's (DOA's) update on the status of its efforts to implement recommendations related to Findings 2023-001, 2023-002, and 2023-003 identified by the Legislative Audit Bureau (LAB) in Audit Report 23-26: State of Wisconsin FY 2022-23 Financial Statements. These recommendations are related to DOA's statutory responsibilities to ensure all state data processing facilities develop proper privacy and security procedures and safeguards and to provide oversight and monitoring of executive branch agency IT operations. See Wis. Stat. s. 16.971(2) & (3).

Since the publication of the Report in December 2023, DOA has continued to work to address all the Audit Bureau's findings in Audit Report 23-26. Please note that work on some recommendations was already in progress prior to the publication of Audit Bureau Report 23-26 due to repeat findings. DOA previously reported to the Committee its progress concerning the relevant repeat recommendations from Findings 2022-002, 2022-003, and 2022-004, in March 2023.

We thank the Audit Bureau for their work on these important IT-related issues and welcome the opportunity to improve our operations by implementing the recommendations made in Audit Report 23-26.

Sincerely,

Kathy Blumenfeld
Secretary

Enclosure

FINDING 2023-001: DOA DET INFORMATION SECURITY ACCESS REVIEW PROCESS

LAB Recommendation: For certain types of accounts, develop access review requirements by December 29, 2023.

On November 6, 2023, the Division of Enterprise Technology (DET) developed access review requirements for active directory accounts, which were shared with a vendor specializing in access review automation. Documentation of these requirements will be provided to the LAB during the upcoming FY24 audit.

LAB Recommendation: For certain types of accounts, work with a vendor to obtain an automated tool 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 by June 30, 2024.

DET is currently working with its access review vendor to perform a proof-of-concept to test the functionality of the vendor-provided tools and to ensure it meets DET's active directory review requirements prior to procurement. Upon successful testing, DET will procure and implement the tool to perform access reviews of active directory privileged and non-privileged accounts in accordance with the State of Wisconsin IT Security Policy Handbook. The access reviews will include updating access based on the review and retaining documentation of the review and the updates made to access.

DET will provide the results of the proof-of-concept testing, an update on the audit tool procurement and implementation, and an update on the access review progress to LAB during the upcoming FY24 audit.

LAB Recommendation: For other types of accounts, perform access reviews in accordance with the State of Wisconsin IT Security Policy Handbook, including by updating access based on the review and retaining documentation of the review and the updates made to access, by December 29, 2023.

In October 2023, DET performed access reviews of other types of privileged mainframe accounts in accordance with the State of Wisconsin IT Security Policy Handbook. The access reviews performed included updating access based on the review, retaining documentation of the review, and making updates to access if needed. In January 2024, DET generated non-privileged mainframe account access review reports and distributed these reports to supervisors. These reports are currently being reviewed and changes are expected to be documented by February 29, 2024, in accordance with the State of Wisconsin IT Security Policy Handbook.

DET will provide documentation of the privileged and non-privileged mainframe access reviews to LAB during the upcoming FY24 audit.

FINDING 2023-002: DOA DET INFORMATION SECURITY POLICY EXCEPTION PROCESS

LAB Recommendation: Develop a plan and begin to identify and document exceptions where agencies are noncompliant or partially compliant with controls listed in the State of Wisconsin IT Security Policy Handbook and related standards by April 30, 2024.

As part of its IT Policies, Standards and Procedures quarterly meetings, in January and February 2024, DET met with the Chief Information Security Officers of each executive branch agency to obtain feedback on DET's proposed plan to identify and document exceptions where agencies are noncompliant or partially compliant with controls listed in the State of Wisconsin IT Security Policy Handbook and related standards. DET will provide progress reports to LAB during the upcoming FY24 audit.

FINDING 2023-003: DOA INFORMATION TECHNOLOGY OVERSIGHT AND MONITORING RESPONSIBILITIES

LAB Recommendation: Comply with its statutory responsibilities to provide oversight and monitoring of executive branch agency adherence to the State's IT policies by developing and communicating to executive branch agencies by May 31, 2024, a monitoring plan to review the effectiveness of all agency-reported compliance with controls in the State of Wisconsin IT Security Policy Handbook and related standards.

DET is working with the executive branch agency CISOs to develop a monitoring plan to review the effectiveness of all agency-reported compliance with the controls from the State of Wisconsin IT Security Policy Handbook and related standards.

DET will provide progress reports to LAB during the upcoming FY24 audit.

LAB Recommendation: Update its risk management program by December 29, 2023, including by considering the risks related to approved policy exceptions and remediating known vulnerabilities.

In December 2023, DET drafted an updated Risk Assessment Plan to include the risks related to approved policy exceptions and remediating known vulnerabilities. The new DET Chief Information Security Officer is currently reviewing the updated Risk Assessment Plan for potential additional revisions based upon the emerging security threat landscape.

DET will provide progress reports to LAB during the upcoming FY24 audit.