DEPARTMENT OF ADMINISTRATION

STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Joel Brennan, Secretary

3/29/2019

Sen. Robert Cowles, and
Rep. Samantha Kerkman, Co-chairpersons
Joint Legislative Audit Committee
State of Wisconsin
22 East Mifflin St., Suite 500
Madison, WI 53703

Dear Senator Cowles and Representative Kerkman,

The Department of Administration has been asked to provide a report to you outlining the status of our efforts to implement the recommendations of the Legislative Audit Bureau (LAB) regarding information technology security policies, procedures, and controls. The two specific LAB findings (2018-003 and 2018-004), the LAB recommendations and our corrective actions are as follows:

Finding 2018-003: Department of Administration Division of Enterprise Technology Security Concerns

LAB Recommendation	DOA Planned Corrective Action	Anticipated Corrective Action Date
1. We recommend the Department of Administration, Division of Enterprise Technology (DET) complete written procedures for all areas	The Department will continue to execute its plan as follows: • Town hall sessions were held in the spring of 2018 with DET staff to reinforce the need to align procedures with policies and standards. Critical build procedures were completed by 2/28/2019 as previously identified in our plan for: • Server Builds • Staff Onboarding • Network Builds DET has also identified and prioritized the remaining operating procedures. As of today, over half of those identified procedures are completed.	Critical procedures completed 2/28/2019 Anticipated completion 10/1/2019

LAB Recommendation	DOA Planned Corrective Action	Anticipated Corrective Action Date
	As new services are developed, it is required to document the appropriate procedures to align with Executive Branch IT Security policies and standards. First annual review of Policies and Standards is planned to start August 2019 with annual reviews of all procedures to follow.	
2. We recommend DET review all settings and practices to ensure they align with policies, standards, and procedures	The process to review DET supported server configurations has been completed for the monthly review of settings to ensure alignment with Executive Branch IT Security policies, standards and procedures and the initial review of settings is planned in April. Work has started on establishing a similar process to review settings for DET supported endpoint (desktops, laptops, etc.) and network devices. The review of settings may identify issues related to practices documented by our procedures that may require procedure updates in addition to the annual review of procedures identified above.	Begin on or before 2/28/2019 with anticipated completion 6/30/2019
3. Complete projects initiated in response to security concerns LAB identified	DET has assessed the risk and initiated two projects to address the high-risk concerns. One project has been completed and the remaining project is in process.	Remaining project anticipated completion 1/14/2020

LAB Recommendation	DOA Planned Corrective Action	Anticipated Corrective Action Date
4. Develop, document, and implement a proactive process to identify, assess, and address risks	DET has established three approaches to continuously review and mitigate risks related to people, process and technology. People are being addressed through our security awareness training program. Process is being addressed through our process for documenting and reviewing procedures. Technology will be addressed by the review of patching and configuration settings. Processes are in place and will continue to be improved as the threat landscape changes.	Completed

Finding: 2018-004: Executive Branch Agency Information Technology Policies and Standards

LAB Recommendation	DOA Planned Corrective Action	Anticipated Corrective Action Date
1. Develop and implement a proactive process to identify, assess, and address risks for the parts of the state's IT environment that DOA is statutorily responsible for, including: Prioritizing its plans and timelines to complete vulnerability assessments and penetration testing across all state devices and networks within the Division of Enterprise Technology data centers	Since vulnerability assessments and penetration testing are two separate functions, DOA will address these as separate plans and implementations as follows: DOA has completed implementation of a vulnerability management process for servers within the DET data centers. Initial assessment for servers is planned for April and monthly thereafter. This monthly assessment process includes: • review of the current environment • prioritization of identified patching or configuration vulnerabilities; • remediation of patching and configuration vulnerabilities needing immediate attention.	Completed

LAB Recommendation	DOA Planned Corrective Action	Anticipated Corrective Action Date
	DOA is working to implement a process similar to the above for vulnerability assessments of DET managed network devices within the DET data centers. *Note this does not include devices located in the DET data centers that are managed by other entities.	Anticipated completion 6/30/2019
	Penetration Testing for a subset of DET managed devices and networks within the DET data centers was conducted by a third party in Fall of 2018. Additional penetration testing will be conducted by a third party after the vulnerability remediation efforts have been addressed.	Anticipated completion to be determined based upon third party availability
2. Complete a comprehensive risk assessment across all executive branch agencies	Partial risk assessment information will be gathered based upon the steps completed above. For systems and data not managed by DET, DOA will work with executive branch agencies to develop a plan and timeline to determine the appropriate level of vulnerability assessments and penetration testing to be completed on a regular basis.	Begin 07/31/2019 with anticipated completion 12/31/2019
	• Implementation of vulnerability assessments of the identified systems and data including a process for review of results, prioritization of identified issues, and tracking of remediation activity.	Begin 12/31/2019 with anticipated completion to be determined, based on plan

LAB Recommendation	DOA Planned Corrective Action	Anticipated Corrective Action Date
	• Implementation of penetration testing of the identified systems and data including a process for review of results, prioritization of identified issues, and tracking of remediation activity.	Begin post vulnerability remediation with anticipated completion to be determined, based on plan

The Department of Administration takes protecting the State of Wisconsin's information assets very seriously and will continue our efforts to improve the security measures that are in place. If you have any questions or concerns regarding our response to the LAB findings, please contact Bill Nash, Director for the Bureau of Security in the Division of Enterprise Technology at Bill.Nash@Wisconsin.gov.

Sincerely,

Joel T. Bren

Joel Brennan
Department of Administration, Secretary