UNIVERSITY OF
WISCONSIN SYSTEM

Office of the President

1700 Van Hise Hall
1220 Linden Drive
Madison, Wisconsin 53706-1559
(608) 262-2321 Phone
(608) 262-3985 Fax

e-mail: rcross@uwsa.edu
website: www.wisconsin.edu/

August 30, 2018

Senator Robert Cowles
Co-Chair, Joint Legislative Audit Committee
Room 118 South, State Capitol
Madison, WI 53707

Representative Samantha Kerkman
Co-Chair, Joint Legislative Audit Committee
Room 315 North, State Capitol
Madison, WI 53708

RE: Audit Report 18-2 Follow-up

Dear Senator Cowles and Representative Kerkman:

Thank you for the opportunity to update the Joint Legislative Audit Committee on progress made by the University of Wisconsin System Administration ("UW System") to address the Legislative Audit Bureau's ("LAB") recommendations in Audit Report 18-2, *University of Wisconsin System Fiscal Year 2016-17, Finding 2017-001: Information Technology Controls of the University of Wisconsin System.*

Preparing for and against threats to UW System information security is of critical importance and a fundamental responsibility of all our universities. Protecting the privacy of all members of the university community, safeguarding our critical and sensitive information and guaranteeing the intellectual property of our faculty is an ongoing effort that the UW System and Board of Regents takes seriously, and it does not start or end with this audit. To that end, UW System established an Office of Information Security at the Associate Vice President level who reports to the Vice President for Administration. She is currently building out the information security workforce to focus on risk and compliance efforts, policy refinement, and implementation assistance to institutions as needed. These efforts are intended to provide systemwide focus for this critical mission area.

LAB Audit Report 18-2 includes four recommendations for the UW System to consider implementing. As always, we appreciate and welcome the LAB's recommendations to enhance the effectiveness of our information security program. In response, UW System divided the recommendations into nine action steps, also articulated in our corrective action plan. This letter provides an update on the status of each action step as it relates to the LAB's recommendations.

Universities: Madison, Milwaukee, Eau Claire, Green Bay, La Crosse, Oshkosh, Parkside, Platteville, River Falls, Stevens Point, Stout, Superior, Whitewater. Two-Year Campuses: Baraboo/Sauk County, Barron County, Fond du Lac, Fox Valley, Manitowoc, Marathon County, Marinette, Marshfield/Wood County, Richland, Rock County, Sheboygan, Washington County, Waukesha. Extension: Statewide.

Six of the nine action steps are complete:

- *Develop a UW System Information Security Program document, accompanied by a 12-month work plan.*
- *Develop documentation, which provides comprehensive guidance to all UW Institutions on suggested methods to implement information security policies and procedures.*
- *Conduct monthly reviews, during which UW System institutions will share best practices, identify way to most effectively use available resources, as well as receive guidance from UW System on resources, which can be used to implement policies.*
- *Engage monthly with the UW System institutions, advising them of potential ways to address audit recommendations and confirming progress as planned. Lead in aligning resources with institution priorities to address audit recommendations.*
- *Complete external UW System Information Security Assessment to establish a baseline for assessing the level of protection provided for systems and data.*
- *Use results of external Information Security Assessment to establish an order of priority in which to address deficiencies of data and systems protection, across UW System institutions and consistent with the Information Security Program.*

Additional fidelity on these efforts is as follows. The UW System Information Security Program document, accompanied by a 24-month work plan was published and distributed on April 30, 2018. This document provides comprehensive guidance to institutions. Additionally, working groups, expertise aligned to NIST-based control areas, have been formed to provide further guidance and clarity on policy and procedure implementation, methodologies and best practices. Moreover, the comprehensive nature of the workplan demanded a 24-month timeline vice 12-month.

An external UW System information security assessment was conducted to establish a baseline for assessing the level of protection provided for systems and data. This effort was completed on March 30, 2018. The results of this security assessment, along with results of several penetration test events formed the basis of the 24-month work plan. The action items within the work plan have been prioritized based on highest information security risks that exist within the UW System environment.

Routine engagements and reviews are on-going with institutions' security professionals as well as Chief Information Officers (CIOs) to discuss and assist with resource constraints and challenges to implementation. Monthly meetings via the Technology and Information Security Council (TISC) and bi- monthly meetings with the Information Assurance Council (IAC) are held to review progress of corrective actions regarding institution-specific LAB findings as well as Internal Audit findings, status/progress is confirmed, and challenges and assistance needed, if applicable is discussed.

The three remaining action steps are in progress:

- *Create Additional systemwide, NIST- based information security policies to support the Information Security Program. Include in the 12-month work plan the next set of policies to be developed.*
- *Provide an advanced General Data Protection Regulation readiness assessment to assist UW System institutions with awareness of the regulations; actions to comply with the regulations; and assessment to monitor progress.*
- *Establish an on-going program to assess the level of protection provided for UW systems and data.*

More specific detail on these in-progress efforts include the development of nine additional systemwide, NIST-based information security policies, accompanied by 12 procedures documents. These drafts are being reviewed and will be introduced within the prioritized, phased implementation schedule that has been developed. This schedule includes policy vetting, feedback/governance mechanisms and publishing in accordance with the 24-month work plan.

An external General Data Protection Regulation readiness assessment has been conducted. The resulting report is intended to assist UW System institutions with awareness of the regulation; actions to comply with the regulation; and assessments to monitor progress. Feedback and implementation actions will be discussed and provided to all institutions. Anticipated receipt of report date: September 2018.

Finally, external assessments and penetration tests are being planned for several institutions in calendar year 2019. These will be scheduled and prioritized following completion of internal and external audits conducted through Fall 2018 as part of an on-going program to assess the level of protection provided for UW systems and data.

In addition to the recommendations provided by LAB and our corresponding nine-step action plan, UW System has put a variety of measures in place to increase the robustness of our information security program. For example, UW System recently purchased an integrated suite of security tools in a systemwide deployment, endorsing our strategy of enterprise delivery of commodity services while allowing institutions to focus on those services and capabilities that are truly mission differentiating. These security tools include endpoint protection, cloud security, phishing and malware defense tools and network/threat monitoring.

I want to thank the LAB for its work. If you have any questions regarding this update, please feel free to contact me.

Sincerely,

Ray Cross

Ray Cross
UW System

CC: State Auditor Joe Chrisman
Chief Audit Executive Lori Stortz
Board of Regents
Chancellors
UW System President's Cabinet

Action Steps		
LAB Recommendation	UW Action	Status
Continue development and maintenance of a comprehensive IT security program including developing systemwide IT security policies and procedures across the remaining critical IT areas as recommended by the National Institutes of Standards and Technology publications	• Develop a UW System Information Security Program document, accompanied by a 12- month work plan • Create Additional systemwide, NIST- based information security policies to support the Information Security Program. Include in the 12-month work plan the next set of policies to be developed.	• Complete • In Progress
Provide guidance and training to the institutions regarding information technology security policies and procedures, as needed	• Develop documentation, which provides comprehensive guidance to all UW Institutions on suggested methods to implement information security policies and procedures. • Conduct monthly reviews, during which UW System institutions will share best practices, identify way to most effectively use available resources, as well as receive guidance from UW System on resources, which can be used to implement policies.	• Complete • Complete
Assist the institutions in implementing timely corrective actions related to our institution specific recommendations	• Engage monthly with the UW System institutions, advising them of potential ways to address audit recommendations and confirming progress as planned. Lead in aligning resources with institution priorities to address audit recommendations.	• Complete
Complete development of and implement procedures for assessing the level of protections provided for UW systems and data.	• Complete external UW System Information Security Assessment to establish a baseline for assessing the level of protection provided for systems and data • Use results of external Information Security Assessment to establish an order of priority in which to address deficiencies of data and systems protection, across UW System institutions and consistent with the Information Security Program. • Provide an advanced General Data Protection Regulation readiness assessment to assist UW System institutions with awareness of the regulations; actions to comply with the regulations; and assessment to monitor progress • Establish an ongoing program to assess the level of protection provided for UW systems and data.	• Complete • Complete • In Progress • In Progress