



Office of the President

1700 Van Hise Hall
1220 Linden Drive
Madison, Wisconsin 53706-1559
608-262-2321
tthompson@uwsa.edu
www.wisconsin.edu

November 13, 2020

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: Follow-Up to LAB Report 20-10: IT Needs Assessment, Procurement, and Security

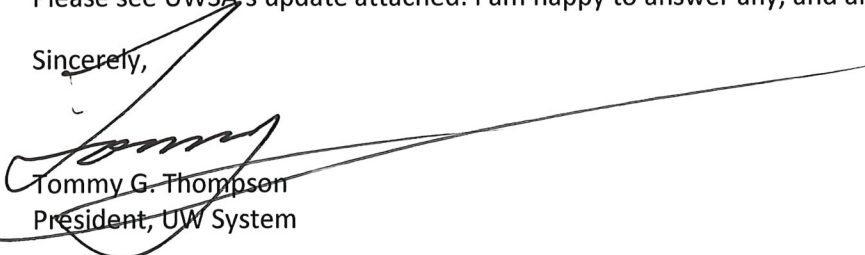
Dear Senator Cowles and Representative Kerkman:

Thank you for the opportunity to update the Joint Legislative Audit Committee on progress made by the University of Wisconsin System Administration (UWSA) to address the recommendations regarding the information technology (IT) security processes outlined in report 20-10. IT security remains an important area of focus for UWSA, and we are making progress on IT security challenges, which stem from aging and archaic IT systems and the decentralized approach to technology, procurement, and governance across the UW System. I am in the process of completely and totally changing this approach and overhauling our IT infrastructure.

I appreciate the Legislative Audit Bureau's (LAB) work on this comprehensive audit. My administration and the larger UW System team are absolutely, and passionately, committed to investing in and strengthening our IT security. We have several initiatives planned that will continue to improve the effectiveness of our IT security program and the delivery of efficient, high-quality services across the UW System. We are deploying critical initiatives, such as IT as a Service (ITaaS) and the Administrative Transformation Project (ATP), to upgrade and modernize our IT infrastructure and improve our IT security posture. These initiatives are elemental to our efforts, and if we do not take these bold steps, we will have breakdowns, data breaches, and financial losses. I am committed to preventing such problems.

Please see UWSA's update attached. I am happy to answer any, and all, questions regarding this update.

Sincerely,



Tommy G. Thompson
President, UW System

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

Information Technology (IT) Security Recommendations

The success of UW System's IT security program is based on a comprehensive approach and strategies for systemwide policy development and compliance, targeted technology investments, workforce development, enterprise standardization, and appropriate consolidation of security operations. During the past year, UWSA focused on many initiatives to improve IT security, which include:

- Deploying the first enterprise suite of security tools throughout UW System (operationalizing of these tools is in progress).
- Deploying multi-factor authentication for employees and many students.
- Developing a systemwide incident response plan and conducting the first systemwide incident response tabletop exercise.
- Performing external security risk assessments at all UW System institutions and conducting application and network penetration tests for select institutions and environments.
- Establishing a governance, risk, and compliance function, including the development of a comprehensive risk register and associated risk mitigation and risk acceptance policies and procedures.
- Developing a vendor security risk assessment process.
- Expanding partnerships with local, state, and federal entities to share cyber threat intelligence.
- Obtaining an incident response retainer with third-party digital forensics experts.
- Procuring an enhanced security awareness training platform for the UW System workforce.

In report 20-10, the LAB made three recommendations regarding IT security. We provide updates on our progress implementing these recommendations below.

Recommendation: Develop comprehensive information technology security policies and procedures that are based on National Institute of Standards and Technology (NIST) standards.

The UW System continues to improve in the area of IT security, particularly in the development of policies and procedures based on NIST, by using a risk-based assessment approach. Existing policies were significantly updated in 2019, and several additional policies were ready for publication and implementation when the COVID-19 pandemic struck. UWSA leadership decided to temporarily hold the publication of these new policies due to the need to pivot and create interim policies to provide flexibilities to our institutions to successfully utilize our IT infrastructure to continue education online and in-person. Due to the COVID-19 pandemic, our IT staff focused on transitioning nearly 40,000 employees to remote work and more than 170,000 students to online learning by the end of the 2019-2020 spring semester. IT staff worked through the following months to ensure campuses could safely welcome students back for in-person, hybrid, and some online classes for the 2020-2021 fall semester.

Beginning in August 2020 and in subsequent months, four new IT security policies and four new procedures were published in the areas of IT Asset Management, Information Security Risk Management, Privacy, and a comprehensive set of definitions. Review dates are established for every policy and procedure published. Policies are updated in response to a changing threat landscape, modernizing technology, and other factors. Additionally, a policy calendar was developed more than a year ago, and it is shared with all UW System institutions. The policy calendar outlines UW System's plans for continued policy development, while balancing other systemwide IT security initiatives necessary to increase UW System's information security maturity.

Recommendation: Address each of the 46 information technology security concerns that LAB found.

UW System's information security program, workplan, and initiatives have been, and will continue to be, aligned with the NIST Cyber Security Framework (CSF), while balancing the need to be effective in an open-collaboration, information-sharing higher education environment. Progress has been made in the last year across the five CSF core areas (identify, protect, detect, respond, and recover). In particular, UW System made focused improvements in the protect and respond functions. Of note, 3 of the 46 concerns identified in report 20-10 had been corrected before the publication of the report.

Of the remaining 43 areas identified, more than half have plans to be addressed at either the enterprise level or through campus-specific initiatives. Campus-specific efforts in the areas of event log review and management, penetration testing, and change management are all in progress. At the system-level, ITaaS is a vital enterprise initiative. While some enterprise-wide IT services do exist, most IT resources are controlled by an institution and are deployed in a non-standard manner across the institutions. This fragmented approach creates redundancies and inefficiencies across the UW System and leads to higher and unsustainable costs, and in many cases, greater IT security risk. UW System's ITaaS initiative and associated projects will bring improvements in IT asset management (inventory hygiene and disposal) as well as tighter controls in change management processes.

Other system-level initiatives include UWSA's Internal Audit's focus on IT disaster recovery over the next year, and the Office of Information Security's development of methods for monitoring the quality and compliance of controls in place by third-party vendors to protect UW System's data. This is accomplished through both qualitative and quantitative analysis and by leveraging industry standard documentation, such as SOC II reports, to evaluate vendor-based IT environments in an efficient and consistent manner.

UWSA continues to collaborate with the institutions to develop and execute specific plans that outline actions and initiatives to address IT security concerns. As indicated above, with the decentralized nature of the UW System environment, many of the security concerns identified by LAB will be implemented at the campus level, while others are the responsibility of UWSA for systemwide implementation.

Recommendation: Ensure all University of Wisconsin institutions, including [UWSA], comply with its policies and procedures.

UWSA and UW System institutions are continuing the implementation of policies and procedures related to IT security. Board of Regents Policy 25-5 *Information Technology: Information Security* delegates to the UW System President the authority to implement and maintain an information security program, and it requires each institution to consistently apply the program and related processes. It further articulates that the Chancellors are responsible for compliance with the systemwide information security program and related processes. UWSA works to ensure compliance with policies and procedures by UWSA and the institutions through the work of UWSA Internal Audit and by using external auditors. UWSA's Office of Information Security continues to act as a resource for institutions to assist with interpreting and implementing systemwide policies and addressing findings of noncompliance. Additionally, investments in ITaaS and ATP are absolutely critical and provide the foundation for standardization and consolidation, which will reduce UW System's attack surface, improve UW System's IT security posture, and modernize our operations. Otherwise, we cannot effectively ensure each institution's compliance until we complete these initiatives.