Legislative Fiscal Bureau
One East Main, Suite 301 • Madison, WI 53703 • (608) 266-3847 • Fax: (608) 267-6873
Email: fiscal.bureau@legis.wisconsin.gov • Website: http://legis.wisconsin.gov/lfb

June 8, 2023 Joint Committee on Finance Paper #145

Cybersecurity Initiatives (Administration -- Information Technology)

[LFB 2023-25 Budget Summary: Page 40, #1]

CURRENT LAW

Under current law, the Department of Administration (DOA) has broad authorities and responsibilities relating to IT services and executive branch agencies under state statute, excluding the UW System, which generally manages its own IT resources. The Administration indicates that the Division of Enterprise Technology (DET) currently provides protection for the state against cybersecurity attacks by: (a) monitoring for detection of potential attacks; (b) monitoring and logging events, alerts, and abnormalities; (c) operating and sharing security endpoint and server system protections; (d) providing application security services; (e) providing vulnerability management services; (f) deploying multi-factor access; (g) providing access control oversight; (h) conducting security technology studies, security architecture reviews, and system security reviews prior to deploying IT and software systems; (i) ensuring security is embedded in state IT projects; (j) upgrading existing security technologies and applications; and (k) collaborating with state partners, other states, and federal partners to protect Wisconsin's cyber infrastructure.

Additionally, DET has an enterprise audit and compliance program that ensures state agencies are meeting regulatory requirements for security. The Division provides oversight, guidelines, policies, procedures, standards, security awareness training, and information throughout the state, and conducts cybersecurity education through partnerships with universities, colleges, K-12 schools, and all levels of government. Additionally, DET leads several state cybersecurity working groups, including the Wisconsin Security Working Group and the Wisconsin Security Lead Working Group, and also partners with two privately-led groups that connect public and private security leaders. The Division also supports leagues and associations across the state which provide cybersecurity education and working sessions on different cybersecurity topics. Finally, DET provides security reviews of cloud systems, cloud applications, and IT technologies. For all security technology contracts, DET ensures that the pricing paid by

the state can be offered to municipalities, counties, K-12 schools, libraries, and tribes to allow for the advantage of volume price discounts.

The Department of Military Affairs leads the Cyber Response Team (CRT), which consists of security volunteers across the state. The CRT is deployed in the event of a cybersecurity attack and provides support to counties, municipalities, K-12 schools, and libraries during a cybersecurity event. The CRT program is funded by federal grants that provide for training and equipment.

The Joint Committee on Information Policy and Technology (JCIPT) is a 10 member legislative committee charged with the following duties: (a) review of information management and technology systems, plans, practices, and policies of state and local units of government, including their responsiveness to the needs of state and local units of government for delivery of high-quality services on an efficient, effective, and economical basis, their data security and integrity, their protection of the personal privacy of individuals who are subjects of databases of state and local governmental agencies and their provision of access to public records; (b) review proposals for the expansion of existing information technology and the implementation of new information technology by the state in terms of how such proposals would affect the needs of state and local governments; (c) review the impact of proposed legislation on existing technology utilization by state and local units of government; and (d) upon receipt of strategic plans from DOA, the Joint Committee on Legislative Organization, and the Director of State Courts, review and transmit comments concerning the plans to the entities submitting the plans.

The Committee may also do any of the following: (a) direct DOA to conduct studies or prepare reports on items related to the Committee's duties; (b) make recommendations to the Governor, the Legislature, state agencies, or local units of government regarding the policies, practices, proposals, legislation, and reviewed reports; (c) direct the UW Board of Regents to prepare and submit reports to the Committee; and (d) with the concurrence of the Joint Committee on Finance, direct DOA to report semiannually to both committees concerning any specific information technology system project which is being designed, developed, tested, or implemented and which the committees anticipate will have a total cost to the state exceeding $1,000,000 in the current or any succeeding fiscal biennium. Such a report must include: (a) the major stages and substages of the project, including an assessment of need, design, implementation and testing stages and their major substages; (b) the scheduled, estimated, and actual completion dates for each major stage and substage of the project; (c) the budgeted amounts and amounts actually expended on each major stage and substage of the project; and (d) an evaluation of the project, including any problems encountered or risks associated with proceeding to the next stage of the project, if any.

DISCUSSION POINTS

1. According to media accounts, public-sector cybersecurity is an increasing concern for state and local governments. In 2020, 44% of global ransomware attacks targeted municipalities. In 2021, 77 state and municipal governments and agencies were affected by ransomware attacks in the United States. In general, victims were smaller municipalities and counties. In October, 2022, several state government websites in Colorado, Kentucky, Mississippi, and other states were subject to

attacks by foreign hackers, resulting in periods of website service disruption and outages. State and local governments may be targeted for reasons including: (a) difficulty implementing a unified public-sector cybersecurity strategy across all local governments in the country; (b) state and local governments store sensitive data; (c) state or local government systems may be poorly defended (especially in comparison to federal government systems); (d) state and local governments may face financial constraints in recruiting and hiring security professionals; and (e) state and local governments in some cases deploy internet-connected devices to provide, monitor, and manage services, which may benefit citizens but may also create vulnerabilities and risks for state and local governments.

2. Under Assembly Bill 43/Senate Bill 70, several provisions intended to centralize public-sector cybersecurity functions in Wisconsin under the authority and control of DOA are presented, as described below.

3. Under AB 43/SB 70, an annual GPR appropriation would be created and provided $10,250,000 GPR annually for security operations centers. Additionally, a continuing PR appropriation not limited to the amounts in the appropriation schedule would be created for security operations centers funded from assessments to state agencies (including the Legislature, the Courts, UW System, and authorities) and local governments, and provided expenditure authority of $1,419,300 PR in 2023-24, $1,520,900 PR in 2024-25, and 5.0 PR positions annually. Additionally, $97,500 PR in 2023-24, $122,300 PR in 2024-25, and 1.0 PR position annually would be provided to DOA's appropriation for IT services to state agencies. As a result, a total of $1,516,800 PR in 2023-24, $1,643,200 PR in 2024-25, and 6.0 PR positions would be provided. Funding would support: one or more state security operations centers; annual testing of cybersecurity defenses; a security information and event management (SIEM) tool; and implementation of additional cybersecurity technologies and IT security policies.

4. The bill would require DOA to establish one or more security operations centers (or one or more regional security operations centers, or both) to provide for the cybersecurity of information technology systems maintained by state agencies, local governmental units, and other eligible entities. The bill specifies that the definition of "agency" with respect to security operations centers includes the Legislature, the Courts, and state-created authorities. "Eligible entities" are defined to include: state agencies, local governmental units, educational agencies, federally recognized tribes and bands, critical infrastructure entities identified by DET, and any other entity identified by DOA by administrative rule. The bill specifies that all security operations centers established by DOA be under the supervision and control of DET. The Division would be responsible for managing the operation of each security operations center, including managed security services (services intended to reduce the impact of cybersecurity threats) guidelines and standard operating procedures. The bill would permit DET to provide managed security services to reduce the impact of cybersecurity threats, including monitoring, alerts and guidance, incident response, educational services, and dissemination of information. The Division would be responsible for collaborating with relevant entities in accordance with statewide security plans, leading executive branch agencies through cybersecurity incidents, and taking any needed action to respond to a substantial external security threat, including disconnecting the network of an eligible entity receiving managed security services.

5. The bill would prohibit executive branch agencies, including the UW System, from purchasing managed security services from any entity other than DOA unless DET determines that it cannot provide comparable managed security services at a reasonable cost and DET approves the purchase. The bill would require DET to establish a process for making such determinations and approvals. Under the bill, DOA would be authorized to coordinate with campuses, institutions, and universities in establishing a security operations center. The bill specifies that DOA may assume direct responsibility for the planning and development of IT systems for the UW System as they pertain to security operations centers if it determines it to be necessary to effectively develop or manage such a system, with or without the consent of the Board of Regents of the UW System, and that DOA may charge the Board of Regents for the costs incurred in carrying out such functions. Additionally, the UW System would not be excluded from other powers and responsibilities of DOA with respect to security operations centers.

6. It should be noted that the bill provisions relating to DET's role in managing cybersecurity would largely be effectuated through entirely new statutory language, rather than narrowly targeted or minor changes to existing statutes. As such, provisions that only apply to executive branch agencies, or which would allow (rather than require) participation by the Legislature or the Courts, could potentially be modified through veto in such a manner as to require participation by the Legislature and the Courts (or any other entity specified by DOA), and could bring the IT systems of the legislative and judicial branches of government under the authority of DOA. Other aspects of the proposal could also potentially be made more expansive and broadly applicable, including the purposes of the newly-created PR continuing appropriation, funded from charges to any entity specified by DOA, expenditures from which would only be limited to the amount of revenue available from such charges.

7. The bill specifies that DET may: (a) enter into contracts and interagency agreements to administer security operations centers; (b) apply for grants to administer security operations centers; and (c) charge fees to recover costs associated with managed security services and other cybersecurity support services. The bill requires that a security operations center could only be established at a facility if DET determines that: (a) the facility is secure and restricted, with appropriate infrastructure and staff; (b) all entrances and critical areas can be controlled and monitored; (c) access can be limited to authorized individuals; (d) security alarms can be monitored by law enforcement or other security; and (e) operational information can be restricted to specific personnel.

8. The bill would authorize DOA to license or authorize computer programs developed by security operations centers to the federal government, other states, and municipalities. The bill specifies that DOA must protect the privacy of individuals who are the subjects of information contained in security operations centers and requires DOA to offer to eligible entities the opportunity to voluntarily obtain computer or supercomputer services from DOA or from a security operations center.

9. According to DOA, the recommended funding amount of $10,250,000 GPR annually for security operations centers was determined by considering the estimates for contracts deployed for conducting cybersecurity activities, including a security information and event management (SIEM) tool, annual cybersecurity defense penetration testing, and technological enhancements to the

state's cyber framework. Of this amount, $6 million would fund a SIEM tool to ensure ongoing compliance with state and federal security-related IT event reporting requirements; $4 million would fund implementation of additional cybersecurity technologies within DET; and $250,000 would fund annual testing of state government cybersecurity defenses.

10. The Administration indicates that the 5.0 positions provided to the PR security operation centers appropriation would be information technical services specialists who would support the activities conducted at the security operations center(s). The Department would intend to fund 80% of the cost of these positions, while local governments would fund the remaining 20%. The 1.0 PR position provided to DOA's appropriation for IT services to state agencies would serve as a cybersecurity audit position. This position would assist DOA with its IT security policy adherence. Table 1 below indicates funding under the bill for the six positions and for other supplies and services.

TABLE 1

Funding for Positions and Other Supplies and Services under AB 43/SB 70

Item	2023-24	2024-25
Funding for Positions (PR)		
Salaries and Fringe Benefits (5.0 IT Services Specialists)*	$349,300	$465,900
Supplies and Services (5.0 IT Services Specialists)*	70,000	55,000
Salary and Fringe Benefits (Cybersecurity Audit Position)	83,500	111,300
Supplies and Services (Cybersecurity Audit Position)	14,000	11,000
Subtotal	$516,800	$643,200
Other Supplies and Services		
GPR	$10,250,000	$10,250,000
PR	1,000,000	1,000,000
Subtotal	$11,250,000	$11,250,000
Positions and Other Supplies and Services		
GPR	$10,250,000	$10,250,000
PR	1,516,800	1,643,200
Total	$11,766,800	$11,893,200

* The Department indicates that 20% of these costs would be borne by local governments.

11. According to DOA, the proposed plan would locate the state security operations center at DOA's data center on Femrite Drive in Madison; however, the plan has not been finalized. The Administration indicates that the state security operations center would be intended to: (a) serve as the state's central enterprise security operations center; (b) monitor, correlate, and assist/lead cyber response events; and (c) monitor the overall operations for centralized cybersecurity coordination. Additionally, regional security operations centers are anticipated to be located at UW campuses that are deemed national cybersecurity centers of excellence or have robust cybersecurity degree programs. The Administration would work with the UW System to finalize initial locations at two to

three sites, allowing for processes, procedures, operations, and personnel training to be established and then replicated at future sites.

12. The Administration seeks to create regional security operations centers for three reasons: (a) to provide better security monitoring and response throughout the state; (b) a single security operations site may not adequately support the entire state due to service and geographical limitations; and (c) doing so provides a regionally-focused approach that allows for monitoring in a particular area of the state, resulting in faster response time and improved awareness of activities in that region of the state. Additionally, the regional security operations centers would provide local cybersecurity support. The intent is that designated UW campuses would host security operations centers and support counties, municipalities, K-12 schools, and libraries located in that geographic region. According to DOA, current security monitoring and response efforts are dispersed across the Administration with limited personnel and technology resources. The Administration indicates that the proposal under AB 43/SB 70 would aim to bolster cybersecurity operations across Wisconsin by leveraging universities and college students to provide security support and skills across the state and growing Wisconsin's base of IT security personnel experts.

13. As noted previously, DOA is provided substantial powers and authority under current law with respect to IT, including with respect to cybersecurity efforts. It could be argued that, if provided sufficient funding and position authority, DET could effectively pursue the Administration's goals to establish security operations centers without additional statutory language relating to cybersecurity functions, insofar as the entities to which DET would provide services would choose to participate. In particular, the current law treatment of the UW System, the Legislature, the Courts, and any other entity not considered an executive branch agency, is such that these entities are independent of DOA with regard to managing IT resources. Therefore, close examination of the statutory modifications as proposed, and the potential implications, may be warranted.

14. However, given that a state security operations center and/or regional security operations centers could strengthen cybersecurity in Wisconsin, the Committee could provide funding and position authority to DOA for this purpose. To provide the proposed resources while maintaining legislative oversight, the Committee could create an annual GPR appropriation, and provide $10,250,000 GPR annually for security operations centers. Additionally, the Committee could create an annual PR appropriation for security operations centers, which would be limited to the amounts in the schedule and funded from assessments to state agencies and non-state entities (which would include local governments), and provide expenditure authority of $1,419,300 PR in 2023-24, $1,520,900 PR in 2024-25, and 5.0 PR positions annually. Finally, the Committee could provide $97,500 PR in 2023-24, $122,300 PR in 2024-25, and 1.0 PR position annually to DOA's appropriation for IT services to state agencies. [Alternative 1]

15. Alternatively, given that certain elements of the proposal have yet to be determined and are uncertain at this time, the Committee could provide a lesser amount of funding and position authority, such as funding for 3.0 positions (rather than 6.0 positions) and one-half of supplies and services funding not associated with positions. The Committee could: create an annual GPR appropriation and provide $5,125,000 GPR annually for security operations centers; create an annual PR appropriation for security operations centers funded from assessments to state agencies and non-

state entities and provide expenditure authority of $667,700 PR in 2023-24, $708,400 PR in 2024-25, and 2.0 PR positions annually; and provide $97,500 PR in 2023-24, $122,300 PR in 2024-25, and 1.0 PR position annually to DOA's appropriation for IT services to state agencies. [Alternative 2] Funding for this alternative is shown in Table 2.

TABLE 2

Funding for Positions and Other Supplies and Services, Alternative 2

Item	2023-24	2024-25
Funding for Positions (PR)		
Salaries and Fringe Benefits (2.0 IT Services Specialists)*	$139,700	$186,400
Supplies and Services (2.0 IT Services Specialists)*	28,000	22,000
Salary and Fringe Benefits (Cybersecurity Audit Position)	83,500	111,300
Supplies and Services (Cybersecurity Audit Position)	14,000	11,000
Subtotal	$265,200	$330,700
Other Supplies and Services		
GPR	$5,125,000	$5,125,000
PR	500,000	500,000
Subtotal	$5,625,000	$5,625,000
Positions and Other Supplies and Services		
GPR	$5,125,000	$5,125,000
PR	765,200	830,700
Total	$5,890,200	$5,955,700

* The Department indicates that 20% of these costs would be borne by local governments.

16. Finally, the Committee could take no action. [Alternative 3] Under this alternative, DOA would continue providing cybersecurity services as specified under current law, and could submit a passive review request to the Committee for additional PR funding or position authority for its IT services to state agencies appropriation under s. 16.515/505 of the statutes. Further, given the importance and broad nature of cybersecurity to the state as a whole and its governmental entities, JCITP could be involved in a closer examination of DOA's proposed cybersecurity improvements, and review any necessary legislation to implement the Department's proposal. Subsequent to any such JCITP review, the Finance Committee could authorize any necessary PR funding and/or positions.

17. Under any of the above alternatives, if funding or position authority are provided for cybersecurity initiatives and the Administration determines additional statutory modifications would be required to accomplish its cybersecurity goals, separate legislation could be enacted to effectuate such changes.

ALTERNATIVES

1. Create an annual GPR appropriation and provide $10,250,000 GPR annually for security operations centers. Create an annual PR appropriation for security operations centers funded from assessments to state agencies and non-state entities and provide expenditure authority of $1,419,300 PR in 2023-24, $1,520,900 PR in 2024-25, and 5.0 PR positions annually. Provide $97,500 PR in 2023-24, $122,300 PR in 2024-25, and 1.0 PR position annually to DOA's appropriation for IT services to state agencies for a cybersecurity audit position.

ALT 1	Change to Base	
	Funding	Positions
GPR	$20,500,000	0.00
PR	3,160,000	6.00
Total	$23,660,000	6.00

2. Create an annual GPR appropriation and provide $5,125,000 GPR annually for security operations centers. Create an annual PR appropriation for security operations centers funded from assessments to state agencies and non-state entities and provide expenditure authority of $667,700 PR in 2023-24, $708,400 PR in 2024-25, and 2.0 PR positions annually. Provide $97,500 PR in 2023-24, $122,300 PR in 2024-25, and 1.0 PR position annually to DOA's appropriation for IT services to state agencies for a cybersecurity audit position.

ALT 2	Change to Base	
	Funding	Positions
GPR	$10,250,000	0.00
PR	1,595,900	3.00
Total	$11,845,900	3.00

3. Take no action.

Prepared by: Brianna Murphy