Administration

Information Technology

(LFB Budget Summary Document: Page 40)

LFB Summary Items for Which an Issue Paper Has Been Prepared

Item #	Title
1	Cybersecurity Initiatives (Paper #145)
2	District Attorney Information Technology Program (Paper #146)
3	Technology for Educational Achievement Program Changes (Paper #147)
4 (part)	IT Services for Historical Society (Paper #148)
5	Centralized Online Services to Residents (Paper #149)

LFB Summary Item Addressed in a Separate Paper

Item #	Title
4 (part)	IT Services for Certain Agencies -- Safety and Professional Services (Paper #682)

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

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 #146

District Attorney Information Technology Program (Administration -- Information Technology and District Attorneys)

[LFB 2023-25 Budget Summary: Page 41, #2 and Page 153, #9]

CURRENT LAW

The District Attorney Information Technology (DAIT) program, administered by DOA, provides IT services and support in district attorney (DA) offices statewide. Budgeted funding for the program is $4,272,800 PR in 2021-22 and $4,273,000 PR in 2022-23 and 15 PR positions, supported with an allocation from the $21.50 justice information system surcharge. The $21.50 justice information system (JIS) surcharge imposed on an individual who is assessed a court fee for the commencement of certain court proceedings. In recent years the JIS surcharge fund has operated in deficit. In 2021-22, the JIS surcharge fund concluded the fiscal year with a cumulative deficit of $9,911,600.

Under the program, DA offices transitioned from independent county networks to a statewide platform, implemented a statewide case management system (PROTECT), and coordinated with the Circuit Courts, the Departments of Justice and Corrections, the Wisconsin State Patrol, and local law enforcement agencies on shared interfaces. Examples of such collaborations include: (a) an interface with the state court system's database (CCAP) in DA offices to provide a two-way transfer of case data; (b) an interface to the criminal history repository to provide updated criminal history records to DA offices; (c) an interface with law enforcement agencies to electronically process referrals; (d) an interface with the Department of Corrections to provide crime victims information from Corrections' notification service; and (e) a criminal eFiling system for all case types.

DISCUSSION POINTS

1. According to DOA, efforts to implement criminal eFiling began in 2015-16. The initial

development of PROTECT was funded through federal JAG/Byrne funds. The PROTECT system is a client server application and requires desktop equipment for all users and includes dependencies on third-party applications, such as Microsoft Word.

2. The Department indicates that there are new platforms that may provide a more efficient system using cloud technology. This may allow users to access the application as long there is an internet connection. In addition, there may be an opportunity to incorporate best practices introduced in the past 10 to 20 years such as mobile-based applications, advanced security controls, and greater integration across the justice system.

3. A request for information was conducted by DOA to gather industry information regarding platform and vendor options as well as estimated costs. Information gathered indicates implementation timelines averaging just over three years with total implementation costs averaging $6.26 million. The project would have three phases: strategy and planning: design and development; and transition support.

4. During strategy and planning, DAIT would contract for consulting services and a software development and IT operations engineer. During design and development, contracted personnel would include a project manager, senior internal business analyst, systems architect, cloud engineer, database developers, and quality assurance. Transition support would contract for systems administration, desktop support, infrastructure, and bandwidth for system access.

5. The Department indicates that maintaining the current system may require an investment in order to continue to provide service to each DA office and ensure the system is stable and meets security standards. The increase in users, the move to subscription software, increase in storage costs due in part to digital evidence and need to increase bandwidth all may require additional resources just to keep the current environment functioning.

6. Under AB 43/SB 70, the Department is provided with $3,000,000 GPR annually for the 2023-25 biennium only. The Department indicates that this funding will primarily be used for software licensing fees, infrastructure costs and consulting resources to rearchitect the system to a cloud-ready application. A variety of contracted staff hourly wage rates could range from $75 to $150 per hour. [Alternative A1] This alternative would also create an annual GPR appropriation for justice information systems. Further, the new appropriation would be included in a list of appropriations for which the Department is annually required to report to the Legislature regarding efforts to improve and increase the efficiency of integration of justice information systems.

7. In order to account for the time it will take to fully initiate the project during 2023-24, the Committee could provide less funding in the first year. Reduced funding assumes that work in the first year would be more equivalent to six months rather than a full year. [Alternative A2] This alternative would provide $1,700,000 GPR in 2023-24 and $3,000,000 GPR in 2024-25 on a one-time basis. However, the Department indicates that the additional flexibility additional funding would provide may allow for more expedited implementation.

8. In previous biennia, the DAIT program has provided IT hardware, software, and legal subscription services to DAs, ADAs, and other DA office staff. Due to decreasing revenue provided

to DAIT through the JIS surcharge and the movement to subscription-based software, DAIT is no longer positioned to provide these services.

9. In addition to updating the PROTECT system, under AB 43/SB 70, $1,400,000 GPR annually is provided for laptops and software for 1,600 state- and county-funded employees statewide utilizing the DAIT network and to provide TIME access (Department of Justice information), Westlaw subscription, and State Bar legal research tools for eligible DA office employees. The bill would use the same annual GPR appropriation created for the PROTECT system to fund IT upgrades.

10. The Department indicates that funding for the IT upgrades is sufficient to cover the laptop (4-year life cycle) and necessary software (Microsoft Office 365 G3) for the 1,600 employees working in the District Attorney offices statewide and utilizing the DAIT network. Additionally, this item provides funding to cover DOJ/TIME Access, Westlaw Subscription and State Bar legal research tools for eligible DA office employees. The table below from DOA breaks down this estimate. [Note that the table sums to more than is provided.]

Item	Total Annual
Laptop	$640,000
Office 365 License	640,000
DOJ/TIME Access	78,000
Westlaw	99,900
State Bar	10,900
Total	$1,468,800

11. Given that the current source of funding for DAIT is the JIS, which is in deficit, the Committee could provide GPR funding in an amount sufficient to cover hardware and software costs associated with DAIT. [Alternative B1] This alternative would provide $1,400,000 GPR annually in a new annual appropriation.

12. The DAIT PR appropriation does have a base amount of funding for hardware and software costs. However, the amount in the base is $200,000 annually for hardware and $810,000 for software costs, which is $458,900 less than the total estimated cost in the table above. In order to balance the needs of DAIT and the PR funding that is in deficit, the Committee could provide the GPR requested, but reduce PR authority. [Alternative B2] This alternative would provide $1,400,000 GPR and -$1,000,000 PR annually.

13. If the Committee decides to take no action related to the PROTECT system or IT upgrades, funding for DAIT would remain at $4,329,700 PR in 2023-24 and 15 PR positions. [Alternative A3 and B3]

ALTERNATIVES

A. PROTECT System

1. Provide $3,000,000 GPR annually on a one-time basis to support the District Attorney Information Technology (DAIT) program, which provides IT hardware, software, and legal subscription services to the District Attorneys (DA), Assistant District Attorneys, and other District Attorney Office staff. Create a new annual GPR appropriation for justice information systems. Further, include the new appropriation in a list of appropriations for which the Department is annually required to report to the Legislature regarding efforts to improve and increase the efficiency of integration of justice information systems.

ALT A1	Change to Base
GPR	$6,000,000

2. Provide $1,700,000 GPR in 2023-24 and $3,000,000 GPR in 2024-25 on a one-time basis to support the District Attorney Information Technology (DAIT) program, which provides IT hardware, software, and legal subscription services to the District Attorneys (DA), Assistant District Attorneys, and other District Attorney Office staff. Create a new annual GPR appropriation for justice information systems. Further, include the new appropriation in a list of appropriations for which the Department is annually required to report to the Legislature regarding efforts to improve and increase the efficiency of integration of justice information systems.

ALT A2	Change to Base
GPR	$4,700,000

3. Take no action.

B. IT Upgrades

1. Provide $1,400,000 GPR annually in a new annual appropriation to fund information technology upgrades for District Attorney offices. Create a new annual GPR appropriation for justice information systems. Further, include the new appropriation in a list of appropriations for which the Department is annually required to report to the Legislature regarding efforts to improve and increase the efficiency of integration of justice information systems.

ALT B1	Change to Base
GPR	$2,800,000

2. Provide $1,400,000 GPR to fund information technology upgrades for District Attorney offices. Reduce PR expenditure authority for DAIT funded from the Justice Information Fee by

$1,000,000 PR annually. Create a new annual GPR appropriation for justice information systems. Further, include the new appropriation in a list of appropriations for which the Department is annually required to report to the Legislature regarding efforts to improve and increase the efficiency of integration of justice information systems.

ALT B2	Change to Base
GPR	$2,800,000
PR	-2,000,000
Total	$800,000

3. Take no action.

Prepared by: Sarah Wynn

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 #147

Technology for Educational Achievement Program Changes (Administration -- Information Technology)

[LFB 2023-25 Budget Summary: Page 41, #3]

CURRENT LAW

The Technology for Educational Achievement (TEACH) program, administered by the Department of Administration (DOA), provides eligible entities access to the Internet through rate discounts and subsidized installation of data lines. Eligible entities include public school districts, private schools, cooperative educational service agencies (CESAs), technical college districts, charter school sponsors, juvenile correctional facilities, private and tribal colleges, public museums, and public libraries.

Under current law, program participants may make monthly payments of $100 for Internet service covering bandwidth of less than 1 gigabit per second, and $250 for bandwidth of 1 gigabit or more per second (up to 10 gigabits). Payments are deposited to the state universal service fund (USF). Payment for the cost to provide the service is made by DOA to the vendor in accordance with rates determined under the state contract. For a service request requiring fiber construction to a site, one-time installation costs are evaluated on a case-by-case basis and may be subsidized by the TEACH program based on need and available funding.

State funding for the TEACH program is provided through the segregated USF, which is primarily funded by assessments on annual gross operating revenues from intrastate telecommunications providers. If funding from the USF is insufficient to support the TEACH program, federal e-rate reimbursement monies may be utilized, to the extent revenue is available.

DISCUSSION POINTS

1. In 2021-22, the TEACH program expended $13,645,100 SEG for eligible entities,

including subsidized Internet access for 273 public school sites. In 2023-23, the program is allocated $15,984,200 SEG.

2. Under 2023 Assembly Bill 43/Senate Bill 70, a biennial GPR appropriation would be created to make payments to telecommunications providers under the TEACH program and $1,553,100 GPR in 2023-24 and $1,831,900 in 2024-25 would be provided to the appropriation. The bill would reduce funding from the state segregated universal service fund for the TEACH program by $5,254,000 SEG in 2023-24 and $5,532,800 SEG in 2024-25 to offset USF appropriation increases under the Department of Public Instruction (DPI). As modified by the errata submitted by DOA on April 27, 2023, the bill would provide DPI increased funding from the USF totaling $10,786,800 SEG over the 2023-25 biennium. Additionally, the bill would amend the statutes to remove language relating to the information technology infrastructure grant program, which ended on June 30, 2021.

3. The SEG funding offset by reductions to the TEACH appropriation would be directed instead to four DPI purposes, including: (a) public library aid ($5 million annually); (b) recollection Wisconsin, a new appropriation ($150,000 in 2023-24 and $300,000 in 2024-25); (c) library services contracts ($29,800 in 2024-25); and (d) BadgerLink ($104,000 in 2023-24 and $203,000 in 2024-25). The proposed funding for DPI will be addressed at a subsequent executive session of the Committee, at which time SEG funding for the TEACH appropriation could be further reduced and instead funded from a newly created GPR appropriation under DOA.

4. The Department indicates that, accounting for the GPR funding that would be provided for the TEACH program, the net reduction of SEG funding for the program ($3,700,900 SEG annually) would not impact service to participating school districts and institutions, and that projected expenditures for the program in the 2023-25 biennium would be adequately funded by the combination of GPR funding and segregated universal service fund amounts. The TEACH program is anticipated to underspend $3,700,900 in 2023-24 compared to the appropriated amount of $15,984,200, according to a financial statement prepared by the Department in November, 2022. The recent reduction in expenditures is due to the IT infrastructure grant program under TEACH ending on June 30, 2021. Under the bill, funding for the program from the remaining SEG appropriation and newly-created GPR appropriation would total $12,283,300 annually, equal to the amount of annual expenditures projected by DOA for the 2023-25 biennium. The Department indicates that, if expenditures exceed program need, federal e-rate reimbursement may be a potential source of funding. While the e-rate appropriation had a closing balance of -$4,050,800 FED on June 30, 2022, DOA expects the appropriation to receive sufficient federal e-rate reimbursement funds to enable the account to return to a positive financial position by the end of 2023-24. The receipt of e-rate reimbursement funds is subject to federal review and approval.

5. Given that a GPR funding source for the TEACH program would allow SEG funding previously expended for the TEACH program to offset USF appropriation increases under DPI, the Committee could choose to create a GPR appropriation for the TEACH program and provide $1,553,100 GPR in 2023-24 and $1,831,900 GPR in 2024-25, and reduce funding from the USF for the TEACH program by $5,254,000 SEG in 2023-24 and $5,532,800 SEG in 2024-25. [Alternative A1]

6. On the other hand, the Committee has not yet made a determination with regard to

proposed USF funding for DPI programs. As such, the Committee could choose to reduce the TEACH appropriation by the net reduction amounts under the bill at this time, $3,700,900 SEG annually, and address the DPI provisions at a later date. [Alternative A2] Under this alternative, remaining funding of $12,283,300 SEG annually is anticipated to adequately fund the program.

7. Alternatively, the Committee could take no action. [Alternative A3] The TEACH program would function and be funded as it is under current law. If funding for the appropriation is not fully expended, the unexpended portion will remain in the balance of the USF.

8. With regard to obsolete statutory language, given that the IT infrastructure grant program under TEACH ended on June 30, 2021, the Committee could choose to remove language relating to the program. [Alternative B1]

9. If the Committee takes no action to remove the IT infrastructure grant program language from statute, unless the statutes are amended to reauthorize the program, the program will remain inactive. [Alternative B2]

ALTERNATIVES

A. Program Funding

1. Create a biennial GPR appropriation to make payments to telecommunications providers under the telecommunications access for educational agencies (TEACH) program and provide $1,553,100 GPR in 2023-24 and $1,831,900 in 2024-25. Reduce funding from the state segregated universal service fund for the TEACH program by $5,254,000 SEG in 2023-24 and $5,532,800 SEG in 2024-25.

ALT A1	Change to Base
GPR	$3,385,000
SEG	- 10,786,800
Total	- $7,401,800

2. Reduce funding from the state segregated universal service fund for the TEACH program by $3,700,900 SEG annually.

ALT A2	Change to Base
SEG	- $7,401,800

3. Take no action.

B. Information Technology Infrastructure Program

1. Amend the statutes to remove language relating to the information technology

infrastructure grant program.

2. Take no action.

Prepared by: Brianna Murphy

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 #148

IT Services for Historical Society (Administration -- Information Technology)

[LFB 2023-25 Budget Summary: Page 42, #4]

CURRENT LAW

The Department of Administration's (DOA) Division of Enterprise Technology (DET) provides IT services to state agencies. Funding for DOA's annual PR appropriation for IT services to state agencies is from charges to state agencies for services provided by DET.

MODIFICATION

Provide $2,494,500 PR in 2023-24 and $1,996,700 PR in 2024-25 to DOA's annual PR appropriation for IT services to state agencies, for DET to provide IT services to the Wisconsin Historical Society.

Explanation: On May 4, 2023, in executive session, the Committee provided the Wisconsin Historical Society with $2,494,800 GPR in 2023-24 and $1,996,700 GPR in 2024-25 for the Historical Society to transition IT services and support to DET. The modification would provide the same amounts of expenditure authority to DOA's PR appropriation for IT services to state agencies. Funding for DOA would reflect the amounts that would have been provided under AB 43/SB 70, as modified by a technical errata submitted by DOA on April 27, 2023.

	Change to Base
PR	$4,491,500

Prepared by: Rachel Janke

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 #149

Centralized Online Services to Residents (Administration -- Information Technology)

[LFB 2023-25 Budget Summary: Page 43, #5]

CURRENT LAW

Currently, Wisconsin state agencies host public-facing applications, data, and services from their own websites, many of which require different logins and passwords. There are approximately 700 datasets on various agency websites open to the public, not all of which require the creation of an account to gain access.

DISCUSSION POINTS

1. Under Assembly Bill 43/Senate Bill 70, an annual GPR appropriation to develop and maintain an online customer service hub would be created and provided $2,000,000 GPR in 2023-24 ($465,000 ongoing and $1,535,000 one-time) and $465,000 GPR in 2024-25. The Department of Administration (DOA) indicates that the customer service hub (also known as the "Wisconsin Front Door online services hub") would be a comprehensive portfolio of state resources in a consolidated and centralized format. The Wisconsin Front Door online services hub could potentially improve the online experience for individuals interacting with state government by: (a) requiring only a single login credential and account profile to access services from across state government; (b) developing a searchable, online centralized customer data hub that makes over 700 publicly-available datasets currently found on state agency websites accessible; and (c) developing online services and data-centric websites oriented around key resident issues and interests.

2. The Department indicates that an online customer service hub would enable the public to access state services and information using one account and password. The Department is presently undertaking a project to unify various state government applications that require user authentication by requiring users of all state government services to create a single username associated with their

persona, which is known as "MyWisconsin ID." The "single sign-on" technology is already being employed by a number of state applications requiring a user to create one MyWisconsin ID account by providing a first and last name, email address, and creating a password. A user would then log in using this single ID and password, and be permitted access to all software systems integrated into the platform without re-entering their login information each time. Beginning in 2024, this unified login will be required for all state employees, and any local government employees or retirees who are covered by a state Group Insurance Board-offered health plan, to enter benefits elections for health insurance and supplemental benefits for themselves and their dependents. Included among the goals of the MyWisconsin ID project is improved security, which entails encryption of user data as well as required multi-factor authentication for all applications. The project aims to migrate all compatible state applications to MyWisconsin ID over the next two biennia.

3. The Wisconsin Front Door online services hub would be intended to create a central location of state online services, including a new data portal which would consolidate more than 700 data sources across various state agencies to a single point of access using the MyWisconsin ID, eliminating the need for users to search specific agency websites to find certain data. For data sets that are currently available without user authentication, the Administration indicates the intent would be to maintain the data sets as publicly accessible without requiring a login. Site navigation for data access could include data categories such as economy, education, health, labor force, natural resources, public safety, taxes, and transportation data. The ultimate goal of creating a data portal would be to provide users with potential information on the hub necessary to make decisions. According to DOA, other states and federal agencies have completed similar data portal projects to facilitate effective sharing of information. It is expected that the data portal would be accessed from Wisconsin.gov and provide direct reference to the existing services, information, and data sources located across agency websites.

4. Another goal of the Wisconsin Front Door online services hub would be to eventually support notifications for subscribers of particular state services. For example, a product could potentially notify users of expiring licenses or plates, as is currently done through the State of Texas's website.

5. According to DOA, a total of $2,000,000 GPR, including $1,535,000 GPR in one-time funding in 2023-24 and $465,000 GPR annually in ongoing funding in each year of the 2023-25 biennium, would be needed to develop and maintain an online customer service hub. Funding estimates were determined by estimating: (a) costs of comparable projects in other states; (b) costs of technology in the current market; and (c) costs of certain software and vendor products. The $1,535,000 in one-time funding provided in 2023-24 would fund a software product and professional services to support implementation of a shared data solution and a governance framework for agency researchers and analysts. In both years of the 2023-25 biennium, $465,000 would fund annual subscription costs and contractor staff. The Department indicates that contractor staff would support the IT solution's maintenance and licensing activities.

6. It could be argued that an online customer service hub could improve the online experience for individuals interacting with the state government by: (a) requiring only a single login credential and account profile to access services from across state government; (b) developing a

searchable, online centralized customer data hub that makes over 700 publicly-available datasets currently found on state agency websites accessible from one location; and (c) developing online services and data-centric websites oriented around key resident issues and interests. The Committee could, therefore, choose to create an annual GPR appropriation to develop and maintain an online customer service hub and provide $2,000,000 GPR in 2023-24 and $465,000 GPR in 2024-25. [Alternative 1]

7. Alternatively, the Committee could create an annual GPR appropriation to develop and maintain an online customer service hub, funded $0 annually, and provide $2,000,000 GPR in 2023-24 and $465,000 GPR in 2024-25 to the Committee's supplemental GPR appropriation. Under this alternative, DOA could submit a request to the Committee for release of the funding under s. 13.10 of the statutes. [Alternative 2]

8. On the other hand, it could be argued that the quality of the user experience online varies according to individual preference and, depending on the execution of the proposal, could potentially be poorer for some users or certain applications. As an example, using a single username and password to access all state government services could be convenient if the interface is user-friendly, all technology involved works smoothly and consistently, and access is securely maintained at all times. However, if any of these elements is missing, the experience could range from less convenient (such as requiring multi-factor authentication to access information that is not sensitive and could be provided requiring less user effort) to extremely challenging (if a service outage occurs, for example, or a legitimate user is locked out of their account). In addition, although the technology may be more secure for some state-provided services than the technology currently utilized for those applications, the integration of all state services using single sign-on technology could present a security concern if a malicious actor were somehow able to gain entry to the system and more easily access information across applications.

9. If the Committee takes no action, according to DOA, it would not have sufficient funding to pursue the online customer service hub project as proposed. However, as indicated previously, the MyWisconsin ID initiative is currently being implemented and efforts will continue to integrate state applications using the single sign-on technology. In addition, under this alternative, DOA would continue to evaluate other data centralization-related solutions with state agencies. Its ability to do so would be more limited in scope and speed of implementation, depending on resource availability in DOA and any other impacted state agencies. [Alternative 3]

ALTERNATIVES

1. Create an annual GPR appropriation to develop and maintain an online customer service hub. Provide $2,000,000 GPR in 2023-24 ($465,000 ongoing and $1,535,000 one-time) and $465,000 GPR in 2024-25.

ALT 1	Change to Base
GPR	$2,465,000

2. Create an annual GPR appropriation to develop and maintain an online customer service hub. Provide $2,000,000 GPR in 2023-24 and $465,000 GPR in 2024-25 to the Committee's supplemental GPR appropriation.

ALT 2	Change to Base
JFC	$2,465,000

3. Take no action.

Prepared by: Brianna Murphy

ADMINISTRATION

Information Technology

LFB Summary Items for Which No Issue Paper Has Been Prepared

Item #	Title
4 (part)	IT Services for Certain Agencies -- Commissioner of Insurance
6	Business Portal Website Redesign