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

May 16, 2023 Joint Committee on Finance Paper #745

Cybersecurity Program Funding (Supreme Court)

[LFB 2023-25 Budget Summary: Page 610, #2]

CURRENT LAW

The Director of State Courts Office (DSCO), among other duties, is responsible for maintaining the security of confidential data and information systems used by the state court system. The Circuit Court Automation Program (CCAP) was created in 1987 and, in 2021, merged with the DSCO's Office of Information Technology Services to provide technology automation services to all counties and court levels in the state. Information technology initiatives for the courts are funded by program revenue in the continuing court information systems appropriation (known colloquially as the CCAP appropriation). Base funding for the appropriation is $9,518,800.

DISCUSSION POINTS

1. Cybersecurity threats and attacks have been on the rise nationally. For example, in 2021, a global threat report from a cybersecurity firm (CrowdStrike) found that cybersecurity threats (including hacking efforts) grew by 400% in 2019 and 2020 combined. These incidents are anticipated to continue to grow as advances in, and reliance on, technology increase.

2. Wisconsin has seen similar trends. In 2022, the DSCO tracked and managed 10 major security incidents in the court system. In addition, the DSCO investigated over 4,000 phishing messages, 256 endpoint detection response incidents (which alert and contain malicious activity), nearly 500,000 malicious domain blocking and/or reporting incidents, and over 1,000,000 suspicious emails.

3. Simultaneous to the increase in cybercrimes is the increase in remote work for certain offices and job types, and changes in court procedures that allow for greater technology use, as a result of the COVID-19 public health emergency. For example, prior to the public health emergency, the DSCO had approximately three to four individuals in administrative roles who

were working remotely in some capacity, while the rest of the staff was working in-office. Effective June 1, 2021, the court system's remote work policy allowed department heads to permit certain employees to work remotely up to 50% of the time (and for a total of six individuals, to work remotely 100% of the time). In addition, recent changes to Supreme Court Rules have increased the use of remote video hearings and digital court reporting (rather than in-person, stenographic court reporting). Generally, increased use of technology increases the potential risk of cyber threats and attacks.

4. In January, 2020, a small cybersecurity team was created to implement additional security systems and procedures to keep the court system infrastructure and data secure. The courts' on-going cybersecurity efforts include, but are not limited to: (a) an email protection program and an email phishing detection program (which uses an Internet mail gateway to provide protections in business email, attachments, and uniform resource locator (URL) links, as well as a tool that uses email metadata and threat intelligence to triage reported phishing emails); (b) a firewall service (which gives CCAP control over the network to identify cyber traffic and prevent malware); and (c) a penetration testing service (which provides external testing of cybersecurity measures and assists with developing remediation strategies for weaknesses).

5. In September, 2022, the DSCO published a Strategic Information Technology Plan, which included recommendations from the cybersecurity team. Nearly all of the programs that would be supported by the funding provided under the budget bill were recommended in the publication.

6. In addition to the on-going cybersecurity programming currently used by the DSCO, the courts' cybersecurity team identified approximately 12 new cybersecurity programs for future implementation. The programs were identified as either high-priority, or lower-priority. Some of the higher-priority programs include: (a) denial of service protection, security information and event management (which aggregates data and provides real-time analysis for security monitoring and attack recovery); (b) upgraded remote access solutions; and (c) Network Access Control (which manages network software to ensure that no unauthorized applications are installed or executed). Lower priority programs include: (a) data loss prevention software (which detects and blocks potential breaches of data); and (b) Secure Access Server Edge (which extends security protections to devices outside of the court system network, such as to personal devices used by remote employees, and blocks certain websites, such as social media platforms).

7. According to the DSCO, most of the programs identified would need to be purchased from a vendor, as the programs are too complex to run in-house due to the required infrastructure, monitoring, and expertise needed. Further, the DSCO indicates that it is not industry standard to build these kinds of systems internally, and if built internally, the courts would be required to hire "top-level cybersecurity development teams to build and constantly maintain the software, and would still be unable to build the hardware." The courts believe that the in-house model would be both cost prohibitive, time-consuming, and in most cases, not possible given the level of expertise needed to build cybersecurity hardware.

8. As a result, all cost estimates were based on the use of vendors. While the DSCO has preferred vendors, specific vendor(s) used and cost of equipment and services to be acquired would

be determined through the state bidding and procurement process, if an existing state contract is unavailable. It is estimated that costs would be broken down as follows: (a) $372,100 in 2023-24 and $787,100 in 2024-25 for on-going cybersecurity program maintenance and testing (including those identified in point 4.); (b) $820,000 in 2023-24 and $665,000 in 2024-25 for the purchase and maintenance of new, high-priority cybersecurity programs (identified in point 6.); and (c) $640,000 annually for the purchase and maintenance of new, lower-priority cybersecurity programs (identified in point 6.).

9. The amount of courts' cybersecurity funding provided under the budget bill matches the 2023-25 budget request from the DSCO, except that the budget bill provides funding from increased program revenue expenditure authority, and the budget request provided funding from general purpose revenue.

10. The CCAP appropriation receives revenue from a number of sources, including the court automation fee, the justice information surcharge, the eFiling fee, and Wisconsin Circuit Court Access subscriptions. Both the DSCO (in its budget request) and the Administration (in the budget bill) estimate the CCAP appropriation to receive approximately $14,371,500 in revenue in 2023-24. In 2024-25, the DSCO anticipates the appropriation will receive $14,404,000, and the Administration anticipates the appropriation will receive $14,391,500 (the difference of $12,500 is related only to the 2024-25 opening balance, impacted by expenditures). These figures are identified in the table, below.

	Courts		Governor	
	2023-24	2024-25	2023-24	2024-25
Revenue	$14,371,536	$14,404,025	$14,371,536	$14,391,524
Expenditures				
Other Items*	$10,450,118	$10,520,694	$10,818,519	$10,722,794
Reestimate	2,188,000	2,188,000	0	0
Cybersecurity	0	0	1,832,100	2,092,100
Closing Balance	**$1,733,418**	**$1,695,331**	**$1,720,917**	**$1,576,630**

*Largely includes fixed amounts for items such as standard budget adjustments and reserve items (including health insurance reserves, and compensation reserves).

11. The largest difference between the DSCO and the Administration's appropriation accounting is in expected expenditures. Based on historical spending averages from 2017-18 to present, the DSCO's budget request sought a PR re-estimate of $2,188,000 annually for the CCAP appropriation, associated with items such as software license renewals, staff travel, rent, utilities, and telecommunications costs. The budget bill did not, however, include this PR re-estimate, but instead included $1,832,100 in 2023-24 and $2,092,100 in 2024-25 associated with cybersecurity. The budget bill, including the PR-funded cybersecurity item, anticipates that the CCAP appropriation will have a positive closing balance of approximately $1,576,600.

12. Given that the DSCO anticipates spending $2,188,000 annually for CCAP appropriation related activities, beyond what was identified by the Administration, and given actual expenditure levels in the prior year ($14,765,200), it could be argued that the CCAP

appropriation does not have sufficient revenue to fully support the cybersecurity initiatives (the anticipated spending of $2.2 million identified by the DSCO is larger than the anticipated closing balance of $1.7 and 1.6 million identified by the Administration for each year of the biennium) and regularly occurring expenditures. According to the DSCO, funding cybersecurity with increased PR expenditure authority in the CCAP appropriation "would result in deferrals of other critical expenditures." In addition, the DSCO notes that, even without the new cybersecurity programs, it has been required for the last two budgets to delay purchases because revenues received during the course of a fiscal year may lag in timing to projected expenditures in a given period. Further, the DSCO notes that "the Governor's recommendation to fund the cybersecurity program by PR rather than GPR adds to the stress of the timing of purchases in support of other CCAP operations, as [they] are required to wait until revenue balances are sufficient to spend additional money."

13. However, the Administration recommends funding the cybersecurity item with CCAP PR because "it is consistent with how the cybersecurity program was initially funded, and it's projected that funding will be available." It is important to note that expenditure authority may not be available to fully fund the cybersecurity programs if the DSCO continues to spend $2,188,000 annually on other items, as anticipated based on historical trends and in its budget request. If the cybersecurity initiatives were funded with CCAP PR, the courts may have to prioritize what items are most important to fund from the CCAP appropriation.

14. Given the increased reliance on technology and the increased threats to cybersecurity, the Committee may wish to provide $1,832,100 in 2023-24 and $2,092,100 to fund the DSCO's on-going cybersecurity programs, as well as its high-priority and lower-priority cybersecurity initiatives with increased PR expenditure authority, as recommended under the budget bill. [Alternative 1]

15. The Committee may, however, wish to provide $1,832,100 in 2023-24 and $2,092,100 to fund the DSCO's on-going cybersecurity programs, as well as its high-priority and lower-priority cybersecurity initiatives with GPR in the Director of State Courts' general program operations appropriations. In addition, the Committee may wish to re-estimate the CCAP appropriation by $2,188,000 annually to better align the appropriation with anticipated expenditures, as identified in the budget request. [Alternative 2]

16. Alternatively, the Committee may wish to support only the DSCO's on-going and high-priority cybersecurity initiatives. This could be accomplished by providing $1,192,100 in 2023-24 and $1,452,100 in 2024-25 in increased PR expenditure authority [Alternative 3] or with increased GPR expenditure authority [Alternative 4]. Reestimated expenditure authority associated with historical CCAP expenditure trends ($2,188,000 PR annually) would not be provided under Alternative 3, but would be provided under Alternative 4, given that the appropriation is anticipated to have revenue to support the expenditure trends, if cybersecurity is funded by GPR.

17. If the Committee takes no action, the DSCO will continue to fund cybersecurity efforts from existing CCAP revenue, and would likely be unable to implement some, or all, of the newly proposed programs. [Alternative 5]

ALTERNATIVES

1. Provide $1,832,100 PR in 2023-24 and $2,092,100 PR in 2024-25 for new and on-going cybersecurity initiatives and related maintenance.

ALT 1	Change to Base
PR	$3,924,200

2. Provide $1,832,100 GPR in 2023-24 and $2,092,100 GPR in 2024-25 for new and on-going cybersecurity initiatives and related maintenance. In addition, re-estimate the CCAP appropriation expenditure authority by $2,188,000 PR annually.

ALT 2	Change to Base
GPR	$3,924,200
PR	4,376,000
Total	$8,300,200

3. Provide $1,192,100 PR in 2023-24 and $1,452,100 PR in 2024-25 for high-priority and on-going cybersecurity and related maintenance. This alternative would not fund the lower priority items identified by the DSCO.

ALT 3	Change to Base
PR	$2,644,200

4. Provide $1,192,100 GPR in 2023-24 and $1,452,100 GPR in 2024-25 for high-priority and on-going cybersecurity and related maintenance. In addition, re-estimate the CCAP appropriation expenditure authority by $2,188,000 PR annually. This alternative would not fund the lower priority items identified by the DSCO, but would increase CCAP expenditure authority.

ALT 4	Change to Base
GPR	$2,644,200
PR	4,376,000
Total	$7,020,200

5. Take no action.

Prepared by: Shannon E. Huberty