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 14, 2015 Joint Committee on Finance Paper #125

Information Technology Security Expenditure Authority (DOA -- Information Technology)

[LFB 2015-17 Budget Summary: Page 43, #1]

CURRENT LAW

Information technology (IT) security for the state is provided by DOA's Division of Enterprise Technology (DET). Funding for DOA's IT services to state agencies appropriation, from which this function is funded, is $100,934,100 PR in 2014-15. Funding to the appropriation is from assessments to state agencies for services provided by DOA.

GOVERNOR

Provide $2,538,000 PR in 2015-16 and $2,661,000 PR in 2016-17 to DOA's printing, mail, communication, and information technology services to state agencies and veterans services appropriation (renamed under the bill to include veterans services to consolidate two information technology appropriations) for IT security services. The Budget in Brief indicates that the additional resources are intended to decrease the risk of a security breach.

DISCUSSION POINTS

1. The Department provides IT security services to state agencies with: (a) support provided by 8.0 PR positions in DET's Bureau of Security; (b) free open source software; and (c) resources made available to states by a non-profit organization, the Multi-State Information Sharing and Analysis Center. The Department is responsible for security of the network, data center, email, database management, and storage. State agencies are responsible for their own data, application, user, and desktop security.

2. Currently, the DET security team performs auditing, compliance, and monitoring of all security access logs from most application and database servers. In addition, DET monitors security to outside threats, and identifies potential vulnerabilities. Each month, the security team alerts agency staff to malicious computer code that is being downloaded, and issues instructions to staff to mitigate damage. Towards this end, the security team operates several applications to log, monitor, audit, and scan to find and remediate potential vulnerabilities. However, according to DOA, the decentralized nature of state IT systems leaves the state more vulnerable with regard to IT security. In particular, DOA notes that security risks have become more sophisticated over time, and recent examples of data breaches experienced by large corporations illustrate the scale of the problem. The administration's recommendation is intended to provide comprehensive, advanced IT security services that could be extended to protect state agencies in general.

3. Expenditure authority would be provided for supplies and services as follows, in order of highest to lowest priority: (a) managed security services contract ($1.5 million in 2015-16 and $1.7 million in 2016-17); (b) secure endpoint management ($419,000 in 2015-16 and $342,000 in 2016-17); (c) identity and access management ($237,000 annually); (d) distributed denial of service prevention and mitigation ($194,000 annually); and (e) security awareness training program ($188,000 annually).

4. Managed security services would be provided by certified security analysts, who would monitor all network traffic in and out of the state's data center for malicious computer code or data breaches. If provided, this service would enable the state to shut off a connection if data loss is detected, to minimize damages from a security breach.

5. Endpoint management refers to the centralized management of multiple devices, which in this case would be provided to minimize security exposure for the tens of thousands of devices, including personal computers, on the state's network. Depending on the services purchased, examples of endpoint management services might include facilitating improved policy enforcement, visibility and control of devices from a central console, applying specific actions to particular types of devices, or providing continuous security and software updates remotely.

6. Identity and access management ensures that only authorized users are permitted access to sensitive data. Services provided would aim to improve the management of information access and permissions.

7. Distributed denial of service prevention and mitigation would support DET's efforts to prevent and address distributed denial of service attacks (a specific type of cyber attack). According to DOA, attempted data breaches occur on a daily basis and the state has faced several denial of service attack threats in particular.

8. Finally, a security awareness training program would be provided to train state employees to recognize potential IT threats that may occur in the course of employees' daily work responsibilities. The Department indicates that security awareness can act as the state's first line of defense against a security threat.

9. By purchasing the above contractual services, DET indicates that the state would

provide additional layers of security protection, and would benefit from the provider's historical experience with security incidents of other customers. The administration argues that the current decentralized approach is inadequate to ensuring that state residents are fully protected from data breaches, which would damage the trust placed in the state in its management of sensitive information. The Committee could, therefore, approve the Governor's recommendation to provide $2,538,000 PR in 2015-16 and $2,661,000 PR in 2016-17 to DOA to purchase and provide IT security services and manage a security awareness training program. [Alternative 1]

10. If the Committee wishes to provide DOA a lesser amount of additional funding to strengthen IT security, it could provide funding for one or more of the security services that DOA has indicated are most important for the state's IT needs: (a) $2,350,000 PR in 2015-16 and $2,473,000 in 2016-17 for a managed security services contract, secure endpoint management, identity and access management, and distributed denial of service prevention and mitigation (would not fund an awareness program) [Alternative 2a]; (b) $2,156,000 PR in 2015-16 and $2,279,000 in 2016-17 for a managed security services contract, secure endpoint management, and identity and access management (would not fund distributed denial of service prevention or an awareness program) [Alternative 2b]; (c) $1,919,000 PR in 2015-16 and $2,042,000 in 2016-17 for a managed security services contract and secure endpoint management (would not fund identity access management, distributed denial of service prevention, or an awareness program) [Alternative 2c]; or (d) $1.5 million PR in 2015-16 and $1.7 million in 2016-17 for a managed security services contract [Alternative 2d].

11. Finally, it could be argued that DOA should continue to prioritize the state's IT security, but should do so within its existing resources. Therefore, the Committee could delete the provision. [Alternative 3]

ALTERNATIVES

1. Approve the Governor's recommendation to provide $2,538,000 PR in 2015-16 and $2,661,000 PR in 2016-17 to DOA's IT services to state agencies appropriation to purchase and provide IT security services and to manage a security awareness training program.

2. Modify the provision to provide funding of a lower amount:

a. $2,350,000 PR in 2015-16 and $2,473,000 PR in 2016-17 for: (a) managed security services contract ($1.5 million in 2015-16 and $1.7 million in 2016-17); (b) secure endpoint management ($419,000 in 2015-16 and $342,000 in 2016-17); (c) identity and access management ($237,000 annually); and (d) distributed denial of service prevention and mitigation ($194,000 annually). [Reductions would be -$188,000 annually.]

ALT 2a	Change to Bill
PR	- $376,000

b. $2,156,000 PR in 2015-16 and $2,279,000 PR in 2016-17 for: (a) managed security

services contract ($1.5 million in 2015-16 and $1.7 million in 2016-17); (b) secure endpoint management ($419,000 in 2015-16 and $342,000 in 2016-17); and (c) identity and access management ($237,000 annually). [Reductions would be -$382,000 annually.]

ALT 2b	Change to Bill
PR	- $764,000

c. $1,919,000 PR in 2015-16 and $2,042,000 PR in 2016-17 for: (a) managed security services contract ($1.5 million in 2015-16 and $1.7 million in 2016-17); and (b) secure endpoint management ($419,000 in 2015-16 and $342,000 in 2016-17). [Reductions would be -$619,000 annually.]

ALT 2c	Change to Bill
PR	- $1,238,000

d. $1.5 million PR in 2015-16 and $1.7 million PR in 2016-17 for a managed security services contract. [Reductions would be -$1,038,000 in 2015-16 and -$961,000 in 2016-17.]

ALT 2d	Change to Bill
PR	- $1,999,000

3. Delete provision.

ALT 3	Change to Bill
PR	- $5,199,000

Prepared by: Rachel Janke