State of Wisconsin
2023 - 2024 LEGISLATURE

LRB-1459/P4
MPG:skw

DOA:.....Sherwin, BB0335 – Cybersecurity Duties & Appropriations

FOR 2023-2025 BUDGET -- NOT READY FOR INTRODUCTION

AN ACT ...; **relating to:** the budget.

Analysis by the Legislative Reference Bureau

STATE GOVERNMENT

GENERAL STATE GOVERNMENT

Security operations centers

This bill requires DOA to establish one or more security operations centers to provide for the cybersecurity of information technology systems maintained by state agencies, local governmental units, and other eligible entities specified in the bill. The bill requires the Division of Enterprise Technology within DOA to manage the operation of the centers. The bill authorizes DOA to charge fees in connection with the division's cybersecurity support services provided under the bill.

For further information see the state fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 16.971 (2) (a) of the statutes is amended to read:

16.971 **(2)** (a) Ensure that an adequate level of information technology services is made available to all agencies by providing systems analysis and application

programming services to augment agency resources, as requested. The department shall also ensure that executive branch agencies, other than the board of regents of the University of Wisconsin System except for purposes of s. 16.978, make effective and efficient use of the information technology resources of the state. The department shall, in cooperation with agencies, including the board of regents for purposes of s. 16.978, establish policies, procedures and planning processes, for the administration of information technology services, which executive branch agencies, including the board of regents for purposes of s. 16.978, shall follow. The policies, procedures and processes shall address the needs of agencies, other than the board of regents of the University of Wisconsin System except for purposes of s. 16.978, to carry out their functions. The department shall monitor adherence to these policies, procedures and processes.

SECTION 2. 16.971 (2) (c) of the statutes is amended to read:

16.971 **(2)** (c) Develop and maintain procedures to ensure information technology resource planning and sharing between executive branch agencies, including the board of regents of the University of Wisconsin System for purposes of s. 16.978. The procedures shall ensure the interconnection of information technology resources of executive branch agencies, if interconnection is consistent with the strategic plans formulated under pars. (L) and (m).

SECTION 3. 16.971 (2) (j) of the statutes is amended to read:

16.971 **(2)** (j) Ensure that all executive branch agencies, including the board of regents of the University of Wisconsin System for purposes of s. 16.978, develop and operate with clear guidelines and standards in the areas of information technology systems development and that they employ good management practices and cost–benefit justifications.

SECTION 4. 16.971 (4) (a) of the statutes is amended to read:

16.971 **(4)** (a) The department may license or authorize executive branch agencies to license computer programs developed by executive branch agencies or security operations centers and regional security operations centers under s. 16.978 to the federal government, other states and municipalities. Any agency other than an executive branch agency may license a computer program developed by that agency to the federal government, other states and municipalities.

SECTION 5. 16.972 (2) (g) of the statutes is amended to read:

16.972 **(2)** (g) Assume direct responsibility for the planning and development of any information technology system in the executive branch of state government outside of the University of Wisconsin System, but including the University of Wisconsin System for purposes of s. 16.978, that the department determines to be necessary to effectively develop or manage the system, with or without the consent of any affected executive branch agency and the board of regents of the University of Wisconsin System for purposes of s. 16.978. The department may charge any executive branch agency and the board of regents for the department's reasonable costs incurred in carrying out its functions under this paragraph on behalf of that agency or a security operations center or regional security operations center under s. 16.978.

SECTION 6. 16.973 (3) of the statutes is amended to read:

16.973 **(3)** Facilitate the implementation of statewide initiatives, including development and maintenance of policies and programs to protect the privacy of individuals who are the subjects of information contained in the databases of agencies or security operations centers and regional security operations centers under s. 16.978, and of technical standards and sharing of applications among

agencies, security operations centers and regional security operations centers, and any participating local governmental units or other eligible entities, as defined in s. 16.978 (1) (c), or entities in the private sector.

SECTION 7. 16.973 (8) of the statutes is amended to read:

16.973 **(8)** Offer the opportunity to local governmental units and other eligible entities, as defined in s. 16.978 (1) (c), as determined by the department, to voluntarily obtain computer or supercomputer services from the department or a security operations center or regional security operations center under s. 16.978 when those services are provided under s. 16.972 (2) (b) or (c) or 16.978, and to voluntarily participate in any master contract established by the department or a security operations center or regional security operations center under s. 16.972 (2) (h) or 16.978 or in the use of any informational system or device provided by the department or a security operations center or regional security operations center under s. 16.974 (3) or 16.978.

SECTION 8. 16.978 of the statutes is created to read:

16.978 Security operations centers. (1) DEFINITIONS. In this section:

(a) Notwithstanding s. 16.97 (1m), "agency" includes each authority.

(b) "Division" means the division of enterprise technology in the department.

(c) "Eligible entity" means all of the following:

1. An agency.

2. A local governmental unit.

3. An educational agency, as defined in s. 16.99 (2g).

4. A federally recognized American Indian tribe or band located in this state.

5. A critical infrastructure entity, as determined by the division.

6. Any other entity identified by the department by rule.

(d) "Managed security services" means services intended to reduce the impact of cybersecurity threats.

(2) ESTABLISHMENT OF SECURITY OPERATIONS CENTERS. (a) The department shall 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 eligible entities.

(b) All security operations centers, including regional centers, established by the department shall be under the supervision and control of the division. The department shall include the centers in carrying out its responsibilities, powers, and duties under ss. 16.971 (2) (b), (c), (cm), (g), (h), and (k), 16.972 (2) (d) and (e), and 16.973 (1), (3), (4), and (5), as determined by the department.

(c) The department may coordinate with any of the following entities in the establishment of a security operations center or regional security operations center:

1. A campus, as defined in s. 36.05 (3).

2. A college campus, as defined in s. 36.05 (6m).

3. An institution, as defined in s. 36.05 (9).

4. A university, as defined in s. 36.05 (13).

(3) DUTIES OF THE DIVISION. (a) The division shall manage the operation of each security operations center and regional security operations center established under sub. (2), including by establishing managed security services guidelines and standard operating procedures for the operation of the centers.

(b) As appropriate and in coordination with participating eligible entities, the division may provide, and if provided, shall oversee the provision of, managed security services and other support through each security operations center and regional security operations center, including all of the following:

1. Real-time security monitoring to detect and respond to cybersecurity events that may jeopardize this state or the residents of this state.

2. Continuous, 24-hour alerts and guidance for defeating cybersecurity threats.

3. Immediate incident response to counter cyber activity that exposes this state or the residents of this state to cybersecurity risks.

4. Educational services regarding cybersecurity.

5. Dissemination of incident-related information to supported eligible entities, constituents, and external parties.

(c) In operating the security operations centers and regional security operations centers, including functions such as detecting, analyzing, responding to, and prioritizing responses to cybersecurity incidents, the division shall do all of the following:

1. Collaborate with any relevant state, local, federal, critical infrastructure, or tribal entity in accordance with statewide plans.

2. Lead executive branch agencies through cybersecurity incidents, including by directing and prioritizing cybersecurity incident responses, and provide guidance and expertise to other eligible entities that may be affected by such events.

3. If needed to respond to a substantial external cybersecurity threat, take any action, including disconnecting the computer network of an eligible entity receiving managed security services.

(d) The division shall ensure that each agency in the executive branch of state government uses the division's managed security services to the extent practicable. No executive branch agency may purchase managed security services from a person other than the department unless the division determines that the division cannot

provide comparable managed security services at a reasonable cost and the division approves the purchase. The division shall establish a process for making such determinations and approvals.

(4) POWERS OF THE DIVISION. The division may do all of the following:

(a) Enter into contracts and interagency agreements as necessary to administer this section.

(b) Apply for and use the proceeds from grants to administer this section.

(c) Charge fees to recover costs associated with the division's provision of managed security services and other cybersecurity support services provided under this section, including via an assessment to agencies or as a component of any services provided.

(5) CENTER FACILITIES. The division may establish a security operations center, including a regional center, only at a facility that satisfies all of the following:

(a) The facility is a secure and restricted facility that contains cybersecurity infrastructure, an available trained workforce, and supportive educational capabilities.

(b) All entrances and critical areas can be controlled and monitored to prevent unauthorized entry.

(c) Access can be limited to only authorized individuals.

(d) Security alarms can be monitored by local law enforcement or security companies according to service availability.

(e) Operational information can be restricted to personnel at the facility, except as coordinated and approved by both the division and the participating eligible entity.

SECTION 9. 20.505 (1) (fv) of the statutes is created to read:

20.505 **(1)** (fv) *Security operations centers.* The amounts in the schedule for the establishment and operation of security operations centers and regional security operations centers under s. 16.978.

****NOTE: This SECTION involves a change in an appropriation that must be reflected in the revised schedule in s. 20.005, stats.

SECTION 10. 20.505 (1) (jg) of the statutes is created to read:

20.505 **(1)** (jg) *Security operations centers; program revenues.* All moneys from fees charged under s. 16.978 (4) (c) for the operation of security operations centers and regional security operations centers under s. 16.978 and for the provision of services through those centers.

****NOTE: This SECTION involves a change in an appropriation that must be reflected in the revised schedule in s. 20.005, stats.

(END)