



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 1, 2023

Joint Committee on Finance

Paper #665

Cybersecurity Positions (Public Service Commission -- Departmentwide and Utility Regulation)

[LFB 2023-25 Budget Summary: Page 520, #3]

CURRENT LAW

The Division of Business Operations and Office Management within the Public Service Commission (PSC) is responsible for human resources and personnel management, budget and financial management, information technology, records management, staff development, space acquisition, and facilities development. Within the Division is the Office of Business and Information Technology (IT) Services. The Office of Business and IT Services contains 12.0 positions, and is responsible for managing, developing, and maintaining all of PSC's applications, databases, data warehouses, and reporting tools.

DISCUSSION POINTS

1. The National Institute of Standards and Technology (NIST) developed NIST 800-53, a set of guidelines to help federal agencies in the U.S. manage and secure their information systems and infrastructure, in September, 2020. NIST 800-53 guidelines are designed to help organizations protect their information and information systems from a variety of threats, such as cyberattacks, natural disasters, and human error. While NIST 800-53 was designed for federal agencies, it is a widely recognized standard for cybersecurity. PSC reports that the agency is working towards complying with NIST 800-53 standards, and reviewing current agency inventory and baseline configurations of all servers, applications, computers, and mobile devices.

2. In addition to NIST, in 2018, the U.S. Department of Energy (DOE) released a Multiyear Plan for Energy Cybersecurity and established an Office of Cybersecurity, Energy Security, and Emergency Response (CESER). DOE reports that the United States' energy infrastructure has become a target for cyberattacks in recent years, stating that cyberattacks have the potential to disrupt energy

services, damage highly-specialized equipment, and threaten human health and safety. The multiyear plan outlines strategies for improving cybersecurity nationwide and improving the resilience of the nation's energy system by: (a) strengthening energy sector cybersecurity preparedness; (b) coordinating cyber incident response and recovery; and (c) accelerating research and development of resilient energy delivery systems. In the plan, DOE calls upon state and local governments to be included in cybersecurity planning and response efforts.

3. PSC has identified cybersecurity as an agency focus in its latest Strategic Energy Assessment (SEA), covering the period between 2022 and 2028. PSC reports that Commission staff have participated in cybersecurity training to identify information-sharing mechanisms and define roles and responsibilities during potential cyber incidents. In September, 2020, Commission staff participated in cybersecurity training provided by the National Association of Regulatory Utility Commissioners (NARUC), focusing on managing cybersecurity risk within the NIST 800-53 framework. Additionally, in December, 2020, Wisconsin was one of four states to participate in DOE's CESER Liberty Eclipse exercise to support the Multiyear Plan for Energy Cybersecurity.

4. Assembly Bill 43/Senate Bill 70 would provide \$173,400 in 2023-24 and \$222,500 in 2024-25 with 2.0 positions in the Division of Business Operations and Office Management for supporting cybersecurity activities at PSC. PSC contends that the positions are necessary to comply with national cybersecurity standards, to improve overall cybersecurity status, and to improve PSC's ability to respond and recover from cybersecurity incidents.

5. One requested position would be dedicated to bringing cybersecurity perspectives to management of existing business processes, software development, and project management. Primary duties would include: (a) analyzing, documenting, and modeling relevant business processes to ensure alignment with NIST 800-53 standards; and (b) acting as a liaison with businesses and stakeholders in addressing cybersecurity risks and challenges for all IT projects. The second position would focus on cybersecurity risk mitigation support and primary duties would include: (a) supporting PhishNotify, the Commission's email phishing detection and quarantine software; (b) building and deploying phishing exercises; and (c) building and conducting incident response exercises.

6. PSC contends that 2.0 positions would fill ongoing needs in two distinct areas: (a) cybersecurity compliance in business processes and development; and (b) cybersecurity awareness and training. PSC states that having 2.0 positions dedicated to cybersecurity would also ensure sufficient resources to train additional employees in cybersecurity practices.

7. PSC intends with additional positions to control agency information more strictly by classifying and labeling information assets throughout the agency. PSC contends that this will impact document management systems, data warehouses, reporting infrastructure, applications and all system users. Due to the adoption of NIST 800-53 standards, PSC must implement specific controls for ensuring confidentiality and availability of systems, which PSC estimates could take significant time and effort.

8. Given the prevalence of cybersecurity concerns on the national and state level and PSC's intended efforts to improve cybersecurity in Wisconsin, the Committee could consider providing 2.0 positions to the agency [Alternative 1]. If the Committee determined that 1.0 position could be

sufficient to address cybersecurity goals outlined by PSC, the Committee could instead choose to provide 1.0 position [Alternative 2]. The Committee could also choose to take no action [Alternative 3].

ALTERNATIVES

1. Provide \$173,400 PR in 2023-24 and \$222,500 in 2024-25 and 2.0 positions in PSC's Office of Business and Information Technology Services to support cybersecurity activities.

ALT 1	Change to Base	
	Funding	Positions
PR	\$395,900	2.00

2. Provide \$86,700 PR in 2023-24 and \$111,300 in 2024-25 and 1.0 position in PSC's Office of Business and Information Technology Services to support cybersecurity activities.

ALT 2	Change to Base	
	Funding	Positions
PR	\$198,000	1.00

3. Take no action.

Prepared by: Margo Poelstra