HB 2049 STAFF MEASURE SUMMARY

Joint Committee On Information Management and Technology

Prepared By: Sean McSpaden, Committee Coordinator
Meeting Dates: 2/1, 2/8

WHAT THE MEASURE DOES:

House Bill 2049 establishes the Oregon Cybersecurity Center of Excellence within Portland State University to supplement the cybersecurity related activities of the State Chief Information Officer and to coordinate, fund, and provide cybersecurity workforce development, education, awareness, and training for public, private, and nonprofit sector organizations, and cybersecurity-related goods and services to Oregon public bodies with a targeted focus on the unmet needs of regional and local government, special districts, Education Service Districts, K-12 school districts and libraries. The measure directs Portland State University, Oregon State University and University of Oregon to jointly operate the center by agreement and to provide administrative and staff support and facilities for center operations. Further, the measure transfers the existing Oregon Cybersecurity Advisory Council from the office of Enterprise Information Services to the center and modifies the composition and duties, powers and functions of the Council to serve as the Advisory Body for the center.

House Bill 2049 establishes an Oregon Cybersecurity Center of Excellence Operating Fund and continuously appropriates moneys in the fund to the center to carry out the functions and operations of the center. The measure establishes an Oregon Cybersecurity Workforce Development Fund and continuously appropriates moneys in the fund to the center to invest in cybersecurity workforce development programs. The measure establishes an Oregon Cybersecurity Grant Program Fund and continuously appropriates moneys in the fund to the center to provide cybersecurity-related goods and services to Oregon public bodies. Further, the measure establishes an Oregon Cybersecurity Public Awareness Fund and continuously appropriates moneys in the fund to the center to raise public awareness regarding cybersecurity threats and resources to be safer and more secure online.

House Bill 2049 becomes operative October 1, 2023, declares emergency, and is effective on passage.

ISSUES DISCUSSED:

- Various aspects of House Bill 2049.
- City and Special District perspectives on ransomware attacks, cybersecurity vulnerabilities and challenges, and cybersecurity workforce gaps.
- K-12 School/Education Service District perspectives on cybersecurity threats, challenges, and cyberattacks experienced by Oregon's public schools/education service districts.
- Regional and local government, Special District, and K-12 School/Education Service District perspectives on cybersecurity insurance, the accelerating threat from malware and ransomware, cost of recovery from and response to a cyberattack, and cybersecurity workforce challenges facing Oregon public bodies.
- Increasing costs for and decreasing coverage included within cybersecurity insurance policies. Uncertainty in the cybersecurity insurance market.
- Need for immediate additional investments to help regional governments, local governments, special districts, schools, education service districts and libraries - IT modernization, cybersecurity, and workforce development and training.
- Need to better position Oregon to efficiently compete for and receive federal funding for cybersecurity. Belief that establishing the Cybersecurity Center of Excellence would help Oregon do that.
- Need for collaboration on cybersecurity across all sectors. Cybersecurity as a team activity; the cybersecurity challenges that exist are too many and too complex for any single organization to solve on their own.

- Collaboration, information sharing, and partnerships are key across Oregon's public, private, and non-profit sectors.

EFFECT OF AMENDMENT:

No amendment.

BACKGROUND:

Ransomware and other cyberattacks threaten the nation's critical infrastructure, economy and public health and safety. The threats from ransomware and other cyberattacks continue to worsen each day for public, private and nonprofit sector organizations operating in Oregon and across the nation. In the public sector - a whole of state approach involving coordinated cybersecurity planning, investment, and action across jurisdictions is required.

At the same time, Oregon and the nation face a shortage of qualified cybersecurity professionals to address these threats and vulnerabilities. According to cyberseek.org, an organization that provides detailed information on the cybersecurity job market across the nation, there are approximately 7,500 unfilled cyber jobs in Oregon across all sectors. In response, multiple cybersecurity workforce development and educational programs have been initiated within Oregon's public universities and community colleges over the past few years.

Oregon law (ORS 646A.600-646A.628) requires a business, state agency, or other "covered entity" to notify any Oregon consumer whose personal information, as defined, was subject to a breach of security. The law also requires that a sample copy of a breach notice sent to more than 250 Oregon consumers must also be provided to the Oregon Attorney General. The searchable database available on the Oregon Department of Justice Consumer Protection website indicates that 822 breach notices have been submitted from October 30, 2015 to January 20, 2023.

Oregon's local and regional governments, education service districts, school districts and libraries have recently completed a variety of assessments that identify critical cybersecurity vulnerabilities and information technology modernization needs they cannot meet alone.

PRELIMINARY