HB 2049 Cybersecurity Center of Excellence – Floor speech

Colleagues: today I ask for your support for House Bill 2049, a measure introduced by the Joint Committee on Information Management and Technology, designed to supplement the cybersecurity activities of the State Chief Information Officer, and specifically focused on serving the **unmet cybersecurity needs of Oregon's local governments, regional governments, special districts, education service districts, school districts and libraries.**

The threat of cyber warfare and ransomware is real and not just a theoretical discussion. In the event that some of you aren't watching the news releases, industry journal articles, and government security agency reports, here's a partial picture of the situation in Oregon.

Just in the past four months, two school districts, one city (Oregon City), one county (Curry County), one special district (Mapleton Water District), and a private college (Lewis and Clark College) have experienced cybersecurity incidents; several were ransomware attacks.

The DOJ Data Breach Reporting Database increased from 822 to 882 breach notifications from February 1, 2023 to today - with 60 breach notifications during that period of time - averaging nearly 1 breach notification every other day. Let me tell you just a few of those: Bank of Eastern Oregon, Asante, PayPal, Klamath County, The Springs Living, Mount Vernon Mills, Heritage Life Insurance, OnPoint Community Credit Union, Heceta Water People's Utility District, Epson Portland, and Treasure Valley Community College.

This bill has been several years in the making, and the concept has been the subject of public hearings and work with stakeholders since 2017.

It would launch a cybersecurity center of excellence jointly operated by three of Oregon's public universities to meet the challenge of nearly 7,000 unfilled, high paying cybersecurity jobs in Oregon, and help local governments, school districts and other public, non-profit, and private entities prepare for and defend against cyberattacks. Built into the concept is expanding to Oregon's other universities and community colleges as quickly as feasible. For example, OIT, offering Oregon's earliest curriculum in cybersecurity. Establishing or expanding cyber education and workforce development programs at WOU, SOU, and EOU. Expanding the Mount Hood Community College cyber certification scholarship fund program across Oregon's Community College system over time.

We have a unique opportunity to do something to help expand the workforce with proposed investments in cybersecurity workforce development programs at our public universities, community colleges, and high schools.

Our public, private, and non-profit entities will benefit exponentially from the expertise and hands-on "teaching hospital" model of learning, which allows for students to learn on the same software and equipment as they will use after completing the program and entering the workforce.

This bill also allows us to set aside state matching funds that will be needed to access the federal funds to help local governments. The initial appropriation in this bill is a good faith

investment, but (because the cyber risks we face are growing) we know more funding in this area will be needed in the next several legislative sessions.

Committee testimony included people representing nearly 30 public bodies, associations, and private tech sector representatives. Oregon's regional and local governments, special districts, education service districts, and K-12 schools and libraries are at risk. All are vulnerable to cyberattack, and they cannot, on their own, address the challenges they face.

There are 36 counties, more than 200 cities, 1,000 special districts, 19 education service districts, and 197 school districts that deliver services and oversee critical infrastructure. These organizations have their own data to secure, and many exchange information with other systems routinely, exposing them to greater risk. Smaller entities that can't afford full time cybersecurity personnel will have the ability to work with the Center which can conduct vulnerability assessments and offer cyber hygiene services to prevent a cross-domain attack.

And *we* – our state agencies – are vulnerable when *they* are. This is why it's important for state agencies. There are numerous connections where local and state computers are communicating with each other. Sending data, making queries of databases.

A few examples: local agencies accessing records for fingerprint checks for people applying for jobs working with children, vulnerable seniors, or financial information. Schools sending data to the Department of Education. Municipal governments depositing funds with State Treasury or sending information to the Homeless information system at Housing and Community Services. Department of Justice work with county District Attorneys on child support payments. Secretary of State managing voter registration and elections in coordination with county election offices; e-permitting with Building Codes Division.

The scale of this issue requires a whole-of-government approach, which is exactly what the Cybersecurity Center of Excellence has been designed to offer. A coordinated effort among governments, special districts, private enterprises, non-profits, and other community organizations is necessary to protect against, mitigate, respond to, and recover from cyber-attacks. Security is priceless…

House Bill 2049 is formally supported by over 40 public, private, and non-profit sector organizations, had five hearings in the Joint Committee on Information Management and Technology and was reported out with a do-pass recommendation to the Joint Committee on Ways and Means. On June 9, the full Joint Committee on Ways and Means voted unanimously to recommend House and Senate approval of HB 2049, as amended.

I ask for your support for this modest, essential investment to establish Oregon's Cybersecurity Center of Excellence.