LEAGUE OF WOMEN VOTERS® OF OREGON

The League of Women Voters of Oregon, established in 1920, is a grassroots nonpartisan political organization that encourages informed and active participation in government. We envision informed Oregonians participating in a fully accessible, responsive, and transparent government to achieve the common good. LWVOR Legislative Action is based on advocacy positions formed through studies and member consensus. The League never supports or opposes any candidate or political party.

February 22, 2023

To: **Co-Chairs Representative Nathanson and Senator Woods**

Joint Information Management and Technology

Re: **HB 2049** – Cybersecurity Center of Excellence, workforce development – **Support**

The League supports HB 2049's comprehensive efforts to address Oregon's growing cybersecurity vulnerability, with attacks increasing in frequency, criminal sophistication, and disruptive consequences. Our support echoes HB 4155 (2022) testimony, based on our cybersecurity position. We support government efficiency, evidenced in this bill's extensive collaboration to optimize efforts. The precisely targeted cybersecurity attacks described in hearings have disrupted critical government services we depend on. These can mushroom with dire consequences to our critical infrastructures. This warrants a third League position, to promote maximum protection of public health, safety, and the environment.

HB 2049 can assess and oversee needs, leverage funds, anticipate and facilitate protection with:

The Oregon Cybersecurity **Advisory Council**
The Oregon Cybersecurity **Center of Excellence**
The Oregon Cybersecurity **Workforce Development Fund**
The Oregon Cybersecurity **Public Awareness Fund**

Please consider abridged comments from this committee's extensive briefings. Cyberattacks and underlying weaknesses make us more vulnerable. Coordinating with partners will protect us. This bill brings together a comprehensive effort from government agencies seeking help to the private sector, working with academia, for learning from K-20 to work. We need critical cyber & IT modernization, along with current and long-term workforce development, and improved public awareness.

The PROBLEM: Few of us know how bad Oregon's paralyzing cybercrime is. Remote work today has connected our vulnerabilities. Ransomware damages are making budgets already strained by COVID impossible. With 7,557 cyber jobs open in Oregon, we're competing for trained staff, making hiring costs out of reach. Outdated systems, euphemistically called "legacy" make us more vulnerable. This huge exposure includes major infrastructures: our power grid, transportation, fire districts. water, and emergency communications. What if communications are blocked for 911, schools, and benefits like food stamps and childcare?

The first line of defense, cyber hygiene training, can stop 98% of these attacks and it is in the bill. We heard that 77% of special districts don't know how to encrypt or pay for data encryption. 66% don't use multi-factor authentication. Federal cyber grants require ".gov" email addresses, mostly not in use.

COST: This significant TAX is costing all of us. The average ransom is over $200,000. It may take months or longer to recover data and balance budgets that lack these cyber investments.
Tillamook County's ransomware attack took them offline for two weeks, despite paying $300,000 in ransom. Their in-bound email dropped off and stopped at day three. They estimated missing 45,000 phone calls over 4 days. They couldn't tell how they were infiltrated but their attackers had better customer services than most vendors, promptly delivering encryption keys. It took months to regain full operation.

A US Department of Justice letter shared that two leaders of "R Evil", the group that attacked them, were caught vacationing in eastern Europe, were extradited to the US, and are now in prison. But there would be no retrieval of our money, long since spent in Russia, the attackers' base.

The Glendale City Recorder, facing a ransom of $500 in bitcoin, worried about sewer outflow into their streams and said "SECURITY is PRICELESS". Glendale, in Douglas County, has a population of 863.

We may not be the weakest link. What if our Vendors are vulnerable? Attacks affecting multiple state agencies used the same providers. St Charles Hospital in Bend was attacked through their HR Vendor, with overnight, significant impact, lasting for 3 months! They had to manage the "incident", then clean up, with additional costs of re-entering data taken off line.

We can't do this alone. With HB 2049 we can efficiently compete for & get long-term federal infrastructure funds, short term local grants, and promote workforce development & public education. We can't protect ourselves against threats we don't understand. The goal is secure permanent, long-term, not one and done funding. If we don't act now, this will get MUCH WORSE.

We strongly urge your Support for HB 2049. Thank you for the opportunity to discuss this legislation.

Rebecca L. Gladstone

Rebecca Gladstone
Cybersecurity Advocate
President LWVOR

Norman Turrill

Norman Turrill
Governance Coordinator