

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.

March 21, 2025

To: [Representative Nancy Nathanson](#) and [Senator Aaron Woods](#), Co-Chairs

[Joint Committee On Information Management and Technology](#)

Re: [HB 3228](#) – Oregon Cybersecurity Council to study cybersecurity insurance – **SUPPORT**

The League of Women Voters of Oregon strongly supports HB 3228 with modifications based on our positions for cybersecurity and government efficiency, for flexible regulatory structures that can quickly adapt to social and scientific realities and technical and economic policy challenges. We appreciate that HB 3228 provides for

- A study from the Oregon Cybersecurity Advisory Council for state and local governments to use cybersecurity insurance.
- Also, an Oregon Cybersecurity Resilience Fund, separate from the General Fund, to assist in meeting insurance policy requirements and to prepare, plan for, mitigate, respond to, and recover from a 1 2 3 4 5 cyberattack, information security incident or data breach.

Cyber warfare and ransomware threats are not theoretical. Our increasingly digital government infrastructure is like plumbing; it also doesn't get much attention until there's a problem. This committee has heard from Oregon city and county folks sharing their devastating ransomware attacks. We know their rebuilding costs were much, much higher than getting help to set up protocols, train staff and monitor insurance requirements. Observing those protocols could avert the majority of attacks. The laudable track record since 2023 from the Oregon Cybersecurity Center of Excellence and Advisory Council makes this brisk study timeline attainable to help our folks understand what we're up against. ***Understanding how to budget for protection and preventive measures makes HB 3228 a must-have study.***

Getting cybersecurity insurance is not an end-run around responsible cyber hygiene; in fact, observing protocols is a policy requirement. Despite these precautions, policy costs have skyrocketed out of reach, policies are harder to find, and liability limits are shrinking. Now with federal safety net uncertainty, our supporting protections and preventive measures are necessary, not optional. Budget allocations for cyber hygiene could be superseded in negotiations, bypassed for more pressing "plumbing problems," making the Oregon Cybersecurity Resilience Fund invaluable.

However, the League urges the committee to consider expanding the scope of this bill to include artificial intelligence (AI) alongside cybersecurity considerations.

While cybersecurity is crucial, AI is rapidly becoming an equally important consideration for public bodies. AI technologies present interconnected risks and benefits that we should address in parallel. By expanding the bill's focus, we can ensure that Oregon's public institutions are prepared for the full spectrum of digital risks and opportunities.

1. **Evolving Threat Landscape:** Many modern cyberattacks leverage AI technologies, making it increasingly difficult to separate cybersecurity from AI security concerns.



NIST Risk Management Framework
Aims

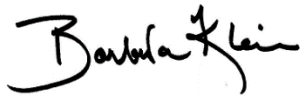
2. **Public Sector AI Adoption:** Oregon's public bodies are increasingly adopting AI systems for service delivery and operational efficiency. These systems introduce new risk vectors not traditionally covered by cybersecurity insurance (as noted under Insurance Gaps below).
3. **Insurance Gap:** Current cybersecurity insurance policies typically do not adequately address AI-specific risks, including algorithmic bias, automated decision-making errors, and AI system vulnerabilities.
4. **Comprehensive Protection:** A holistic approach that considers both cybersecurity and AI would better protect Oregon's public bodies and the people they serve.

To support this expansion, the League suggests these HB 3228 modifications:

1. Broaden the study mandate to include AI risks and insurance needs.
2. Rename the fund to "Oregon Digital Resilience Fund" to encompass both cybersecurity and AI.
3. Expand the Oregon Cybersecurity Center of Excellence's role to include AI expertise.

We strongly urge your support for HB 3228 with the recommended modifications.

Thank you for the opportunity to discuss this legislation.



Barbara Klein
Acting President, LWVOR



Lindsey Washburn
Artificial Intelligence



Rebecca Gladstone
Cybersecurity



Norman Turrill
Governance Coordinator