February 6, 2026

Senator Kahn Pham, Co-Chair
900 Court St. NE, S-407
Salem, OR 97301

Representative Nancy Nathanson, Co-Chair
900 Court St. NE, H-279
Salem, OR 97301

RE: League of Oregon Cities Opposition to HB 4055

Co-Chair Nathanson, Co-Chair Pham and members of the Joint Information Management and Technology Committee,

The League of Oregon Cities appreciates the opportunity to be before you today to respectfully express concerns with the 48-hour reporting requirements, fiscal challenges, and technical components related to reporting cyber-attacks in HB 4055.

The League's primary concern is that the 48-hour reporting requirement is too aggressive for IT departments of all sizes, but especially in small cities. 181 of Oregon's 241 incorporated cities are classified as small with limited budgets and resources. The 48-hour requirement diverts critical resources during investigation, containment and recovery. Additionally, it is likely that a city will still be seeking to understand what exactly they are dealing with, actively trying to control systems and determining what immediate and long-term mitigation strategies are needed to prevent future events.

The League respectfully asks this committee to consider amending HB 4055 to eliminate the 48-hour incident report mandate and substitute a simple notification to the State CIO within 72 hours of learning of a cyber-attack. Submission of the report through an electronic portal is appropriate, but we suggest adding dual/multifactor authentication for added security.

> Water System Breach: after discovering a cyber security breach a city will be testing to determine if the system has been contaminated or not, switching to manual operations, doing damage assessments, verifying the security of customer data, and bringing in OHA and EPA. To add a layer of reporting that does not immediately

> trigger support, technical or financial, is a departure from the immediate needs of the investigation.

The League is also concerned with the broad definition of what constitutes a reportable incident. As we read the definition of an "Information Security Incident," a regular operational outage could be classified under this definition.

The bill appears to grant the State CIO authority to share reported information with parties that office deems appropriate. Cybersecurity training emphasizes that public communications during an incident are critical to recovery efforts and liability mitigation. These communications are best managed in coordination with the agency's cyber insurance provider to ensure proper handling and coverage protection.

> Cities have seen in the past where the Water-ISAC's collection of breaches and incidents from critical infrastructure was compromised, resulting in the leakage of sensitive information for multiple agencies. Depending on the reporting data the state will require, this could result in additional risk for cities. We propose that the data be anonymized to remove the risk of that data being compromised.

Finally, the league requests HB 4055 be amended to encourage the State CIO's office to provide best-effort assistance to reporting entities during major incidents, leveraging the State's resources to aid in recovery efforts. Including this language will promote a culture of collaboration across government entities, potentially reducing the impact of incidents on affected agencies and the communities they serve.

Thank you,

Greg Miller
League of Oregon Cities