Chairs Pham, Nathanson and Members of the Committee,

We are writing to express the City's opposition to HB 4055 as currently written. This bill has been discussed during Oregon State cybersecurity workshops with peer agencies, and it is clear that the State's frustration with the lack of consistency and visibility surrounding cyber incidents is understandable. However, the approach outlined in HB 4055 raises concerns for local agencies like Lebanon.

HB 4055 would add a new requirement to the process that the City notify the State Chief Information Officer within 48 hours. While coordination is important, this additional reporting layer creates concerns rather than clarity. Our standard practice as a City in the event of an applicable breach is to immediately contact the CISA SOC, as we utilize CISA-provided antivirus and malware agents citywide, and our network is monitored through the ALBERT intrusion detection system. **In addition, we are already required to report applicable incidents to the Oregon State Police**.

At present, our engagement during a cybersecurity incident is voluntary and flexible. Depending on the nature of the incident, we may involve our cyber insurance provider, the U.S. Department of Homeland Security's CISA Security Operations Center (SOC), and/or the State of Oregon. The timing and order of notifications are incident-specific and based on best practices for response, recovery, and liability management.

The bill appears to grant the State CIO authority to share reported information with parties they deem 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— in our case, CIS — to ensure proper handling and coverage protection. Additionally, the bill appears to grant the State CIO broad authority to establish rules or take other actions necessary to carry out the act. While no penalties are explicitly listed, it is unclear whether enforcement mechanisms or penalties could later be established at the discretion of the State CIO. There is also uncertainty about whether reporting would trigger follow-up mandates directing specific response actions that could conflict with guidance from our insurance provider or Homeland Security's SOC.

Rather than creating a new reporting requirement for cities, a more effective, efficient approach would be **for the State CIO to obtain relevant incident information directly from existing reporting partners, such as Homeland Security CISA and the Oregon State Police.** Doing so would reduce duplication, maintain established response workflows, and still provide the State with necessary situational awareness.

If HB 4055 moves forward, we respectfully suggest that it:

- Limit the scope of rulemaking authority granted to the State CIO within this bill,
- Clearly define any penalties for noncompliance within the statute itself, and
- Clarify that reporting requirements will not result in conflicting response mandates for local agencies.

Thank you for your consideration and for your continued work on cybersecurity policy for Oregon.

Sincerely,

Brent Hurst
IT Director, City of Lebanon

Ron Whitlatch
City Manager