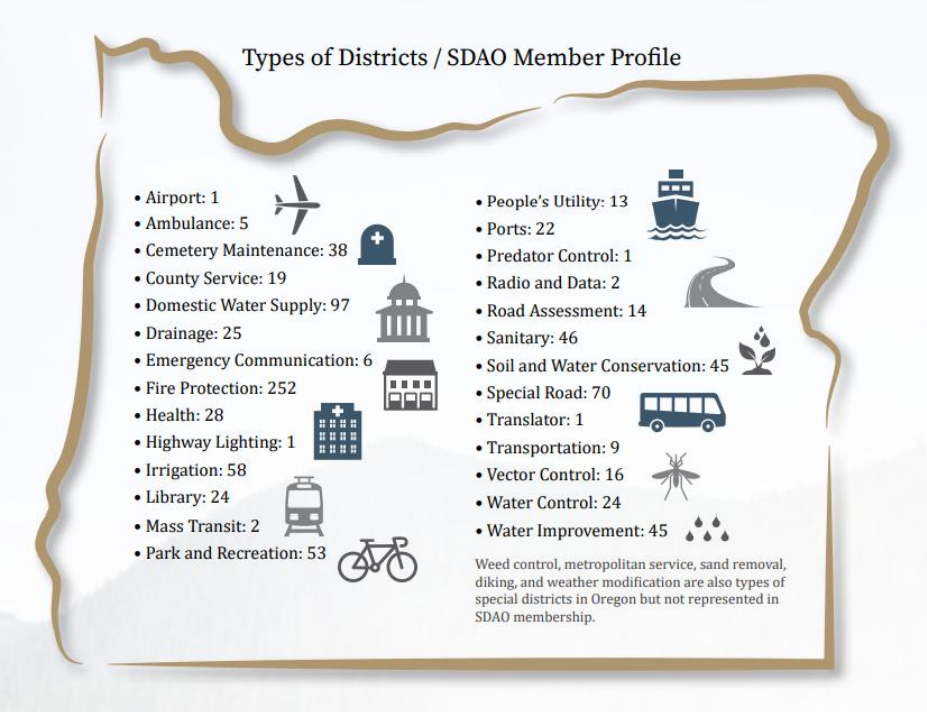
Joint Committee on Information Management and Technology
February 6, 2026
Special Districts Association of Oregon
HB 4055 – Support with Amendments

Thank you for the opportunity to provide testimony regarding HB 4055. My name is Hasina Wittenberg, and I serve as the Government Affairs Director for the Special Districts Association of Oregon (SDAO). SDAO represents approximately over 950 special districts throughout the state; a breakdown of our membership with labor and financial statistics is listed below:

- 34 types of special districts
- 4,350 locally elected volunteer board members
- 350 districts operate exclusively with volunteers
- 350+ districts with annual budgets under $100,000
- Special districts of some type provide services to nearly every Oregonian



HB 4055 Support and Suggested Timeline Changes

Currently, no statutory requirements exist that local governments report cyber security breaches/incidents to a central state government entity. We support mandating notification to a central state agency point of contact as described in HB 4055.

However, the provisions of HB 4055 require that **notification** occurs within 48 hours, and we **respectfully request that the timeline be increased to 72 hours**. This will allow our smaller, and potentially technologically limited members to properly navigate compliance with this new requirement.

Furthermore, HB 4055's provisions apply the 48 hour requirement to require that public bodies **submit a report** to the State CIO that **"describes the actions the public body has taken or must reasonably take to prevent, mitigate or recover from damage** to, unauthorized access to, unauthorized modifications or deletions of or other impairments of the integrity of the public body's information system." This requirement is not feasible and cannot reasonably be accomplished within a 48-hour timeframe. When an incident occurs local governments immediately attempt to prevent unauthorized access but submitting a report on how we have stopped the event may not be possible within 48 hours.

We suggest that if the intent is to require public bodies to **submit a report of action, we have taken to stop a cyber event that we are given at least 7 days** to do so. Furthermore, we request that we are given **at least 30 days to submit a report of actions we must reasonably take to mitigate or recover from damage**.

It appears to us that there are truly two different issues – 1) reporting what we have done to stop the attack and 2) what we are doing to mitigate and/or recover from the attack. Local governments aren't going to know within 48 hours how we plan to prevent, mitigate and recover from a cyber security attack. The events that unfold after a known incident occur involve other outside third parties (insurance carriers, technology consultants etc.) and pulling everyone together to identify the problem is one thing but developing a plan to prevent, mitigate and recover is an entirely different matter that should have a much longer time frame to comply with.

Thank you for the opportunity to testify and we look forward to working further on this important topic.