Co-Chairs Nathanson and Pham and Members of the Joint Information Management Technology Committee,

School districts and education service districts take cybersecurity seriously to protect our students, employees and communities interacting with schools. Many school districts band together with education service districts to pool resources for technology and IT support which makes coordination around cyber incidents easier. We understand the value of coordination being a foundational principle of cybersecurity as many public technology systems at different levels of government are interconnected. Thoughtful coordination can reduce overall risk.

We appreciate the intent of HB 4055 as introduced, which would provide notification to the state chief information officer of information security and ransomware incidents. However, we have some concerns. As you know, Oregon has many small public bodies. Of the 197 school districts in Oregon, nearly two-thirds are small districts – serving 1,650 students or fewer. Small school districts work with limited staff and resources. Sometimes, a small school employee may wear many hats at the same time like teacher, principal and IT administrator. On top of this, school districts are already required to submit close to 300 data collections and reports to the state throughout the year. We suggest the following amendments to HB 4055 to make it more workable for schools:

1. **Change the initial reporting requirements to 72 hours instead of 48 hours.** Small school districts will likely be balancing trying to stop a cyber incident while teaching or providing other key services to students. Extending the time to 72 hours will allow staff to work through handling the cyber incident instead of worrying about reporting.

2. **Tier what needs to be reported, and when, to ensure the best information can be provided.** Currently in the bill, the report would require the public agency to describe the actions it 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 all in that 48 hour period. We suggest having tiered reports. Within 72 hours a simple notification with limited details should be provided to alert the state to an attack. Within 7 business days, the public body should report more details of the attack and what actions it has taken to resolve the attack. Within 30 business days, the public body should report what actions it plans to take to mitigate and recover from damage and how to prevent future attacks.

3. **Consider tying notification to state resources or technical assistance capacity.** Many school districts would benefit from additional technical assistance from the state during a cyber incident. If notifying the state could trigger additional support that would be extremely valuable.

Respectfully,

COSA COALITION OF OREGON SCHOOL ADMINISTRATORS

OAESD OREGON ASSOCIATION OF EDUCATION SERVICE DISTRICTS

OREGON SCHOOL BOARDS ASSOCIATION

MESD

Northwest Regional Education Service District