SDAO Special Districts Association of Oregon

TO: Members of the Joint Committee on Information Management & Technology

FROM: Frank Stratton, Executive Director, Special Districts Association of Oregon

DATE: February 11, 2022

RE: **Testimony in Support of HB 4155**

Members of the Joint Committee on Information Management & Technology, thank you for the opportunity to submit written testimony in support of HB 4155 on behalf of the Special Districts Association of Oregon (SDAO). Our association was formed in 1978 and our membership consists of approximately 924 special service districts that provide a range of services (including but not limited to water, wastewater, irrigation, parks, and recreation, 9-1-1 and rural fire protection) statewide to citizens who reside within cities and in unincorporated communities.

There are 1,000+ special districts located in every region of the state. There are 34 types of special districts, and 4,350 locally elected volunteer board members govern these local governments. Our members provide services to nearly every Oregonian. 350 districts operate exclusively with volunteers and have budgets under $100,000.

HB 4140 would accomplish the following:

- Establish an Oregon Cybersecurity Center of Excellence (CCOE) charged with coordinating, funding, and providing cybersecurity workforce development, education, awareness and training and facilitating cybersecurity-related goods and services to Oregon public bodies focusing on the needs of regional and local government, special districts, ESDs, K-12 schools and libraries.

- Creates a 15-member council, comprised of a geographically diverse set of representatives would serve as the governing body for the CCOE moving forward.

- Directs PSU, OSU, and U of O to jointly operate the CCOE by an operating agreement, provide administrative and staff support and facilities for center operations.

- Authorize the CCOE to accept moneys from the federal government and other sources; and establish several targeted Funds to accomplish its mission.

A recent survey of 400 of our member districts further reveals the need and benefit HB 4155 would have on local government's ability to respond to and maintain cybersecurity (see page 2):

Survey Question	Responded "NO"
Does your district require all endpoint devices to be encrypted?	77%
Does your district provide users access to a password manager to store and create secure passwords?	74%
Does your district require multi-factor authentication for remote access (e.g., like a VPN and Email?)	66%
Does your district configure accounts to lock after 5 consecutive failed login attempts?	64%
Does your district ensure that only district owned devices are connected to the corporate wireless network (no personal devices)?	61%
Does your district require a minimum password length of no less than 8 characters?	50%
Does your district restrict users from being administrators on their workstations?	45%
Does your district ensure that the password to any corporate wireless network (not guest wireless) is not provided to end users, but is only known by key personnel?	39%
Does your district perform daily backups of all data that is essential to your operations?	37%
Does your district utilize a firewall between the district's internal network and any external, untrusted network (i.e., internet)?	36%
Does your district utilize a tool or service that monitors emails for malicious files, spam, and phishing emails?	36%
Does your district utilize an endpoint protection tool (sometimes referred to as antivirus) on all devices?	32%
Does your district maintain at least one copy of your data backups offsite (e.g. cloud or different facility)?	30%

As a result of this survey, we learned the following important lessons:

- Much of Oregon's critical infrastructure is operated by special districts
- Estimated that less than 50 special districts have fulltime IT staff
- Critical lack of financial recourses to address the problem
- Need funding to:
    - Provide statewide staff training on cyber awareness and social engineering
    - Purchase endpoint monitoring services
    - Implement multi-factor authentication
    - Consulting that includes security assessments and penetration testing
    - Uniform standards and training for administrators
- Mandates without financial support will not be feasible

Ransomware and other cyberattacks are continuing to increase in both the public and private sector. HB 4155 will assist in the development of properly trained cybersecurity professionals to address cybersecurity threats and vulnerabilities. The Infrastructure Investment and Jobs Act contains a state and local cybersecurity grant fund that is expected to provide Oregon with approximately $15 million in federal funding. HB 4155 will assist local government's ability to access that funding in a one-stop coordinated manner.

Thank you for the opportunity to submit testimony in support of HB 4155.