October 26, 2021

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

All sectors of Oregon's industry, public and private sectors, critical infrastructure, and citizens are increasingly under cyber-attack due to both an increased reliance on online services, and due to the increasing technical sophistication of criminals and hostile nations. No one is safe, and most organizations and citizens are vulnerable and under-defended. Currently, we are unable to rely on Federal, State or Local law enforcement to protect us. The problem has grown too large for any single organization or sector to solve this on our own: we must do it together.

Solving these problems requires many types of solutions in the realms of technical, process and policy, and requires addressing common, and unique problems across sectors. However, a prerequisite to implementing nearly all envisioned solutions is to address the lack of trained cybersecurity professionals – an issue that all sectors agree is a dire and critical need. Today, there are 4,000 unfilled cybersecurity openings in Oregon, and that number has grown by 36 per month for the past 30 months – the last time we updated JLCIMT. Our Oregon schools were behind 30 months ago and this supply-demand gap has now widened by an additional 1,000 graduates.

The State of Oregon is uniquely qualified to address this workforce issue for the good of all Oregonians. While this will not solve the problem by itself, doing nothing only exacerbates the problem. Conversely, rapidly growing our cybersecurity workforce has the potential to result in a myriad of benefits – including improving cybersecurity for all Oregonians, filling high-paying jobs with Oregonians, and even providing on-ramps to family-wage careers for underserved Oregonians.

Today, multiple fledging cybersecurity workforce development and educational programs stand ready and able to scale up to produce more qualified, trained graduates, but for lack of funding.

These programs include:

- **Awareness building.** To increase the supply of trained graduates, workforce development programs need increased awareness building to support student recruitment. The expansion of CyberOregon.com is one awareness program that can help address this need.
- **K-12 workforce pipeline building.** To develop a supply of interested students, experts believe that awareness, exposure and education must start in K-12. Stable funding (and expansion) of NW Cyber Camp is a key component to this strategy.
- **Improving Employability of Community College, 2-Year Programs Graduates.** Potential financial assistance for professional certification expenses, for students at leading Oregon community colleges, would substantially improve employability in cybersecurity for these students that include a high percentage of non-traditional, diverse, and veteran students. A limited pilot for this program is underway at Mt. Hood Community College but could be expanded state wide across Oregon's seventeen (17) community colleges.
- **Expansion of University Level Experiential Learning and Internship Programs.** Current programs at 4-year institutions can currently graduate just a small fraction of the needed workforce. Experiential and internship programs in cybersecurity serve just a handful of students today. Expanding and accelerating OSU's Oregon Research & Teaching Security Operations Center (ORTSOC) would provide a substantial boost to the number of qualified, highly-trained cyber graduates.
- **Coalition Building and Coordination.** Coordination between both educational institutions and statewide stakeholders is required to create a coherent workforce pipeline in cybersecurity, and ensure graduates are trained to meet stakeholder needs. Growing a policy coordination function under PSU's Hatfield School of Government, leveraging existing Federal funds, would provide a coordinating body that can serve this function.

Since the signing of SB 90 in September 2017, the current fiscal climate has never been stronger, and with the prospect of a positive State budget, as well as Federal funding programs specifically targeted for cybersecurity investment, we believe now is the time to allocate funds to grow these programs to meet Oregon's cybersecurity workforce needs, for the good of all Oregonians.

We, the undersigned entities, look forward to working with the Legislature to take a first step forward to improving our cybersecurity, by securing desperately needed funding, long overdue.

Sincerely,

Oregon Cybersecurity Advisory Council, Charlie Kawasaki, CISSP, Vice-Chair

Technology Association of Oregon, Skip Newberry, President and CEO

Oregon State University, Scott A. Ashford, Ph.D., P.E. (CA), Kearney Dean of Engineering

Portland State University, Professor Sy Adler, Interim Dean College of Urban and Public Affairs

Mt. Hood Community College, Dr. Lisa Skari, President; Dr. Al McQuarters, VP of Instruction

EnergySec (The Energy Sector Security Consortium, Inc.), Steve Parker, President