HB 4155 A STAFF MEASURE SUMMARY

Joint Committee On Information Management and Technology

Action Date:	02/18/22
Action:	Do pass with amendments and be referred to Ways and Means. (Printed A-Eng.)
House Vote	
Yeas:	2 - Marsh, Nathanson
Nays:	1 - George
Senate Vote	
Yeas:	2 - Armitage, Lawrence Spence
Nays:	1 - Boquist
Fiscal:	Fiscal impact issued
Revenue:	No revenue impact
Prepared By:	Sean McSpaden, Committee Coordinator
Meeting Dates:	2/11, 2/18

WHAT THE MEASURE DOES:

House Bill 4155 establishes the Oregon Cybersecurity Center of Excellence as an independent, nonprofit public corporation charged with overseeing, coordinating, funding and providing cybersecurity education, awareness and training for public, private and nonprofit sectors, cybersecurity workforce development and cybersecurity-related goods and services to Oregon public bodies with a targeted focus on the unmet needs of regional and local governments, special districts, education service districts, K-12 schools, and libraries. The measure directs Portland State University, Oregon State University and University of Oregon to jointly operate the center by agreement and to provide administrative and staff support and facilities for the center. Further, the measure authorizes these universities to operate the center as a virtual center, in whole or in part, and modifies the composition and duties, powers and functions of the Oregon Cybersecurity Advisory Council to serve as the governing body for the center.

House Bill 4155 establishes an Oregon Cybersecurity Center of Excellence Operating Fund and continuously appropriates moneys in the fund to the center to carry out the functions and operations of the center. The measure establishes an Oregon Cybersecurity Workforce Development Fund and continuously appropriates moneys in the fund to the center to invest in cybersecurity workforce development programs. The measure establishes an Oregon Cybersecurity Grant Program Fund and continuously appropriates moneys in the fund to the center to provide cybersecurity-related goods and services to Oregon public bodies. Further, the measure establishes an Oregon Cybersecurity Public Awareness Fund and continuously appropriates moneys in the fund to center to raise public awareness regarding cybersecurity threats and resources to be safer and more secure online.

House Bill 4155 becomes operative July 1, 2022, declares emergency, and is effective on passage.

ISSUES DISCUSSED:

- Various components of House Bill 4155
- State, City, County, and Special District perspectives on ransomware attacks, cybersecurity vulnerabilities and challenges, and cybersecurity workforce gaps.
- Regional and local government perspectives on cybersecurity insurance claims, the accelerating threat from malware and ransomware, cost of recovery from and response to a cyberattack, and cybersecurity workforce challenges facing regional and local governments

HB 4155 A STAFF MEASURE SUMMARY

- K-12 School/Education Service District perspectives on cybersecurity threats & challenges, and cyberattacks experienced by Oregon's public schools/education service districts.
- Community College perspectives on cybersecurity risks and challenges facing the education sector and cyberattacks experienced by Community Colleges.
- Private Sector Technology firm perspectives on cybersecurity threats and challenges facing state and local governments and all those in the education sector.
- Studies revealing that the education sector was the #1 target for cybersecurity attacks in 2021. State, regional, local governments and special districts have also been under near constant attack.
- Threats from ransomware, information system vulnerability exploitation, and cyberattacks on industrial control systems and the supply chain are increasing and are increasingly sophisticated. Legacy infrastructure and solutions, cyber workforce shortages, and legacy mindsets on cybersecurity exacerbate these problems.
- Need for immediate additional investments to help regional governments, local governments, special districts, schools, education service districts and libraries while federal grant monies are being secured over the next few years.
- Need to elevate cybersecurity risk management to boards and executives.
- Need for investments in cybersecurity workforce development and regional partnerships. Difficulty hiring, training, and retaining cybersecurity professionals.
- Need for increased investments in technical security systems, staff training & cybersecurity insurance. Current lack of dedicated budgets for IT modernization & cybersecurity.
- Need to better position Oregon to efficiently compete for and receive federal funding for cybersecurity. Belief that establishing the Cybersecurity Center of Excellence would help Oregon do that.
- The current imbalance between cyber attackers and cyber defenders. Defenders protecting legacy systems, using manual methods, and relying on scare cybersecurity staff, can't compete with cyber attackers with seemingly unlimited resources, using machine learning, artificial intelligence, and other automated methods of attack. Integrated, automated, and scalable solutions are needed in addition to increasing the supply of trained and certified cybersecurity professionals.
- Need to support smaller governments and municipalities that often lack adequate resources to provide effective cybersecurity.
- Increasing costs for and decreasing coverage included within cybersecurity insurance policies.
- Inadequate historical community college investments for cybersecurity and the need to increase those investments moving forward.
- Increasing collaboration among and between community college presidents and chief information officers on cybersecurity issues.
- Private technology firm education and training programs available at no-cost to Oregon's public universities, community colleges, K-12 Schools, and state/local governments.
- Efforts of Mount Hood Community College, Chemeketa Community College, Portland Community College and other Oregon community colleges related to cybersecurity education, training, and workforce development.
- Need for collaboration on cybersecurity across all sectors. Cybersecurity as a team activity; the cybersecurity challenges that exist are too many and too complex for any single organization to solve on their own. Collaboration, information sharing, and partnerships are key.
- Need for a sense of community in cyber defense; an increased cadence/tempo of cyber investments and activities; continuous improvement in cybersecurity defense capabilities; and, the use and delivery of evidence-based practices and outcomes.
- Infrastructure Investment and Jobs Act (IIJA) State and Local Cybersecurity Grant Program. Concern that the plan to apply for, receive and distribute the federal grant funds available to Oregon through this program, especially for federal FY 22, may not be developed and ready for execution in a timely manner.
- Concerns about establishment of the cybersecurity center of excellence within the introduced version of the bill as a non-profit public corporation and the potential challenges created by involvement of a public corporation in federal grant programs like the Infrastructure Investment and Jobs Act State and Local Cybersecurity Grant Program.

- Oregon Information Technology/Technology Systems Regional Resiliency Assessment Program (RRAP). Need to closely align the activities of the Cybersecurity Center of Excellence with this and other assessments of this kind.
- Need to identify and assess Oregon's critical infrastructure, and prioritize investments designed to protect that critical infrastructure from cyberattack.
- Need for private sector technology firms to continue to innovate and ensure their products stay a step ahead of cyber attackers over time.
- State agencies and organizations involved in state cybersecurity initiatives or that are authorized to apply for and receive federal grant funds from the U.S. Department of Homeland Security are many - e.g. the Governor's Office, Oregon Homeland Security Council, Oregon Office of Emergency Management, Oregon Department of Justice TITAN Fusion Center, State Executive Interoperability Council (SIEC), Oregon Broadband Office, State Chief Information Officer, etc.. Need for efforts to be coordinated and aligned.

EFFECT OF AMENDMENT:

-1 The amendment deletes Section 1 regarding legislative intent, and would repeal and replace, rather than modify, existing statutes related to the Oregon Cybersecurity Advisory Council and Oregon Cybersecurity Center of Excellence - i.e. ORS 276A.326 and ORS 276A.329, respectively. If adopted, the amendment would establish the Center at Portland State University with the Center to be operated under the joint direction and control of Portland State University, Oregon State University, and the University of Oregon. The amendment would, as a standard procedure, transfer the Council from the office of Enterprise Information Services, where it currently resides, to Portland State University, on behalf of the Center. As the public universities directed to jointly operate the Center already have established governing boards named in ORS 352.054, the amendment would modify the role of the Council to serve as the advisory council for the Center.

BACKGROUND:

Ransomware and other cyberattacks threaten the nation's critical infrastructure, economy and public health and safety. The threats from ransomware and other cyberattacks continue to worsen each day for public, private and nonprofit sector organizations operating in Oregon and across the nation.

At the same time, Oregon and the nation face a shortage of qualified cybersecurity professionals to address these threats and vulnerabilities with an estimated 4,000-5,000 unfilled cyber jobs in Oregon across all sectors. Multiple cybersecurity workforce development and educational programs have been initiated within Oregon's public universities and community colleges over the past few years, but the leaders of these programs indicate they are unable to scale up to produce more qualified, trained graduates rapidly enough to fill this gap, without additional funding.

Meanwhile, the Federal government, via the Infrastructure Investment and Jobs Act, has created the state and local cybersecurity grant fund. This is a non-competitive, formula-based grant program that is expected provide Oregon with approximately $15 million in federal funding (with required state matching funds) between federal FY 2022 and 2025. At least 80% of those funds must be distributed to local governments. Accessing those and other cybersecurity related grant funds will require coordinated governance, planning, grant application, distribution of funds, and project implementation among and between Oregon's state and local government representatives in the months and years to come.

Oregon's local and regional governments, education service districts, school districts and libraries have recently completed a variety of assessments that identify critical cybersecurity vulnerabilities and information technology modernization needs they cannot meet alone. They have asked for help from the Oregon Legislature and have indicated a willingness to work with state government, Oregon's public universities and community colleges, and others to address these problems via the proposed solutions contained within HB 4155.