Legislative Fiscal Office
83rd Oregon Legislative Assembly
2025 Regular Session

Prepared by: Michael Graham
Reviewed by: Sean McSpaden, Kim To
Date: April 17, 2025

Bill Title: Relating to cybersecurity; declaring an emergency.

Government Unit(s) Affected: Higher Education Coordinating Commission, Portland State University, Oregon State University, University of Oregon, Department of Administrative Services, Information Technology

Summary of Fiscal Impact

2025-27 Biennium	General Fund	Lottery Funds	Other Funds	Federal Funds	Total Funds	Positions	FTE
Higher Education Coordinating Commission	$ 1,743,600	$ -	$ -	$ -	$ 1,743,600	-	-
Total Fiscal Impact	**$ 1,743,600**	**$ -**	**$ -**	**$ -**	**$ 1,743,600**	-	-

2027-29 Biennium	General Fund	Lottery Funds	Other Funds	Federal Funds	Total Funds	Positions	FTE
Higher Education Coordinating Commission	$ -	$ -	$ -	$ -	$ -	-	-
Total Fiscal Impact	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	-	-

- The fiscal impact does not include duplicative Other Funds expenditure limitation necessary to expend General Fund revenue deposited into the Oregon Cybersecurity Resilience Fund. Additional Other Funds expenditure limitation will be needed to properly budget for the impact of the measure if it is adopted.

Measure Description
The measure directs the Oregon Cybersecurity Advisory Council to conduct assessments to identify and document cybersecurity vulnerabilities and recommend actions to address the reasons why public bodies throughout the state are unable to meet cybersecurity insurance coverage requirements. The advisory council shall submit a report to interim legislative committees related to information management and technology. The State Chief Information Officer and the Oregon Cybersecurity Center of Excellence (CCOE) shall provide staff and support services to the advisory council necessary for the advisory council to complete the assessments and report.

The measure establishes the Oregon Cybersecurity Resilience Fund, which is continuously appropriated to the Higher Education Coordinating Commission (HECC) for distribution to CCOE for the purpose of assisting public bodies with cybersecurity assessments, meeting cybersecurity insurance coverage requirements, providing cybersecurity training, and preparing for and responding to cyberattacks.

Fiscal Analysis
The fiscal impact of conducting a portion of the assessments required by the measure is $1.7 million General Fund in the 2025-27 biennium. Although the measure does not provide any funding, this fiscal impact assumes that the Oregon Cybersecurity Resilience Fund will be capitalized with General Fund. Once capitalized, HECC will

distribute moneys in the Oregon Cybersecurity Resilience Fund as pass-through funding to CCOE. To distribute this funding, HECC will need additional Other Funds expenditure limitation in the 2025-27 biennium.

Established by HB 2049 (2023), CCOE provides cybersecurity training, education and workforce development services, and assessment and monitoring services to public bodies, among other responsibilities. CCOE has identified over 1,500 public bodies, including cities, counties, school districts, special districts, and regional governments, that would be potential candidates for cybersecurity assessments and awareness trainings. However, because some public bodies already meet the requirements to obtain enhanced cybersecurity insurance coverage, CCOE would not provide assessments to all 1,500 public bodies. To ensure the assessments and the report to the Legislature can be completed by September 30, 2026, CCOE has proposed conducting assessments on a representative sample of approximately 400 public bodies with the greatest need for assistance. Assuming an average cost of $2,000 per assessment, the cost of the assessment and cybersecurity awareness training services, including technical and program management related personnel costs, is estimated at $1.7 million.

Based on the preliminary assessment findings, the Oregon Cybersecurity Advisory Council, assisted by CCOE and the State Chief Information Officer, expects to provide the Legislature with updated cost estimates for conducting additional assessments; cybersecurity awareness trainings; assisting public bodies in meeting cybersecurity insurance coverage requirements; and preparing and planning for, mitigating, responding to, and recovering from a cyberattack, information security incident, or data breach. However, until initial assessment findings and recommendations are reported to the Legislature, the potential one-time or ongoing cost of these additional activities is presently indeterminate.

The measure is anticipated to have a minimal fiscal impact on the Department of Administrative Services.

Relevant Dates

The measure declares an emergency and takes effect on passage.

The Oregon Cybersecurity Advisory Council is required to report to the Legislature by September 30, 2026.

Section 1 of the measure sunsets on January 2, 2027.