

FISCAL IMPACT OF PROPOSED LEGISLATION

Measure: HB 2049 - A4

82nd Oregon Legislative Assembly – 2023 Regular Session

Legislative Fiscal Office

Only Impacts on Original or Engrossed Versions are Considered Official

Prepared by: Michael Graham

Reviewed by: Sean McSpaden, Kim To, Julie Neburka, Amanda Beitel, Tom MacDonald, Paul Siebert

Date: June 5, 2023

Measure Description:

Establishes Cybersecurity Center of Excellence at Portland State University to be jointly operated by Portland State University, Oregon State University, and the University of Oregon. Transfers Oregon Cybersecurity Advisory Council from office of Enterprise Information Services to Oregon Cybersecurity Center of Excellence. Increases the number of Council members to 21 members, including 15 voting members and six nonvoting members. Specifies that legislative members of the Council are entitled to compensation and expense reimbursement.

Government Unit(s) Affected:

Higher Education Coordinating Commission, Public Universities, Department of Administrative Services, Office of the Governor, Cities, Counties, School Districts, Special Districts, Legislative Assembly

Summary of Fiscal Impact:

Costs related to the measure may require budgetary action - See analysis.

Summary of Expenditure Impact:

	2023-25 Biennium	2025-27 Biennium
General Fund		
Center of Excellence Operating Fund	\$2,500,000	\$0
Workforce Development Fund	\$2,150,000	\$0
Grant Program Fund	\$250,000	\$0
Total General Fund	\$4,900,000	\$0
Total Fiscal Impact	\$4,900,000	\$0

Analysis:

House Bill 2049, with the -A4 amendment, establishes the Oregon Cybersecurity Center of Excellence, the Oregon Cybersecurity Center of Excellence Operating Fund, the Oregon Cybersecurity Workforce Development Fund, and the Oregon Cybersecurity Grant Program Fund. The measure appropriates \$4.9 million General Fund to the Higher Education Coordinating Commission to be deposited into these three funds.

The Oregon Cybersecurity Center of Excellence will be established at Portland State University and operated under the joint direction and control of three founding universities - Portland State University, Oregon State University, and the University of Oregon. In addition, the universities are directed to establish the Oregon Cybersecurity Advisory Council to serve as an advisory council for the Center of Excellence.

The Center of Excellence is established to coordinate, fund, and provide education, awareness, and training for public, private, and non-profit sectors. The Oregon Cybersecurity Center of Excellence Operating Fund is established to fund the operations of the Center of Excellence. The measure provides \$2,500,000 General Fund in startup costs for the Center.

The Cybersecurity Workforce Development Fund provides monies to Oregon public bodies for workforce development, education, and training programs. The measure provides \$2,150,000 General Fund to fund the following programs:

- \$1,000,000 for the OSU CyberClinic (ORTSOC) program
- \$425,000 for University of Oregon Cyber Degree/Certificate programs
- \$350,000 for the Mount Hood Community College Cybersecurity Certification Scholarship Fund
- \$375,000 for the NW Cyber Camps program for high school students

The Oregon Cybersecurity Grant Program Fund is established to provide assessment, monitoring, incident response, and competitive grants to government bodies for cybersecurity-related goods and services. The measure provides \$250,000 General Fund to serve as state match in support of Oregon's application for federal funds available through the Infrastructure Investment and Jobs Act (IIJA) and State and Local Cybersecurity Grant Program (SLCGP) through the end of federal fiscal year 2025. However, the actual amount of available federal funding and required state match will not be known until the release of IIJA and SLCGP notices of funding opportunity for each federal fiscal year.

Moneys appropriated to the Cybersecurity Grant Program Fund over time will generally be distributed to public bodies following the submission of grant applications competitively evaluated by the Center through a process outlined in rules. Some moneys in this Fund, as is the case for this 2023 appropriation, may also be used as state matching funds for federal moneys related to cybersecurity grants applied for and received by public bodies. In some cases, applications to these federal grant programs may be submitted by the Center directly, or on behalf of another public body. In other cases, the State Chief Information Officer, the state administrative agency designated by the federal agency administering the grant program, or another state official (or designee) may be responsible for applying for various cybersecurity related federal grants on behalf of the state, the Center or another public body. The specific requirements of each federal grant program will govern the specific approach taken to meet grant application, funds distribution, management, and reporting requirements.