

House Bill 2049

Introduced and printed pursuant to House Rule 12.00. Pre-session filed (at the request of Joint Legislative Committee on Information Management and Technology)

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure **as introduced**.

Transfers Oregon Cybersecurity Advisory Council from office of Enterprise Information Services to Oregon Cybersecurity Center of Excellence. Modifies composition and duties, powers and functions of council.

Establishes Oregon Cybersecurity Center of Excellence within Portland State University to supplement activities of State Chief Information Officer regarding cybersecurity. Charges center with coordinating, funding or 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. Directs Portland State University, Oregon State University and University of Oregon to jointly operate center by agreement and to provide administrative and staff support and facilities for center.

Establishes Oregon Cybersecurity Center of Excellence Operating Fund. Continuously appropriates moneys in fund to Higher Education Coordinating Commission for distribution to center to carry out functions and operations of center.

Establishes Oregon Cybersecurity Workforce Development Fund. Continuously appropriates moneys in fund to commission for distribution to center to invest in cybersecurity workforce development programs.

Establishes Oregon Cybersecurity Grant Program Fund. Continuously appropriates moneys in fund to commission for distribution to center to provide cybersecurity-related goods and services to Oregon public bodies.

Establishes Oregon Cybersecurity Public Awareness Fund. Continuously appropriates moneys in fund to commission for distribution to center to raise public awareness regarding cybersecurity threats and resources to be safer and more secure online.

Becomes operative October 1, 2023.

Declares emergency, effective on passage.

A BILL FOR AN ACT

Relating to cybersecurity; creating new provisions; repealing ORS 276A.326 and 276A.329; and declaring an emergency.

Be It Enacted by the People of the State of Oregon:

OREGON CYBERSECURITY

(Definitions)

SECTION 1. Definitions. As used in this section and sections 3, 7 and 10 of this 2023 Act:

(1) **“Education service district” means a district created under ORS 334.010 that provides regional educational services to component school districts.**

(2) **“Library” means a public agency that provides free and equal access to library and information services that are suitable for persons of all ages.**

(3) **“Local government” means a city or county.**

(4) **“Public body” has the meaning given that term in ORS 174.109.**

(5) **“Regional government” means:**

(a) **A metropolitan service district formed under ORS chapter 268.**

(b) **An intergovernmental entity created by an intergovernmental agreement under ORS**

NOTE: Matter in **boldfaced** type in an amended section is new; matter *[italic and bracketed]* is existing law to be omitted. New sections are in **boldfaced** type.

1 **190.010.**

2 (6) "School district" has the meaning given that term in ORS 330.003.

3 (7) "Special district" means a district as defined in ORS 198.010.

4
5 (Oregon Cybersecurity Advisory Council)

6
7 **SECTION 2.** ORS 276A.326 is repealed and section 3 of this 2023 Act is enacted in lieu
8 thereof.

9 **SECTION 3. Oregon Cybersecurity Advisory Council.** (1) The Oregon Cybersecurity Ad-
10 visory Council is established within the Oregon Cybersecurity Center of Excellence. The
11 council consists of 15 voting members appointed by the Governor after consultation with the
12 State Chief Information Officer and the director of the Oregon Cybersecurity Center of Ex-
13 cellence or the director's designee. A majority of the council's voting members must be ge-
14 ographically diverse representatives of public universities listed in ORS 352.002, local
15 governments, regional governments, special districts, education service districts, school dis-
16 tricts or libraries.

17 (2) The membership of the council consists of:

18 (a) One member who represents Indian tribes, as defined in ORS 97.740;

19 (b) One member who represents the Association of Oregon Counties;

20 (c) One member who represents the League of Oregon Cities;

21 (d) One member who represents the Special Districts Association of Oregon;

22 (e) One member who represents regional governments;

23 (f) One member who represents the Oregon Association of Education Service Districts;

24 (g) One member who represents the Oregon School Boards Association;

25 (h) One member who represents the Coalition of Oregon School Administrators;

26 (i) One member who represents public universities listed in ORS 352.002;

27 (j) One member who represents community colleges;

28 (k) One member who represents the office of Enterprise Information Services;

29 (L) One member who represents a critical infrastructure sector in Oregon as defined by
30 the Cybersecurity and Infrastructure Security Agency of the United States Department of
31 Homeland Security;

32 (m) One member who represents cyber-related industries in Oregon;

33 (n) One member who represents a public sector information technology association in
34 Oregon; and

35 (o) One member who represents a private sector information technology or telecommu-
36 nications association in Oregon.

37 (3) The council shall elect one member of the council to serve as chairperson and one
38 member of the council to serve as vice chairperson.

39 (4)(a) A majority of the voting members of the council constitutes a quorum for the
40 transaction of business.

41 (b) Official action by the council requires the approval of a majority of the voting mem-
42 bers of the council.

43 (5)(a) The term of office of each voting member of the council is four years, but a
44 member serves at the pleasure of the Governor.

45 (b) Before the expiration of the term of a voting member, the Governor, after consulta-

1 tion with the State Chief Information Officer and the director of Oregon Cybersecurity
 2 Center of Excellence or the director's designee, shall appoint a successor whose term begins
 3 on July 1 following the appointment. A voting member is eligible for reappointment.

4 (c) If there is a vacancy for any cause, the Governor, after consultation with the State
 5 Chief Information Officer and the director of Oregon Cybersecurity Center of Excellence or
 6 the director's designee, shall make an appointment to become immediately effective for the
 7 unexpired term.

8 (6) The council shall meet at times and places specified by the call of the chairperson or
 9 a majority of the voting members of the council.

10 (7) Members of the council are not entitled to compensation, but the Oregon
 11 Cybersecurity Center of Excellence may reimburse a member of the council for actual and
 12 necessary travel and other expenses incurred in performing the member's official duties, in
 13 the manner and amounts provided for in ORS 292.495, from funds appropriated to the Higher
 14 Education Coordinating Commission for purposes of the council.

15 (8) The council may:

16 (a) Adopt rules, policies and procedures necessary for the operation of the council.

17 (b) Establish subcommittees, advisory committees or other work groups necessary to
 18 assist the council in performing its duties.

19 (c) Appoint nonvoting members to the council.

20 (9) All agencies of state government, as defined in ORS 174.111, are directed to assist the
 21 council in the performance of the council's duties and, to the extent permitted by laws re-
 22 lating to confidentiality, shall furnish information and advice the council considers necessary
 23 to perform the council's duties.

24 **SECTION 4. Initial terms.** Notwithstanding the term of office specified in section 3 of this
 25 2023 Act, of the members appointed to the Oregon Cybersecurity Advisory Council under
 26 section 3 of this 2023 Act:

27 (1) One-third shall serve for a term ending July 1, 2025.

28 (2) One-third shall serve for a term ending July 1, 2026.

29 (3) The remaining members shall serve for a term ending July 1, 2027.

30 **SECTION 5. Transfer.** (1) The duties, functions and powers of the office of Enterprise
 31 Information Services relating to the Oregon Cybersecurity Advisory Council are imposed
 32 upon, transferred to and vested in the Oregon Cybersecurity Center of Excellence, estab-
 33 lished under section 7 of this 2023 Act.

34 (2)(a) The State Chief Information Officer shall deliver to a representative of Portland
 35 State University, on behalf of the Oregon Cybersecurity Center of Excellence, all records and
 36 property within the jurisdiction of the officer that relate to the duties, functions and powers
 37 transferred by this section.

38 (b) A representative of Portland State University, on behalf of the Oregon Cybersecurity
 39 Center of Excellence, shall take possession of the records and property described in para-
 40 graph (a) of this subsection.

41 (c) The Governor shall resolve any dispute between the office of Enterprise Information
 42 Services and the Oregon Cybersecurity Center of Excellence relating to transfers of records
 43 and property under this subsection, and the Governor's decision is final.

44 (3)(a) The unexpended balances of amounts authorized to be expended by the office of
 45 Enterprise Information Services for the biennium beginning July 1, 2023, from revenues

1 dedicated, continuously appropriated, appropriated or otherwise made available for the pur-
 2 pose of administering and enforcing the duties, functions and powers transferred by this
 3 section are transferred to and are available for expenditure by Portland State University, on
 4 behalf of the Oregon Cybersecurity Center of Excellence for the biennium beginning July 1,
 5 2023, for the purpose of administering and enforcing the duties, functions and powers trans-
 6 ferred by this section.

7 (b) The expenditure classifications, if any, established by Acts authorizing or limiting
 8 expenditures by the office of Enterprise Information Services remain applicable to expen-
 9 ditures by Portland State University on behalf of the Oregon Cybersecurity Center of Excel-
 10 lence.

11
 12 (Oregon Cybersecurity Center of Excellence)

13
 14 **SECTION 6.** ORS 276A.329 is repealed and section 7 of this 2023 Act is enacted in lieu
 15 thereof.

16 **SECTION 7. Oregon Cybersecurity Center of Excellence.** (1) The Oregon Cybersecurity
 17 Center of Excellence is established at Portland State University. The center shall operate
 18 under the joint direction and control of Portland State University, Oregon State University
 19 and the University of Oregon. A director shall be appointed to oversee the center pursuant
 20 to procedures set forth in the charter developed and adopted under subsection (5) of this
 21 section.

22 (2) The purpose of the center is to supplement the activities of the State Chief Informa-
 23 tion Officer regarding cybersecurity in this state by coordinating, funding or providing:

24 (a) Awareness, education and training about cybersecurity and cybersecurity-related is-
 25 sues for public, private and nonprofit sectors;

26 (b) Cybersecurity workforce development programs in coordination with:

27 (A) Public universities listed in ORS 352.002;

28 (B) Community colleges operated under ORS chapter 341; and

29 (C) Science, technology, engineering and mathematics and career and technical education
 30 programs;

31 (c) Research about cybersecurity education and training methodologies;

32 (d) Research and development of cybersecurity technologies, tools, policies and processes;
 33 and

34 (e) Cybersecurity-related goods and services to Oregon public bodies, with priority given
 35 to local governments, regional governments, special districts, education service districts,
 36 school districts and libraries.

37 (3) The center shall:

38 (a) Serve as the statewide advisory body to the Legislative Assembly, Governor and State
 39 Chief Information Officer on cybersecurity and cybersecurity-related issues for local gov-
 40 ernments, regional governments, special districts, education service districts, school dis-
 41 tricts and libraries.

42 (b) Develop, update and submit biennially to the Governor and the appropriate commit-
 43 tees of the Legislative Assembly the Oregon Cybersecurity Resilience Plan described in sub-
 44 section (6) of this section.

45 (c) Provide to public, private and nonprofit sectors in this state information and recom-

1 **mend best practices concerning cybersecurity, cyber resilience and recovery measures, in-**
2 **cluding legal, insurance and other topics.**

3 **(d) Coordinate the sharing of information related to cybersecurity threats, risks,**
4 **warnings and incidents, and promote public awareness and shared, real-time situational**
5 **awareness among public, private and nonprofit sector entities.**

6 **(e) Provide cybersecurity assessment, scanning and analysis, monitoring and incident**
7 **response services to public bodies, with priority given to public bodies with the greatest need**
8 **for services, including local governments, regional governments, special districts, education**
9 **service districts, school districts and libraries.**

10 **(f) Collaborate with public bodies to coordinate cybersecurity efforts with ongoing infor-**
11 **mation technology modernization and resilience projects.**

12 **(g) Identify and participate in appropriate federal, multistate, regional, state, local or**
13 **private sector programs and efforts that support or complement the center's purpose.**

14 **(h) Pursue and leverage federal sources of cybersecurity and cyber resilience funding to**
15 **achieve state goals related to cybersecurity and cyber resilience.**

16 **(i) Manage and award funds distributed to the center for cybersecurity and cyber**
17 **resilience initiatives.**

18 **(j) Encourage the development of Oregon's cybersecurity workforce by, at a minimum:**

19 **(A) Identifying gaps and needs in workforce programs.**

20 **(B) Fostering the growth and development of cybersecurity workforce development pro-**
21 **grams and career and technical education in school districts, community colleges operated**
22 **under ORS chapter 341, and public universities listed in ORS 352.002.**

23 **(C) Assisting in curriculum review and standardization and providing recommendations**
24 **to improve programs.**

25 **(D) Fostering industry involvement in internships, mentorship and apprenticeship pro-**
26 **grams and experiential learning programs.**

27 **(E) Building awareness of industry and career opportunities to recruit students into**
28 **cyber-related educational tracks.**

29 **(4)(a) Portland State University, Oregon State University and the University of Oregon**
30 **shall enter into an operating agreement for administering the center, including the provision**
31 **of administrative and staff support and facilities.**

32 **(b) A public university listed in ORS 352.002, or a community college operated under ORS**
33 **chapter 341, not listed in paragraph (a) of this subsection may join the operating agreement**
34 **and provide administrative and staff support and facilities. The process for joining the oper-**
35 **ating agreement shall be described in the operating agreement or the charter developed un-**
36 **der subsection (5) of this section.**

37 **(5) Portland State University, Oregon State University and the University of Oregon, in**
38 **consultation with the Oregon Cybersecurity Advisory Council, shall develop and adopt a**
39 **charter to serve as the governing document for the center. The charter must contain pro-**
40 **visions regarding the center's operations, budget and any funds administered by the center**
41 **and the procedures for appointing the director to oversee the center. Portland State Uni-**
42 **versity, Oregon State University and the University of Oregon shall annually review and, as**
43 **necessary, update the charter.**

44 **(6) The Oregon Cybersecurity Resilience Plan developed and updated under this section**
45 **must, at a minimum:**

1 (a) Identify cybersecurity risks in critical infrastructure, local governments, regional
2 governments, special districts, education service districts, school districts and libraries;

3 (b) Establish risk-based assessment procedures;

4 (c) Survey and identify technology and process gaps and provide recommendations to
5 address the gaps;

6 (d) Survey public awareness, educational, training and workforce development programs
7 and provide recommendations to improve the programs; and

8 (e) Provide financial estimates and impacts associated with the cost of implementing or
9 not implementing recommendations, including pilot programs and statewide implementation.

10 (7) The center shall, in consultation with the council:

11 (a) Develop and update every four years a strategic plan, including goals and objectives,
12 for the center.

13 (b) Develop and submit a report on the center's strategic goals and objectives, operations
14 and funding requests for continued operations and funds administered by the center, to the
15 Governor and to the appropriate committees of the Legislative Assembly, in the manner re-
16 quired by ORS 192.245, by February 1 of each odd-numbered year. The report must identify
17 any grants, donations, gifts or other forms of conveyances of land, money, real or personal
18 property or other valuable thing made to the state or the center for carrying out the pur-
19 poses of the center.

20 (c) Provide a statewide forum for discussing and resolving cybersecurity issues.

21 (8) All agencies of state government, as defined in ORS 174.111, are directed to assist the
22 center in the performance of the center's duties and, to the extent permitted by laws relating
23 to confidentiality, shall furnish information and advice the center considers necessary to
24 perform the center's duties.

25 **SECTION 8. Center operating fund.** (1) The Oregon Cybersecurity Center of Excellence
26 Operating Fund is established in the State Treasury, separate and distinct from the General
27 Fund. Interest earned by the Oregon Cybersecurity Center of Excellence Operating Fund
28 must be credited to the fund.

29 (2) Moneys in the fund shall consist of:

30 (a) Amounts donated to the fund;

31 (b) Amounts appropriated or otherwise transferred to the fund by the Legislative As-
32 sembly; and

33 (c) Other amounts deposited in the fund from any source.

34 (3) Moneys in the fund are continuously appropriated to the Higher Education Coordi-
35 nating Commission for distribution to the Oregon Cybersecurity Center of Excellence for the
36 purposes of carrying out the functions and operations of the center.

37 (4) The center shall submit to the Governor and to the appropriate committees of the
38 Legislative Assembly, in the manner provided under ORS 192.245, a biennial report that
39 summarizes the balance of the fund, lists the deposits into and expenditures from the fund
40 and provides such other details as necessary regarding the operation of the fund.

41 **SECTION 9. Cybersecurity workforce development fund.** (1) The Oregon Cybersecurity
42 Workforce Development Fund is established in the State Treasury, separate and distinct
43 from the General Fund. Interest earned by the Oregon Cybersecurity Workforce Develop-
44 ment Fund must be credited to the fund.

45 (2) Moneys in the fund shall consist of:

1 (a) Amounts donated to the fund;

2 (b) Amounts appropriated or otherwise transferred to the fund by the Legislative As-
3 sembly; and

4 (c) Other amounts deposited in the fund from any source.

5 (3) Moneys in the fund are continuously appropriated to the Higher Education Coordi-
6 nating Commission for distribution to the Oregon Cybersecurity Center of Excellence for the
7 purposes of making targeted investments in workforce development programs designed to
8 accelerate the growth, qualifications and availability of Oregon's cybersecurity workforce.

9 (4) The center shall submit to the Governor and to the appropriate committees of the
10 Legislative Assembly, in the manner provided under ORS 192.245, a biennial report that
11 summarizes the balance of the fund, lists the deposits into and expenditures from the fund
12 and provides such other details as necessary regarding the operation of the fund.

13 **SECTION 10. Cybersecurity grant program fund.** (1) The Oregon Cybersecurity Grant
14 Program Fund is established in the State Treasury, separate and distinct from the General
15 Fund. Interest earned by the Oregon Cybersecurity Grant Program Fund must be credited
16 to the fund.

17 (2) Moneys in the fund shall consist of:

18 (a) Amounts donated to the fund;

19 (b) Amounts appropriated or otherwise transferred to the fund by the Legislative As-
20 sembly; and

21 (c) Other amounts deposited in the fund from any source.

22 (3) Moneys in the fund are continuously appropriated to the Higher Education Coordi-
23 nating Commission for distribution to the Oregon Cybersecurity Center of Excellence for the
24 purposes of providing:

25 (a) Cybersecurity assessment, scanning and analysis, monitoring, incident response and
26 technical assistance and other cybersecurity-related goods and services to Oregon public
27 bodies on a competitive basis with specific emphasis on serving the unmet needs of local
28 governments, regional governments, special districts, education service districts, school dis-
29 tricts and libraries.

30 (b) Matching funds for federal moneys related to cybersecurity received by public bodies.

31 (4) The center shall adopt standards, objectives, criteria and eligibility requirements for
32 the use of moneys distributed from the fund. In developing criteria and eligibility standards,
33 the center shall take into consideration any requirements of federal programs awarding
34 moneys related to cybersecurity.

35 (5) The center shall submit to the Governor and to the appropriate committees of the
36 Legislative Assembly, in the manner provided under ORS 192.245, a biennial report that
37 summarizes the balance of the fund, lists the deposits into and expenditures from the fund
38 and provides such other details as necessary regarding the operation of the fund.

39 **SECTION 11. Cybersecurity public awareness fund.** (1) The Oregon Cybersecurity Public
40 Awareness Fund is established in the State Treasury, separate and distinct from the General
41 Fund. Interest earned by the Oregon Cybersecurity Public Awareness Fund must be credited
42 to the fund.

43 (2) Moneys in the fund shall consist of:

44 (a) Amounts donated to the fund;

45 (b) Amounts appropriated or otherwise transferred to the fund by the Legislative As-

1 assembly; and

2 (c) Other amounts deposited in the fund from any source.

3 (3) Moneys in the fund are continuously appropriated to the Higher Education Coordi-
4 nating Commission for distribution to the Oregon Cybersecurity Center of Excellence for the
5 purposes of raising public awareness about the importance of cybersecurity across Oregon
6 and ensuring that Oregonians better understand existing threats and have the information
7 and resources to be safer and more secure online.

8 (4) The center shall submit to the Governor and to the appropriate committees of the
9 Legislative Assembly in the manner provided under ORS 192.245, a biennial report that
10 summarizes the balance of the fund, lists the deposits into and expenditures from the fund
11 and provides such other details as necessary regarding the operation of the fund.

12
13 (Deadlines)

14
15 **SECTION 12.** (1) The Oregon Cybersecurity Resilience Plan described in section 7 (6) of
16 this 2023 Act is first due no later than December 31, 2025.

17 (2) The biennial reports described in sections 8, 9, 10 and 11 of this 2023 Act are first due
18 no later than December 31, 2025.

19 **SECTION 13.** Section 12 of this 2023 Act is repealed on January 2, 2026.

20
21 **APPROPRIATIONS**

22
23 **SECTION 14.** (1) In addition to and not in lieu of any other appropriation, there is ap-
24 propriated to the Higher Education Coordinating Commission, for the biennium beginning
25 July 1, 2023, out of the General Fund, the amount of \$_____, to be deposited into the Oregon
26 Cybersecurity Center of Excellence Operating Fund established under section 8 of this 2023
27 Act.

28 (2) In addition to and not in lieu of any other appropriation, there is appropriated to the
29 Higher Education Coordinating Commission, for the biennium beginning July 1, 2023, out of
30 the General Fund, the amount of \$_____, to be deposited into the Oregon Cybersecurity
31 Workforce Development Fund established under section 9 of this 2023 Act.

32 (3) In addition to and not in lieu of any other appropriation, there is appropriated to the
33 Higher Education Coordinating Commission, for the biennium beginning July 1, 2023, out of
34 the General Fund, the amount of \$_____, to be deposited into the Oregon Cybersecurity
35 Grant Program Fund established under section 10 of this 2023 Act.

36 (4) In addition to and not in lieu of any other appropriation, there is appropriated to the
37 Higher Education Coordinating Commission, for the biennium beginning July 1, 2023, out of
38 the General Fund, the amount of \$_____, to be deposited into the Oregon Cybersecurity
39 Public Awareness Fund established under section 11 of this 2023 Act.

40
41 **CAPTIONS**

42
43 **SECTION 15.** The unit and section captions used in this 2023 Act are provided only for
44 the convenience of the reader and do not become part of the statutory law of this state or
45 express any legislative intent in the enactment of this 2023 Act.

OPERATIVE AND EFFECTIVE DATES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

SECTION 16. (1) Sections 1, 3 to 5 and 7 to 12 of this 2023 Act and the repeal of ORS 276A.326 and 276A.329 by sections 2 and 6 of this 2023 Act become operative on October 1, 2023.

(2) The Governor, the State Chief Information Officer, the Oregon Cybersecurity Advisory Council, Portland State University, Oregon State University and the University of Oregon may take any action before the operative date specified in subsection (1) of this section that is necessary to enable the Governor, the State Chief Information Officer, the Oregon Cybersecurity Advisory Council, Portland State University, Oregon State University and the University of Oregon to exercise, on and after the operative date specified in subsection (1) of this section, all of the duties, functions and powers conferred on the Governor, the State Chief Information Officer, the Oregon Cybersecurity Advisory Council, Portland State University, Oregon State University and the University of Oregon by sections 1, 3 to 5 and 7 to 12 of this 2023 Act and the repeal of ORS 276A.326 and 276A.329 by sections 2 and 6 of this 2023 Act.

SECTION 17. This 2023 Act being necessary for the immediate preservation of the public peace, health and safety, an emergency is declared to exist, and this 2023 Act takes effect on its passage.
