

**A-Engrossed**  
**House Bill 4155**

Ordered by the House February 21  
Including House Amendments dated February 21

Sponsored by COMMITTEE ON RULES (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.

**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 [*Oregon Cybersecurity Advisory Council as governing body of Oregon Cybersecurity Center of Excellence*] **council.**

Establishes Oregon Cybersecurity Center of Excellence [*as independent, nonprofit public corporation charged with overseeing,*] **within Portland State University to supplement activities of State Chief Information Officer regarding cybersecurity. Charges center with** coordinating, funding [*and*] **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. [*Authorizes universities to operate center as virtual center, in whole or in part.*]

Establishes Oregon Cybersecurity Center of Excellence Operating Fund. Continuously appropriates moneys in fund to center to carry out functions and operations of center.

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

Establishes Oregon Cybersecurity Grant Program Fund. Continuously appropriates moneys in fund 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 center to raise public awareness regarding cybersecurity threats and resources to be safer and more secure online.

Becomes operative July 1, 2022.

Declares emergency, effective on passage.

**A BILL FOR AN ACT**

1  
2 Relating to cybersecurity; creating new provisions; repealing ORS 276A.326 and 276A.329; and de-  
3 claring an emergency.

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

5  
6 **OREGON CYBERSECURITY**

7 **(Definitions)**

8  
9 **SECTION 1. Definitions. As used in sections 3, 7 and 10 of this 2022 Act:**

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

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

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

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

3 (5) “Regional government” means a metropolitan service district formed under ORS  
4 chapter 268.

5 (6) “School district” has the meaning given that term in ORS 330.003.

6 (7) “Special district” means a district as defined in ORS 198.010.

7  
8 (Oregon Cybersecurity Advisory Council)

9  
10 **SECTION 2.** ORS 276A.326 is repealed and section 3 of this 2022 Act is enacted in lieu  
11 thereof.

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

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

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

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

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

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

24 (e) One member who represents regional governments;

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

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

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

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

29 (j) One member who represents community colleges;

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

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

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

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

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

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

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

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

45 (5)(a) The term of office of each voting member of the council is four years, but a

1 member serves at the pleasure of the Governor.

2 (b) Before the expiration of the term of a voting member, the Governor, after consulta-  
3 tion with the State Chief Information Officer, shall appoint a successor whose term begins  
4 on July 1 following the appointment. A voting member is eligible for reappointment.

5 (c) If there is a vacancy for any cause, the Governor, after consultation with the State  
6 Chief Information Officer, shall make an appointment to become immediately effective for  
7 the 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 center may reim-  
11 burse a member of the council for actual and necessary travel and other expenses incurred  
12 in performing the member's official duties, in the manner and amounts provided for in ORS  
13 292.495, from funds appropriated to the Higher Education Coordinating Commission for pur-  
14 poses of the council or the center.

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 2022 Act, of the members appointed to the Oregon Cybersecurity Advisory Council by section  
26 3 of this 2022 Act:

27 (1) One-third shall serve for a term ending July 1, 2024.

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

29 (3) The remaining members shall serve for a term ending July 1, 2026.

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 2022 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 Systems 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 Systems for the biennium ending June 30, 2023, from revenues dedi-

1 cated, continuously appropriated, appropriated or otherwise made available for the purpose  
2 of administering and enforcing the duties, functions and powers transferred by this section  
3 are transferred to and are available for expenditure by Portland State University, on behalf  
4 of the Oregon Cybersecurity Center of Excellence for the biennium ending June 30, 2023, for  
5 the purpose of administering and enforcing the duties, functions and powers transferred by  
6 this section.

7 (b) The expenditure classifications, if any, established by Acts authorizing or limiting  
8 expenditures by the office of Enterprise Information Systems 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 2022 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.

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

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

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

25 (A) Public universities listed in ORS 352.002;

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

27 (C) Science, technology, engineering and mathematics and career and technical education  
28 programs;

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

30 (d) Research and development of cybersecurity technologies, tools, policies and processes;  
31 and

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

35 (3) The center shall:

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

40 (b) Develop, update and submit biennially to the Governor and the appropriate commit-  
41 tees of the Legislative Assembly the Oregon Cybersecurity Modernization Plan described in  
42 subsection (6) of this section.

43 (c) Provide to public, private and nonprofit sectors in this state information and recom-  
44 mend best practices concerning cybersecurity, cyber resilience and recovery measures, in-  
45 cluding legal, insurance and other topics.

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

4 (e) Provide cybersecurity assessment, monitoring and incident response services to public  
5 bodies, with priority given to public bodies with the greatest need for services, including local  
6 governments, regional governments, special districts, education service districts, school dis-  
7 tricts and libraries.

8 (f) Collaborate with public bodies to coordinate cybersecurity efforts with ongoing infor-  
9 mation technology modernization projects.

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

12 (h) Pursue and leverage federal sources of cybersecurity and cyber resilience funding to  
13 achieve state goals related to cybersecurity and cyber resilience.

14 (i) Manage and award funds distributed to the center for cybersecurity and cyber  
15 resilience initiatives.

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

17 (A) Identifying gaps and needs in workforce programs.

18 (B) Fostering the growth and development of cybersecurity workforce development pro-  
19 grams and career and technical education in school districts, community colleges and public  
20 universities listed in ORS 352.002.

21 (C) Assisting in curriculum review and standardization and providing recommendations  
22 to improve programs.

23 (D) Fostering industry involvement in internships, mentorship and apprenticeship pro-  
24 grams and experiential learning programs.

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

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

30 (b) A public university listed in ORS 352.002 or community college in Oregon not listed  
31 in paragraph (a) of this subsection may join the operating agreement and provide adminis-  
32 trative and staff support and facilities.

33 (5) Portland State University, Oregon State University and the University of Oregon, in  
34 consultation with the Oregon Cybersecurity Advisory Council, shall develop a charter to  
35 serve as the governing document for the center. The charter must contain provisions re-  
36 garding the center's operations, budget and any funds administered by the center. Portland  
37 State University, Oregon State University and the University of Oregon shall annually review  
38 and, as necessary, update the charter.

39 (6) The Oregon Cybersecurity Modernization Plan developed and updated under this sec-  
40 tion must, at a minimum:

41 (a) Identify cybersecurity risks in critical infrastructure, local governments, school dis-  
42 tricts and public sector entities;

43 (b) Establish risk-based assessment procedures;

44 (c) Survey and identify technology and process gaps and provide recommendations to  
45 address the gaps;

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

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

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

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

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

15 (c) Establish, in consultation with the State Chief Information Officer, a statewide  
16 cybersecurity planning committee that meets the purpose, composition and cybersecurity  
17 expertise requirements described in the Infrastructure Investment and Jobs Act (P.L.  
18 117-58).

19 (d) Provide a statewide forum for discussing and resolving cybersecurity issues.

20 (8) 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 8. Center operating fund.** (1) The Oregon Cybersecurity Center of Excellence  
25 Operating Fund is established in the State Treasury, separate and distinct from the General  
26 Fund. Interest earned by the Oregon Cybersecurity Center of Excellence Operating Fund  
27 must be credited to the fund.

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

29 (a) Amounts donated to the fund;

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

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

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

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

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

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

45 (a) Amounts donated to the fund;

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

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

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

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

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

17 (a) Amounts donated to the fund;

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

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

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

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

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

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

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

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

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

42 (a) Amounts donated to the fund;

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

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

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

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

10  
11 (Deadlines)

12  
13 **SECTION 12.** (1) The Oregon Cybersecurity Modernization Plan described in section 7 (6)  
14 of this 2022 Act is first due no later than September 15, 2024.

15 (2) The biennial reports described in sections 8, 9, 10 and 11 of this 2022 Act are first due  
16 no later than September 15, 2024.

17  
18 **APPROPRIATIONS**

19  
20 **SECTION 13.** (1) In addition to and not in lieu of any other appropriation, there is ap-  
21 propriated to the Higher Education Coordinating Commission, for the biennium ending June  
22 30, 2023, out of the General Fund, the amount of \$\_\_\_\_\_, to be deposited into the Oregon  
23 Cybersecurity Center of Excellence Operating Fund established under section 8 of this 2022  
24 Act.

25 (2) In addition to and not in lieu of any other appropriation, there is appropriated to the  
26 Higher Education Coordinating Commission, for the biennium ending June 30, 2023, out of the  
27 General Fund, the amount of \$\_\_\_\_\_, to be deposited into the Oregon Cybersecurity  
28 Workforce Development Fund established under section 9 of this 2022 Act.

29 (3) In addition to and not in lieu of any other appropriation, there is appropriated to the  
30 Higher Education Coordinating Commission, for the biennium ending June 30, 2023, out of the  
31 General Fund, the amount of \$\_\_\_\_\_, to be deposited into the Oregon Cybersecurity Grant  
32 Program Fund established under section 10 of this 2022 Act.

33 (4) In addition to and not in lieu of any other appropriation, there is appropriated to the  
34 Higher Education Coordinating Commission, for the biennium ending June 30, 2023, out of the  
35 General Fund, the amount of \$\_\_\_\_\_, to be deposited into the Oregon Cybersecurity Public  
36 Awareness Fund established under section 11 of this 2022 Act.

37  
38 **MISCELLANEOUS**

39  
40 **SECTION 14. Repeal.** Section 12 of this 2022 Act is repealed on January 2, 2025.

41 **SECTION 15. Captions.** The unit and section captions used in this 2022 Act are provided  
42 only for the convenience of the reader and do not become part of the statutory law of this  
43 state or express any legislative intent in the enactment of this 2022 Act.

44 **SECTION 16. Operative dates.** (1) Sections 1, 3 to 5 and 7 to 14 of this 2022 Act and the  
45 repeal of ORS 276A.326 and 276A.329 by sections 2 and 6 of this 2022 Act become operative



1 on July 1, 2022.

2 (2) The Governor, the State Chief Information Officer, the Oregon Cybersecurity Advi-  
3 sory Council, Portland State University, Oregon State University and the University of  
4 Oregon may take any action before the operative date specified in subsection (1) of this  
5 section that is necessary to enable the Governor, the State Chief Information Officer, the  
6 Oregon Cybersecurity Advisory Council, Portland State University, Oregon State University  
7 and the University of Oregon to exercise, on and after the operative date specified in sub-  
8 section (1) of this section, all of the duties, functions and powers conferred on the Governor,  
9 the State Chief Information Officer, the Oregon Cybersecurity Advisory Council, Portland  
10 State University, Oregon State University and the University of Oregon by sections 1, 3 to  
11 5 and 7 to 14 of this 2022 Act and the repeal of ORS 276A.326 and 276A.329 by sections 2 and  
12 6 of this 2022 Act.

13 SECTION 17. Effective date. This 2022 Act being necessary for the immediate preserva-  
14 tion of the public peace, health and safety, an emergency is declared to exist, and this 2022  
15 Act takes effect on its passage.