LC 261
2022 Regular Session
1/6/22 (CPA/ps)

D R A F T

SUMMARY

Modifies composition and duties, powers and functions of Oregon Cybersecurity Advisory Council as governing body of Oregon Cybersecurity Center of Excellence.

Establishes Oregon Cybersecurity Center of Excellence as 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. 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

Relating to cybersecurity; creating new provisions; amending ORS 276A.326, 276A.329, 276A.332 and 276A.335; and declaring an emergency.

Whereas ransomware and other cyberattacks threaten the nation's critical

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.

infrastructure, economy and public health and safety;

Whereas the threats from ransomware and other cyberattacks continue to worsen each day for public, private and nonprofit sectors in Oregon;

Whereas Oregon's local and regional governments, education service districts, school districts and libraries have identified critical cybersecurity vulnerabilities and information technology modernization needs that require assistance from the State of Oregon, public universities and community colleges;

Whereas Oregon and the nation face a dire shortage of qualified cybersecurity professionals to address these threats and vulnerabilities;

Whereas there are multiple cybersecurity workforce development and educational programs in Oregon that lack funding to produce more qualified cybersecurity professionals;

Whereas the Legislative Assembly anticipated, with passage of chapter 513, Oregon Laws 2017 (Enrolled Senate Bill 90), the need for an Oregon Cybersecurity Center of Excellence;

Whereas the Legislative Assembly continuously seeks to encourage collaboration and shared service among Oregon public bodies to solve common problems; now, therefore,

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

SECTION 1. Legislative intent. It is the intent of the Legislative Assembly to establish:

(1) The Oregon Cybersecurity Center of Excellence, and to establish the Oregon Cybersecurity Center of Excellence Operating Fund for the purpose of funding the center's cybersecurity programs, services and activities and ongoing operations through the appropriation of moneys to the operating fund each biennium for distribution to the center and to the following entities:

(a) The National Center of Academic Excellence in Cyber Research at the Mark O. Hatfield Center for Cybersecurity of Portland State University.

(b) The Oregon Research and Teaching Security Operations Center at the School of Electrical Engineering and Computer Science of Oregon State University.

(c) The School of Law and the Charles H. Lundquist College of Business of the University of Oregon.

(d) Other public universities, community colleges and public bodies in Oregon that support or participate in the center's programs, services and activities.

(2) The Oregon Cybersecurity Workforce Development Fund, and to appropriate moneys to the fund each biennium for distribution to the Oregon Cybersecurity Center of Excellence for the purpose of targeted investments in workforce development programs designed to accelerate the growth, qualifications and availability of Oregon's cybersecurity workforce.

(3) The Oregon Cybersecurity Grant Program Fund, and to appropriate moneys to the fund each biennium for distribution to the Oregon Cybersecurity Center of Excellence for the purposes of cybersecurity assessment, monitoring, incident response and technical assistance and other cybersecurity-related goods and services to Oregon public bodies on a competitive basis with specific emphasis on serving the unmet needs of local governments, regional governments, special districts, education service districts, school districts and libraries.

(4) The Oregon Cybersecurity Public Awareness Fund, and to appropriate moneys to the fund each biennium for distribution to the Oregon Cybersecurity Center of Excellence for the purposes of raising awareness about the importance of cybersecurity across Oregon and ensuring that Oregonians better understand existing threats and have the information and resources to be safer and more secure online.

SECTION 2. ORS 276A.326 is amended to read:

276A.326. (1) The Oregon Cybersecurity Advisory Council is established

within the [*office of Enterprise Information Services*] **Oregon Cybersecurity Center of Excellence and shall be the governing body of the center**. The council consists of [*nine*] **15** voting members appointed by the [*State Chief Information Officer*] **Governor** in consultation with the [*Governor*] **State Chief Information Officer**. A majority of the council's voting members must be [*representatives of cyber-related industries in Oregon. The voting members of the council must include at least one representative of post-secondary institutions of education and one representative of public law enforcement agencies in Oregon*] **geographically diverse representatives of public universities listed in ORS 352.002, local governments, regional governments, special districts, education service districts, school districts and libraries**.

[*(2) The State Chief Information Officer may appoint nonvoting members to the council from:*]

[*(a) The Department of Justice;*]

[*(b) The office of the Secretary of State;*]

[*(c) The Oregon Department of Emergency Management;*]

[*(d) The Department of Consumer and Business Services;*]

[*(e) The Higher Education Coordinating Commission;*]

[*(f) The State Workforce and Talent Development Board;*]

[*(g) The Employment Department;*]

[*(h) The Oregon Business Development Department; or*]

[*(i) Any local, county, state, regional, tribal or federal government partner.*]

[*(3) The State Chief Information Officer shall provide administrative and staff support and facilities as necessary for the council to carry out the purposes set forth in this section.*]

[*(4) The purposes of the council are to:*]

[*(a) Serve as the statewide advisory body to the State Chief Information Officer on cybersecurity.*]

[*(b) Provide a statewide forum for discussing and resolving cybersecurity*

issues.]

[*(c) Provide information and recommend best practices concerning cybersecurity and resilience measures to public and private entities.*]

[*(d) Coordinate cybersecurity information sharing and promote shared and real-time situational awareness between the public and private sectors in this state.*]

[*(e) Encourage the development of the cybersecurity workforce through measures including, but not limited to, competitions aimed at building workforce skills, disseminating best practices, facilitating cybersecurity research and encouraging industry investment and partnership with post-secondary institutions of education and other career readiness programs.*]

[*(5) The council may adopt rules necessary for the operation of the council.*]

(2) The membership of the council consists of:

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

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

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

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

(e) One member who represents regional governments;

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

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

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

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

(j) One member who represents community colleges;

(k) One member who represents the office of Enterprise Information Services of the Oregon Department of Administrative Services;

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

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

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

(o) One member who represents a private sector information technology or telecommunications association in Oregon.

(3) The council shall:

(a) Adopt a charter, drafted in consultation with representatives from Portland State University, Oregon State University and the University of Oregon, as the governing document for the Oregon Cybersecurity Center of Excellence and for the center's operations and budget and the funds administered by the center, and shall review the charter annually.

(b) Develop and update every four years a strategic plan for the center.

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

(d) Establish, in consultation with the State Chief Information Officer, a statewide cybersecurity planning committee that meets the purpose, composition and cybersecurity expertise requirements de-

scribed in the Infrastructure Investment and Jobs Act (P.L. 117-58).

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

(4) The council may:

(a) Adopt rules, policies and procedures necessary for the operation of the council and the center's operations and budget and the funds administered by the center.

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

(c) Appoint nonvoting members to the council.

[*(6)(a)*] **(5)(a)** A majority of the voting members of the council constitutes a quorum for the transaction of business.

(b) Official action by the council requires the approval of a majority of the voting members of the council.

[*(7)*] **(6)** The [*State Chief Information Officer*] **council** shall [*appoint*] **elect** one member of the council to serve as chairperson and one member of the council to serve as vice chairperson. **The process for electing the chairperson and vice chairperson shall be specified in the charter adopted by the council pursuant to subsection (3) of this section.**

[*(8)(a)*] **(7)(a)** The term of office of each voting member of the council is four years, but a member serves at the pleasure of the [*State Chief Information Officer*] **Governor**.

(b) Before the expiration of the term of a voting member, the [*State Chief Information Officer*] **Governor**, in consultation with the [*Governor*] **State Chief Information Officer**, shall appoint a successor whose term begins on July 1 following the appointment. A voting member is eligible for reappointment.

[*(c) A nonvoting member's term of office is two years. A nonvoting member is eligible for reappointment.*]

[*(d)*] **(c)** If there is a vacancy for any cause, the [*State Chief Information Officer*] **Governor**, in consultation with the [*Governor*] **State Chief Infor-**

mation Officer, shall make an appointment to become immediately effective for the unexpired term.

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

[*(10)*] **(9)** Members of the council [*who are not members of the Legislative Assembly*] are not entitled to compensation, but the [*State Chief Information Officer*] **center** may reimburse a member of the council for actual and necessary travel and other expenses incurred in performing the member's official duties, in the manner and amounts provided for in ORS 292.495, from funds appropriated to the [*State Chief Information Officer*] **Oregon Cybersecurity Center of Excellence Operating Fund** for purposes of the council.

[*(11)*] **(10)** All agencies of state government, as defined in ORS 174.111, are directed to assist the council in the performance of the council's duties and, to the extent permitted by laws relating to confidentiality, shall furnish information and advice the council considers necessary to perform the council's duties.

SECTION 3. ORS 276A.329 is amended to read:

276A.329. [*The State Chief Information Officer shall develop a plan for the establishment of an Oregon Cybersecurity Center of Excellence. The State Chief Information Officer shall submit the plan to an appropriate committee or interim committee of the Legislative Assembly no later than January 1, 2019. The plan must identify any grants, donations, gifts or other form of conveyance of land, money, real or personal property or other valuable thing made to the state from any source that is expected to support the establishment and continued operation of the center. The plan must also include a description of the actions, timelines, budget and positions or contractor resources required for the center to:*]

[*(1) Coordinate information sharing related to cybersecurity risks, warnings and incidents.*]

[*(2) Provide support regarding cybersecurity incident response and cybercrime investigations.*]

[*(3) Serve as an Information Sharing and Analysis Organization pursuant to 6 U.S.C. 133 et seq., and as a liaison with the National Cybersecurity and Communications Integration Center within the United States Department of Homeland Security, other federal agencies and other public and private sector entities on issues relating to cybersecurity.*]

[*(4) Identify and participate in appropriate federal, multistate or private sector programs and efforts that support or complement the center's cybersecurity mission.*]

[*(5) Receive and appropriately disseminate relevant cybersecurity threat information from appropriate sources, including the federal government, law enforcement agencies, public utilities and private industry.*]

[*(6) Draft and biennially update an Oregon Cybersecurity Strategy and a Cyber Disruption Response Plan to be submitted to the Governor and an appropriate committee or interim committee of the Legislative Assembly. The plan must:*]

[*(a) Detail the steps that the state should take to increase the resiliency of its operations in preparation for, and during the response to, a cyber disruption event;*]

[*(b) Address high-risk cybersecurity for the state's critical infrastructure, including a review of information security technologies currently in place to determine if current policies are sufficient to prevent the compromise or unauthorized disclosure of critical or sensitive government information inside and outside the firewall of state agencies, and develop plans to better identify, protect from, detect, respond to and recover from significant cyber threats;*]

[*(c) Establish a process to regularly conduct risk-based assessments of the cybersecurity risk profile, including infrastructure and activities within this state;*]

[*(d) Provide recommendations related to securing networks, systems and data, including interoperability, standardized plans and procedures, evolving threats and best practices to prevent the unauthorized access, theft, alteration or destruction of data held by the state;*]

[*(e) Include the recommended content and timelines for conducting cybersecurity awareness training for state agencies and the dissemination of educational materials to the public and private sectors in this state through the center;*]

[*(f) Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public's personal information;*]

[*(g) Include strategies for collaboration with the private sector and educational institutions through the center and other venues to identify and implement cybersecurity best practices; and*]

[*(h) Establish data breach reporting and notification requirements in coordination with the Department of Consumer and Business Services.*]

(1) The Oregon Cybersecurity Center of Excellence is established as an independent, nonprofit public corporation. The center shall exercise and carry out all powers, rights and privileges that are expressly conferred up the center, are implied by law or are incident to such powers.

(2) The mission and purpose of the center is to oversee, coordinate, fund and provide:

(a) Cyber education, awareness and training for public, private and nonprofit sectors;

(b) Cybersecurity workforce development programs in coordination with:

(A) Public universities listed in ORS 352.002;

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

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

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

(3) In carrying out its mission and purpose, the center shall:

(a) Serve as the statewide advisory body to the Legislative Assem-

bly, Governor and State Chief Information Officer on cybersecurity for local governments, regional governments, special districts, education service districts, school districts and libraries.

(b) Provide information and recommend best practices concerning cybersecurity, resilience and recovery measures, including legal, insurance and other topics, to public, private and nonprofit sectors in Oregon.

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

(d) Identify and participate in appropriate federal, multistate, regional, state, local or private sector programs and efforts that support or complement the center's cybersecurity mission.

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

(f) Manage and award funds distributed to the center for cybersecurity initiatives.

(g) Encourage the development of Oregon's cybersecurity workforce through measures including, but not limited to:

(A) Identifying gaps and needs in workforce programs.

(B) Fostering the growth and development of cybersecurity workforce development programs and career and technical education in school districts, community colleges and public universities listed in ORS 352.002.

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

(D) Fostering industry involvement in internships, mentorship and apprenticeship programs and experiential learning programs.

(E) Building awareness of industry and career opportunities to re-

cruit students into cyber-related educational tracks.

(h) Provide cybersecurity assessment, monitoring and incident response services to public bodies, with priority given to public bodies with the most need for services including local governments, regional governments, special districts, education service districts, school districts and libraries.

(i) Collaborate with public bodies to coordinate cybersecurity efforts with ongoing information technology modernization projects.

(j) Develop, update and submit biennially the Oregon Cybersecurity Modernization Plan described in subsection (5) of this section to the Governor and the appropriate committees of the Legislative Assembly.

(4)(a) Portland State University, Oregon State University and the University of Oregon shall jointly operate the center by agreement, using moneys from the Oregon Cybersecurity Center of Excellence Operating Fund established under section 7 of this 2022 Act, and shall provide administrative and staff support and facilities as necessary for the center to carry out the purposes set forth in this section. The universities may operate the center as a virtual center, in whole or in part.

(b) A public university or community college in Oregon not listed in paragraph (a) of this subsection may join the agreement to operate the center and provide administrative and staff support and facilities.

(5) The Oregon Cybersecurity Modernization Plan developed and updated under this section must, at a minimum:

(a) Identify cybersecurity risks in critical infrastructure, local governments, school districts and public sector entities;

(b) Establish risk-based assessment procedures;

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

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

programs; and

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

SECTION 4. As used in sections 4 to 10 of this 2022 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 to all residents of a local government unit 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 metropolitan service district formed under ORS chapter 268.

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

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

SECTION 5. Authority to enter into agreements. Notwithstanding any other provision of law, the Oregon Cybersecurity Center of Excellence may:

(1) Enter into any agreement, or any configuration of agreements, relating to the establishment and ongoing operations and purpose of the center with any private entity or unit of government, or with any configuration of private entities and units of government. The subject of agreements entered into under this section may include, but need not be limited to, cybersecurity workforce development, training and awareness, information technology security assessments and vulnerability testing, cyber disruption and incident response, risk-based remediation measures, application lifecycle maintenance management (ALM) and the funding and provision of cybersecurity-related goods

or services.

(2) Include in any agreement entered into under this section any financing mechanisms, including but not limited to the imposition and collection of franchise fees or user fees and the development or use of other revenue sources.

SECTION 6. Authority to accept moneys. (1) The Oregon Cybersecurity Center of Excellence may accept from the United States Government or any of its agencies any funds that are made available to the State of Oregon for carrying out the purposes of the center, regardless of whether the funds are made available by grant, loan or other financing arrangement. The center may enter into agreements and other arrangements with the United States Government or any of its agencies as may be necessary, proper and convenient for carrying out the purposes of the center.

(2) The center may accept from any source any grant, donation, gift or other form of conveyance of land, money, real or personal property or other valuable thing made to the State of Oregon or the center for carrying out the purposes of the center.

(3) Any cybersecurity initiative, consistent with the purpose of the center, may be financed in whole or in part by contributions of any funds or property made by any private entity or unit of government that is a party to any agreement entered into under the authority of the center.

(4) The center shall deposit, as appropriate, all moneys received under this section into one of the following funds:

(a) The Oregon Cybersecurity Center of Excellence Operating Fund established under section 7 of this 2022 Act.

(b) The Oregon Cybersecurity Workforce Development Fund established under section 8 of this 2022 Act.

(c) The Oregon Cybersecurity Grant Program Fund established under section 9 of this 2022 Act.

(d) The Oregon Cybersecurity Public Awareness Fund established under section 10 of this 2022 Act.

SECTION 7. Center operating fund. (1) The Oregon Cybersecurity Center of Excellence Operating Fund is established in the State Treasury, separate and distinct from the General Fund. Interest earned by the Oregon Cybersecurity Center of Excellence Operating Fund must be credited to the fund.

(2) Moneys in the fund shall consist of:

(a) Amounts donated to the fund;

(b) Amounts appropriated or otherwise transferred to the fund by the Legislative Assembly; and

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

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

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

SECTION 8. Cybersecurity workforce development fund. (1) The Oregon Cybersecurity Workforce Development Fund is established in the State Treasury, separate and distinct from the General Fund. Interest earned by the Oregon Cybersecurity Workforce Development Fund must be credited to the fund.

(2) Moneys in the fund shall consist of:

(a) Amounts donated to the fund;

(b) Amounts appropriated or otherwise transferred to the fund by the Legislative Assembly; and

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

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

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

SECTION 9. Cybersecurity grant program fund. (1) The Oregon Cybersecurity Grant Program Fund is established in the State Treasury, separate and distinct from the General Fund. Interest earned by the Oregon Cybersecurity Grant Program Fund must be credited to the fund.

(2) Moneys in the fund shall consist of:

(a) Amounts donated to the fund;

(b) Amounts appropriated or otherwise transferred to the fund by the Legislative Assembly; and

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

(3) Moneys in the fund are continuously appropriated to the Higher Education Coordinating Commission for distribution to the Oregon Cybersecurity Center of Excellence for the purposes of providing:

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

and libraries.

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

(4) The center shall adopt standards, objectives, criteria and eligibility requirements for the use of moneys distributed from the Oregon Cybersecurity Grant Program Fund. In developing criteria and eligibility standards, the center shall take into consideration any requirements of federal programs awarding moneys related to cybersecurity.

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

SECTION 10. Cybersecurity public awareness fund. (1) The Oregon Cybersecurity Public Awareness Fund is established in the State Treasury, separate and distinct from the General Fund. Interest earned by the Oregon Cybersecurity Public Awareness Fund must be credited to the fund.

(2) Moneys in the fund shall consist of:

(a) Amounts donated to the fund;

(b) Amounts appropriated or otherwise transferred to the fund by the Legislative Assembly; and

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

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

(4) The center shall submit to the Governor and to the appropriate

committees of the Legislative Assembly in the manner provided under ORS 192.245, a biennial report that summarizes the balance of the fund, lists the deposits into and expenditures from the fund and provides such other details as necessary regarding the operation of the fund.

SECTION 11. Section 1 of this 2022 Act and ORS 276A.326 and 276A.329 are added to and made a part of sections 4 to 10 of this 2022 Act.

SECTION 12. ORS 276A.332 is amended to read:

276A.332. Notwithstanding any other provision of law, the State Chief Information Officer may:

(1) Enter into any agreement, or any configuration of agreements, relating to state cybersecurity **or to support the operations of the Oregon Cybersecurity Center of Excellence established by ORS 276A.329,** with any private entity or unit of government, or with any configuration of private entities and units of government. The subject of agreements entered into under this section may include, but need not be limited to, cybersecurity **workforce development,** training and awareness, information technology security assessments and vulnerability testing, cyber disruption and incident response, risk-based remediation measures and application [*life cycle maintenance*] **lifecycle management (ALM)**.

(2) Include in any agreement entered into under this section any financing mechanisms, including but not limited to the imposition and collection of franchise fees or user fees and the development or use of other revenue sources.

SECTION 13. ORS 276A.335 is amended to read:

276A.335. (1) The State Chief Information Officer may accept from the United States Government or any of its agencies any funds that are made available to the state for carrying out the purposes of ORS 276A.323**,** [*to*] **276A.326, 276A.329, 276A.332 and** 276A.335, regardless of whether the funds are made available by grant, loan or other financing arrangement. Under the

authority granted by ORS chapter 190, the State Chief Information Officer may enter into agreements and other arrangements with the United States Government or any of its agencies as may be necessary, proper and convenient for carrying out the purposes of ORS 276A.323**,** [*to*] **276A.326, 276A.329, 276A.332 and** 276A.335.

(2) The office of Enterprise Information Services may accept from any source any grant, donation, gift or other form of conveyance of land, money, real or personal property or other valuable thing made to the state or the office of Enterprise Information Services for carrying out the purposes of ORS 276A.323**,** [*to*] **276A.326, 276A.329, 276A.332 and** 276A.335.

(3) Any cybersecurity initiative, consistent with the purposes of ORS 276A.323**,** [*to*] **276A.326, 276A.329, 276A.332 and** 276A.335, may be financed in whole or in part by contributions of any funds or property made by any private entity or unit of government that is a party to any agreement entered into under the authority of the office of Enterprise Information Services.

(4) The State Chief Information Officer shall deposit into the State Information Technology Operating Fund established under ORS 276A.209 all moneys received under this section.

SECTION 14. (1) In addition to and not in lieu of any other appropriation, there is appropriated to the Higher Education Coordinating Commission, for the biennium ending June 30, 2023, out of the General Fund, the amount of $_____, to be deposited into the Oregon Cybersecurity Center of Excellence Operating Fund established under section 7 of this 2022 Act.

(2) In addition to and not in lieu of any other appropriation, there is appropriated to the Higher Education Coordinating Commission, for the biennium ending June 30, 2023, out of the General Fund, the amount of $_____, to be deposited into the Oregon Cybersecurity Workforce Development Fund established under section 8 of this 2022 Act.

(3) In addition to and not in lieu of any other appropriation, there

is appropriated to the Higher Education Coordinating Commission, for the biennium ending June 30, 2023, out of the General Fund, the amount of $_____, to be deposited into the Oregon Cybersecurity Grant Program Fund established under section 9 of this 2022 Act.

(4) In addition to and not in lieu of any other appropriation, there is appropriated to the Higher Education Coordinating Commission, for the biennium ending June 30, 2023, out of the General Fund, the amount of $_____, to be deposited into the Oregon Cybersecurity Public Awareness Fund established under section 10 of this 2022 Act.

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

SECTION 16. (1) Sections 1, 4 to 10 and 14 of this 2022 Act and the amendments to ORS 276A.326, 276A.329, 276A.332 and 276A.335 by sections 2, 3, 12 and 13 of this 2022 Act become operative on July 1, 2022.

(2) The Governor, State Chief Information Officer, Oregon Cybersecurity Advisory Council and Portland State University, Oregon State University and 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, State Chief Information Officer, Oregon Cybersecurity Advisory Council and Portland State University, Oregon State University and 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, State Chief Information Officer, Oregon Cybersecurity Advisory Council and Portland State University, Oregon State University and University of Oregon by the amendments to ORS 276A.326, 276A.329, 276A.332 and 276A.335 by sections 2, 3, 12 and 13 of this 2022 Act.

SECTION 17. This 2022 Act being necessary for the immediate

preservation of the public peace, health and safety, an emergency is declared to exist, and this 2022 Act takes effect on its passage.
