C-Engrossed
Senate Bill 90

Ordered by the Senate June 2
Including Senate Amendments dated March 17 and May 5 and June 2

Printed pursuant to Senate Interim Rule 213.28 by order of the President of the Senate in conformance with presession filing rules, indicating neither advocacy nor opposition on the part of the President (at the request of Governor Kate Brown for Oregon Department of Administrative Services)

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 information technology security functions of certain state agencies in executive branch to State Chief Information Officer.

Establishes Oregon Cybersecurity Advisory Council in office of State Chief Information Officer.

Directs State Chief Information Officer to develop plan for establishment of Oregon Cybersecurity Center of Excellence and submit plan to committee or interim committee of Legislative Assembly no later than January 1, [*2018*] **2019**.

Authorizes State Chief Information Officer to enter into certain agreements and accept certain funds.

[*Takes effect on 91st day following adjournment sine die.*]

Declares emergency, effective July 1, 2017.

A BILL FOR AN ACT

Relating to information technology security; creating new provisions; amending ORS 291.041; and declaring an emergency.

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

SECTION 1. Unification of agency information technology security functions. (1) As used in this section:

(a) "Executive department" has the meaning given that term in ORS 174.112, except that "executive department" does not include:

(A) The Secretary of State.

(B) The State Treasurer.

(C) The Attorney General.

(D) The Oregon State Lottery.

(E) Public universities listed in ORS 352.002.

(b) "State agency" means an agency, as defined in ORS 183.310, in the executive department.

(2) All state agencies shall carry out the actions necessary to unify agency information technology security functions across the executive department.

(3) The State Chief Information Officer, or a designee of the State Chief Information Officer, and state agencies shall work cooperatively to develop a plan to transfer agency information technology security functions, employees, records and property to the office of the State Chief Information Officer no later than January 1, 2018.

(4) The unexpended balances of amounts that a state agency is authorized to expend

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.

during the biennium beginning July 1, 2017, from revenues dedicated, continuously appropriated, appropriated or otherwise made available for the purpose of administering and enforcing the duties, functions and powers transferred by this section shall remain with the state agency.

(5) In accordance with the plan developed under this section, the director of each state agency shall deliver to the State Chief Information Officer or a designee of the State Chief Information Officer all records and property related to the performance of the agency information technology security functions transferred to the State Chief Information Officer under this section. The property may include contracts pertaining to the functions transferred to the office of the State Chief Information Officer. The State Chief Information Officer shall take possession of the records and property delivered under this subsection.

(6)(a) Under the direction of the Governor and in consultation with state agencies and labor organizations representing the affected employees, the Director of the Oregon Department of Administrative Services or a designee of the director shall identify each position and employee engaged in the performance of agency information technology security functions to be transferred to the office of the State Chief Information Officer, and state agencies shall transfer the identified employees to the office of the State Chief Information Officer.

(b) The State Chief Information Officer shall take charge of and employ the transferred employees without a reduction in the employees' compensation but subject to change or termination of employment or compensation as provided by law.

(c) The State Chief Information Officer or a designee of the State Chief Information Officer may immediately redeploy a transferred employee back to the employee's agency of origin under the continuing supervision of the State Chief Information Officer or a designee of the State Chief Information Officer. An employee engaged primarily in providing management or administrative support for agency information technology security functions may be considered engaged in the performance of functions to be transferred to the office of the State Chief Information Officer.

(d) The Director of the Oregon Department of Administrative Services or a designee of the director shall ensure compliance with all applicable policy provisions and collective bargaining agreements, including providing any required notices within the applicable time periods.

(7) State agencies shall assist the office of the State Chief Information Officer and provide access to personnel and other resources necessary to execute the transfer of functions under this section.

SECTION 2. State agency coordination. (1) As used in this section:

(a) "Executive department" has the meaning given that term in ORS 174.112, except that "executive department" does not include:

(A) The Secretary of State.

(B) The State Treasurer.

(C) The Attorney General.

(D) The Oregon State Lottery.

(E) Public universities listed in ORS 352.002.

(b) "State agency" means an agency, as defined in ORS 183.310, in the executive department.

(2) All state agencies shall:

(a) Cooperate with the office of the State Chief Information Officer in the implementation of a continuing statewide agency-by-agency risk-based information technology security assessment and remediation program.

(b) Cooperate in the development of, and follow, the plans, rules, policies and standards adopted by the State Chief Information Officer with regard to the unification of agency information technology security functions in this state.

(c) Conduct and document the completion of annual information technology security awareness training for all agency employees.

(d) Report security metrics using methodologies developed by the office of the State Chief Information Officer.

(e) Participate in activities coordinated by the office of the State Chief Information Officer in order to better understand and address security incidents and critical cybersecurity threats to the state.

(3) The State Chief Information Officer shall determine and allocate the costs to state agencies associated with providing information technology services, third-party security evaluations, vulnerability assessments and remediation measures. State agencies shall pay the costs to the State Chief Information Officer in the same manner as the state agency pays other claims. The State Chief Information Officer shall deposit into the State Information Technology Operating Fund established under ORS 291.041 all moneys that the State Chief Information Officer receives from state agencies for purposes of providing information technology services and administering and enforcing the duties, functions and powers under this section.

SECTION 3. Oregon Cybersecurity Advisory Council. (1) The Oregon Cybersecurity Advisory Council is established within the office of the State Chief Information Officer. The council consists of nine voting members appointed by the State Chief Information Officer in consultation with the Governor. 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.

(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 Office of Emergency Management;

(d) The Department of Consumer and Business Services;

(e) The Higher Education Coordinating Commission;

(f) The State Workforce Investment 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.

(6)(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) The State Chief Information Officer shall appoint one member of the council to serve as chairperson and one member of the council to serve as vice chairperson.

(8)(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.

(b) Before the expiration of the term of a voting member, the State Chief Information Officer, in consultation with the Governor, 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) If there is a vacancy for any cause, the State Chief Information Officer, in consultation with the Governor, shall make an appointment to become immediately effective for the unexpired term.

(9) 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) Members of the council who are not members of the Legislative Assembly are not entitled to compensation, but the State Chief Information Officer 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 for purposes of the council.

(11) 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 4. Oregon Cybersecurity Center of Excellence. 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.

SECTION 5. Authority of State Chief Information Officer to enter into agreements. 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 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 training and awareness, information technology security assessments and vulnerability testing, cyber disruption and incident response, risk-based remediation measures and application life cycle maintenance.

(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. Moneys from federal government and other sources. (1) The office of 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 sections 1 to 6 of this 2017 Act, regardless of whether the funds are made available by grant, loan or other financing arrangement. Under the authority granted by ORS chapter 190, the office of 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 sections 1 to 6 of this 2017 Act.

(2) The office of the State Chief Information Officer 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 the State Chief Information Officer for carrying out the purposes of sections 1 to 6 of this 2017 Act.

(3) Any cybersecurity initiative, consistent with the purposes of sections 1 to 6 of this 2017 Act, 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 the State Chief Information Officer.

(4) The State Chief Information Officer shall deposit into the State Information Technology Operating Fund established under ORS 291.041 all moneys received under this section.

SECTION 7. ORS 291.041 is amended to read:

291.041. (1) There is established the State Information Technology Operating Fund in the State Treasury, separate and distinct from the General Fund. The moneys in the State Information Technology Operating Fund may be invested as provided in ORS 293.701 to 293.857. Interest earnings on the fund assets must be credited to the fund.

(2) The Director of the Oregon Department of Administrative Services shall deposit into the State Information Technology Operating Fund moneys for enterprise information technology and telecommunications that are appropriated to the Oregon Department of Administrative Services and that are necessary for the State Chief Information Officer to fulfill the duties, implement the functions and exercise the powers imposed upon, transferred to and vested in the State Chief Information Officer under section 1, chapter 807, Oregon Laws 2015.

(3) The State Information Technology Operating Fund consists of:

(a) Moneys deposited into the fund under subsection (2) of this section and sections 2 and 6 of this 2017 Act.

(b) Amounts donated to the fund.

(c) Amounts appropriated or otherwise transferred to the fund by the Legislative Assembly.

(d) Other amounts deposited into the fund from any source.

(4) Amounts in the fund are continuously appropriated to the State Chief Information Officer for the purposes authorized by law.

SECTION 8. (1) Sections 3 to 6 of this 2017 Act become operative on January 1, 2018.

(2) The State Chief Information Officer may take any action before the operative date specified in subsection (1) of this section that is necessary to enable the State Chief Information Officer 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 State Chief Information Officer under sections 3 to 6 of this 2017 Act.

SECTION 9. Notwithstanding the term of office specified by section 3 of this 2017 Act, of the members first appointed to the Oregon Cybersecurity Advisory Council:

(1) Three shall serve for a term ending June 30, 2019.

(2) Three shall serve for a term ending June 30, 2020.

(3) Three shall serve for a term ending June 30, 2021.

SECTION 10. The section captions used in this 2017 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 2017 Act.

SECTION 11. This 2017 Act being necessary for the immediate preservation of the public peace, health and safety, an emergency is declared to exist, and this 2017 Act takes effect July 1, 2017.