House Bill 3221

Sponsored by Representative WITT

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.**

Requires State Chief Information Officer to develop, in collaboration with state agencies and Secretary of State, State Treasurer and Attorney General, curriculum and materials for training state employees in information security. Specifies criteria for curriculum and materials.

Requires state agencies and Secretary of State, State Treasurer and Attorney General to implement information security training for state employees annually or as conditions otherwise warrant.

Takes effect on 91st day following adjournment sine die.

A BILL FOR AN ACT

Relating to information security training for state employees; creating new provisions; amending ORS 182.122 and 182.124; and prescribing an effective date.

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

SECTION 1. ORS 182.122 is amended to read:

182.122. (1) As used in this section:

(a) "Executive department" has the meaning given that term in ORS 174.112.

(b) "Information systems" means computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.

(2) The State Chief Information Officer has responsibility for and authority over information systems security in the executive department, including responsibility for taking all measures that are reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. The State Chief Information Officer shall, after consultation and collaborative development with agencies, establish a state information systems security plan and associated standards, policies and procedures. The plan must align with and support the Enterprise Information Resources Management Strategy described in ORS 291.039.

(3) The State Chief Information Officer may coordinate with the Oregon Department of Administrative Services to:

(a) Review and verify the security of information systems operated by or on behalf of state agencies;

(b) Monitor state network traffic to identify and react to security threats; and

(c) Conduct vulnerability assessments of state agency information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems.

(4) The State Chief Information Officer shall contract with qualified, independent consultants for

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.

the purpose of conducting vulnerability assessments under subsection (3) of this section.

(5) In collaboration with appropriate agencies, the State Chief Information Officer shall develop and implement policies for responding to events that damage or threaten the availability, integrity or confidentiality of information systems or the information stored in information systems, whether those systems are within, interoperable with or outside the state's shared computing and network infrastructure. In the policies, the State Chief Information Officer shall prescribe actions reasonably necessary to:

(a) Promptly assemble and deploy in a coordinated manner the expertise, tools and methodologies required to prevent or mitigate the damage caused or threatened by an event;

(b) Promptly alert other persons of the event and of the actions reasonably necessary to prevent or mitigate the damage caused or threatened by the event;

(c) Implement forensic techniques and controls developed under subsection (6) of this section;

(d) Evaluate the event for the purpose of possible improvements to the security of information systems; and

(e) Communicate and share information with appropriate agencies, using preexisting incident response capabilities.

(6) After consultation and collaborative development with appropriate agencies and the Oregon Department of Administrative Services, the State Chief Information Officer shall implement forensic techniques and controls for the security of information systems, whether those systems are within, interoperable with or outside the state's shared computing and network infrastructure. The techniques and controls must include using specialized expertise, tools and methodologies to investigate events that damage or threaten the availability, integrity or confidentiality of information systems or the information stored in information systems. The State Chief Information Officer shall consult with the Oregon State Police, the Office of Emergency Management, the Governor and others as necessary in developing forensic techniques and controls under this section.

(7) The State Chief Information Officer shall ensure that reasonably appropriate remedial actions are undertaken when the State Chief Information Officer finds that such actions are reasonably necessary by reason of vulnerability assessments of information systems under subsection (3) of this section, evaluation of events under subsection (5) of this section and other evaluations and audits.

(8)(a) The State Chief Information Officer, in collaboration with state agencies in the executive department, shall develop and prescribe a curriculum and materials for training state employees in information security awareness and in proper procedures for detecting, assessing, reporting and addressing information security threats. The curriculum must include activities, case studies, hypothetical situations and other methods that focus on forming good information security habits and procedures among state employees and that teach best practices for detecting, assessing, reporting and addressing information security threats.

(b) The State Chief Information Officer shall coordinate with state agencies in the executive department and with the Secretary of State, the State Treasurer and the Attorney General to implement information security training for state employees on an annual basis or as conditions otherwise warrant.

[*(8)(a)*] **(9)(a)** State agencies [*are responsible for securing*] **shall secure** computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information outside the state's shared computing and net-

work infrastructure[*, following*] **and each year, or as otherwise warranted, shall provide information security training for state employees. Each state agency shall follow** information security standards, policies and procedures [*established by*] **that** the State Chief Information Officer **establishes** and [*developed*] **develops** collaboratively with the **state** agencies **and for information security training shall use the curriculum and materials that the State Chief Information Officer develops collaboratively with the state agencies**. **State** agencies may establish plans, standards**,** [*and*] measures **and training methods** that **address specific state agency needs and** are more stringent than the **plans,** standards**, measures and training methods that the** [*established by*] the State Chief Information Officer [*to address specific agency needs*] **establishes** if the plans, standards**,** [*and*] measures **and training methods** do not contradict or contravene the state information systems security plan. Independent agency security plans must be developed within the framework of the state information systems security plan.

(b) A state agency shall report the results of any vulnerability assessment, evaluation or audit conducted by the agency to the State Chief Information Officer for the purposes of consolidating statewide security reporting and, when appropriate, to prompt a state incident response.

(c) Each state agency shall evaluate the efficacy of the information security training program the state agency provides for state employees and shall forward to the State Chief Information Officer the results of the evaluation, together with any suggestions for improving the curriculum and materials or other aspects of the training program.

[*(9)*] **(10)** This section does not apply to:

(a) Research and student computer systems used by or in conjunction with any public university listed in ORS 352.002; and

(b)(A) Gaming systems and networks operated by the Oregon State Lottery or contractors of the State Lottery; or

(B) The results of Oregon State Lottery reviews, evaluations and vulnerability assessments of computer systems outside the state's shared computing and network infrastructure.

(10) The State Chief Information Officer shall adopt rules to implement the provisions of this section.

SECTION 2. ORS 182.124 is amended to read:

182.124. (1) Notwithstanding ORS 182.122, the Secretary of State, the State Treasurer and the Attorney General have sole discretion and authority over information systems security in their respective agencies, including the discretion and authority to take all measures that are reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems.

(2) The Secretary of State, the State Treasurer and the Attorney General shall each establish an information systems security plan**, an information security training program for employees that uses the curriculum and materials described in ORS 182.122 (8)(a)** and associated standards, policies and procedures in collaboration with the State Chief Information Officer as provided in ORS 182.122.

(3) The plan **and training program** established under subsection (2) of this section, at a minimum, must:

(a) Be compatible with the state information systems security plan and associated standards, policies and procedures established by the State Chief Information Officer under ORS 182.122 (2);

(b) Assign responsibility for:

(A) Reviewing, monitoring and verifying the security of the Secretary of State's, the State

Treasurer's and the Attorney General's information systems; and

(B) Conducting vulnerability assessments of information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems;

(c) Contain policies for responding to events that damage or threaten the availability, integrity or confidentiality of information systems or the information stored in information systems, whether the systems are within, interoperable with or outside the state's shared computing and network infrastructure;

(d) Prescribe actions reasonably necessary to:

(A) Promptly assemble and deploy in a coordinated manner the expertise, tools and methodologies required to prevent or mitigate the damage caused or threatened by an event;

(B) Promptly alert the State Chief Information Officer and other persons of the event and of the actions reasonably necessary to prevent or mitigate the damage caused or threatened by the event;

(C) Implement forensic techniques and controls developed under paragraph (e) of this subsection;

(D) Evaluate the event for the purpose of possible improvements to the security of information systems; and

(E) Communicate and share information with agencies, using preexisting incident response capabilities; [*and*]

(e) Describe and implement forensic techniques and controls for the security of information systems, whether those systems are within, interoperable with or outside the state's shared computing and network infrastructure, including the use of specialized expertise, tools and methodologies, to investigate events that damage or threaten the availability, integrity or confidentiality of information systems or the information stored in information systems[.]**; and**

(f) Train state employees each year or as conditions otherwise warrant in detecting, assessing, reporting and addressing information security threats.

(4) The Secretary of State, the State Treasurer and the Attorney General shall participate in the planning [*process*] **processes** that the State Chief Information Officer conducts under ORS 182.122 (2) **and (8)**.

(5) If the State Chief Information Officer cannot agree with the Secretary of State, the State Treasurer or the Attorney General on a joint information systems security plan and associated operational standards and policies, the State Chief Information Officer, in collaboration with the Oregon Department of Administrative Services, may take steps reasonably necessary to condition, limit or preclude electronic traffic or other vulnerabilities between information systems for which the Secretary of State, State Treasurer or Attorney General has authority under subsection (1) of this section and the information systems for which the State Chief Information Officer has authority under ORS 182.122 (2).

SECTION 3. (1) The amendments to ORS 182.122 and 182.124 by sections 1 and 2 of this 2017 Act become operative on January 1, 2018.

(2) The State Chief Information Officer, the Secretary of State, the State Treasurer and the Attorney General may adopt rules and take any other action before the operative date specified in subsection (1) of this section that is necessary to enable the State Chief Information Officer, the Secretary of State, the State Treasurer and the Attorney General, on and after the operative date specified in subsection (1) of this section, to exercise the duties, powers and functions conferred on the State Chief Information Officer, the Secretary of

State, the State Treasurer and the Attorney General by the amendments to ORS 182.122 and 182.124 by sections 1 and 2 of this 2017 Act.

SECTION 4. This 2017 Act takes effect on the 91st day after the date on which the 2017 regular session of the Seventy-ninth Legislative Assembly adjourns sine die.
