Senate Bill 120

Sponsored by Senator RILEY (Presession filed.)

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.**

Subjects office of Secretary of State and office of State Treasurer to authority of State Chief Information Officer concerning information systems security matters.

Declares emergency, effective on passage.

A BILL FOR AN ACT

Relating to the State Chief Information Officer's authority to ensure information systems security; amending ORS 182.124 and section 1, chapter 110, Oregon Laws 2016; and declaring an emergency.

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

SECTION 1. Section 1, chapter 110, Oregon Laws 2016, is amended to read:

Sec. 1. (1) As used in this section:

(a) "Information resources" means data and the means for storing, retrieving, connecting or using data, including but not limited to records, files, databases, documents, software, equipment and facilities that a state agency owns or leases.

(b) "Information security assessment" means:

(A) An organized method to determine a risk to or a vulnerability of a state agency's information system or a third party information service to which a state agency subscribes; and

(B) An independent examination and review of records, logs, policies, activities and practices to:

(i) Assess whether a state agency's information system is vulnerable to an information security incident;

(ii) Ensure compliance with rules, policies, standards and procedures that the State Chief Information Officer or a state agency, under the state agency's independent authority, adopts or otherwise promulgates; and

(iii) Recommend necessary changes to a state agency's rules, policies, standards and procedures to ensure compliance and prevent information security incidents.

(c) "Information security incident" means an incident that creates a risk of harm to a state agency or the state agency's operations and in which:

(A) Access to, or viewing, copying, transmission, theft or usage of, a state agency's sensitive, protected or confidential information occurs without authorization from the state agency;

(B) A failure of compliance with a state agency's security or acceptable use policies or practices occurs that results in access to a state agency's information system or information resources for viewing, copying, transmission, theft or use without the state agency's authorization; or

(C) A state agency's information system or information resources or a third party information service to which a state agency subscribes becomes unavailable in a reliable and timely manner to authorized individuals or organizations, or is modified or deleted under circumstances that the state

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.

agency does not intend, plan or initiate.

(d)(A) "Information system" means a system of computers and related hardware, software, storage media and networks and any other means by which a state agency collects, uses or manages the state agency's information resources.

(B) "Information system" does not include a third party information service to which a state agency subscribes if the third party information service incorporates or uses hardware, software, storage media and networks that the state agency does not own or lease or that the state agency does not have the legal authority to directly monitor or control.

(e) "State agency" means an officer, board, commission, department, agency or [*institute*] **institution** of state government, as defined in ORS 174.111, except:

(A) Public universities listed in ORS 352.002; and

(B) The Oregon State Lottery and entities with which the Oregon State Lottery has a contract or agreement with respect to the Oregon State Lottery's gaming systems or networks.

(2) A state agency shall promptly notify the Legislative Fiscal Office of an information security incident and describe the actions the state agency has taken or must reasonably take to prevent, mitigate or recover from damage to, unauthorized access to, unauthorized modifications or deletions of or other impairments of the integrity of the state agency's information system or information resources.

(3) Each state agency shall periodically conduct or contract for an information security assessment of the state agency's information system and information resources and shall request results from a third party's information security assessment of an information service that the third party provides and to which the state agency subscribes. Each state agency shall notify the Legislative Fiscal Office of the information security assessment after the state agency receives the results of the information security assessment.

(4)(a) The State Chief Information Officer, [*the Secretary of State, the State Treasurer,*] the Attorney General, the State Court Administrator and the Legislative Administrator shall each submit to, and present in an appropriate hearing or other proceeding before, the Joint Legislative Committee on Information Management and Technology an annual report concerning the security of the information systems and information resources over which the State Chief Information Officer, [*the Secretary of State, the State Treasurer,*] the Attorney General, the State Court Administrator or the Legislative Administrator has direct or supervisory control.

(b) The annual report described in paragraph (a) of this subsection may not include information security information or other materials that are exempt from disclosure under ORS 192.410 to 192.505.

(5)(a) The Legislative Fiscal Office shall use the notifications the office receives under subsections (2) and (3) of this section, and any other information about an information security assessment or an information security incident that a state agency provides to the office, via a method and at a level of detail to which the state agency and the office agree, solely for the purpose of providing support and assistance to the Joint Legislative Committee on Information Management and Technology, the Joint Committee on Ways and Means and the Joint Legislative Audit Committee.

(b)(A) Except as provided in subparagraph (B) of this paragraph, the Legislative Fiscal Officer or an employee of the Legislative Fiscal Office may not disclose to any other person the nature or contents of the notifications that the office receives under subsections (2) and (3) of this section or any other information described in paragraph (a) of this subsection to the extent that the notifica-

tions or the information are exempt from disclosure under ORS 192.410 to 192.505.

(B) The Legislative Fiscal Officer or an employee of the Legislative Fiscal Office may disclose the nature or contents of the notifications or information described in subparagraph (A) of this paragraph if the officer or employee obtains the written consent of:

(i) The State Chief Information Officer, with respect to notifications and information that a state agency within the executive department, as defined in ORS 174.112, provided;

[*(ii) The Secretary of State, with respect to notifications and information that the office of the Secretary of State provided;*]

[*(iii) The State Treasurer, with respect to notifications and information that the office of the State Treasurer provided;*]

[*(iv)*] **(ii)** The Attorney General, with respect to notifications and information that the Department of Justice provided;

[*(v)*] **(iii)** The State Court Administrator, with respect to notifications and information that a court or a state agency within the judicial department, as defined in ORS 174.113, provided; or

[*(vi)*] **(iv)** The Legislative Administrator, with respect to notifications and information that a state agency within the legislative department, as defined in ORS 174.114, provided.

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*] **has** sole discretion and authority over information systems security [*in their respective agencies*] **for the Department of Justice**, 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 and associated standards, policies and procedures in collaboration with the State Chief Information Officer as provided in ORS 182.122.

(3) The plan 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.

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

(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. 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 on its passage.