

Enrolled
House Bill 3145

Sponsored by Representative DALLUM

CHAPTER

AN ACT

Relating to information management in state agencies; and declaring an emergency.

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

SECTION 1. (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 the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.

(2) The Oregon Department of Administrative Services has responsibility for and authority over information systems security in the executive department, including taking all measures reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. The Oregon Department of Administrative Services shall, after consultation and collaborative development with agencies, establish a state information systems security plan and associated standards, policies and procedures.

(3) The Oregon Department of Administrative Services, in its sole discretion, shall:

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

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

(c) Conduct vulnerability assessments of 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 Oregon Department of Administrative Services shall contract with qualified, independent consultants for the purpose of conducting vulnerability assessments under subsection (3) of this section.

(5) In collaboration with agencies, the Oregon Department of Administrative Services 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 department 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 agencies, using preexisting incident response capabilities.

(6) After consultation and collaborative development with agencies, the Oregon Department of Administrative Services 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 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. The department 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 Oregon Department of Administrative Services shall ensure that reasonably appropriate remedial actions are undertaken when the department 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) Agencies are responsible for the security of computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information outside the state's shared computing and network infrastructure following information security standards, policies and procedures established by the Oregon Department of Administrative Services and developed collaboratively with agencies. Agencies may establish plans, standards and measures that are more stringent than the standards established by the department to address specific agency needs if those plans, standards and measures do not contradict or contravene the state information systems security plan. Independent agency security plans shall be developed within the framework of the state information systems security plan.

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

(9) This section does not apply to:

(a) Research and student computer systems used by or in conjunction with the State Board of Higher Education or any state institution of higher education within the Oregon University System; and

(b)(A) Gaming systems and networks operated by the Oregon State Lottery or its contractors; 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 Oregon Department of Administrative Services shall adopt rules to carry out its responsibilities under this section.

SECTION 2. (1) Notwithstanding section 1 of this 2005 Act, 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 taking all measures 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 Oregon Department of Administrative Services as provided in section 1 of this 2005 Act.

(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 department under section 1 (2) of this 2005 Act;

(b) Assign responsibility for:

(A) Reviewing, monitoring and verifying the security of the agency'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 those 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 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 conducted by the department under section 1 (2) of this 2005 Act.

(5) If a joint information systems security plan and associated operational standards and policies cannot be agreed upon by the Oregon Department of Administrative Services and a statewide elected official named in subsection (1) of this section, the department may take steps reasonably necessary to condition, limit or preclude electronic traffic or other vulnerabilities between information systems for which the official has authority under subsection (1) of this section and the information systems for which the department has authority under section 1 (2) of this 2005 Act.

SECTION 3. The Secretary of State, the State Treasurer and the Attorney General shall establish the initial plans required by section 2 (2) of this 2005 Act no later than January 1, 2007.

SECTION 4. This 2005 Act being necessary for the immediate preservation of the public peace, health and safety, an emergency is declared to exist, and this 2005 Act takes effect on its passage.

Passed by House April 11, 2005

Repassed by House July 20, 2005

.....
Chief Clerk of House

.....
Speaker of House

Passed by Senate July 6, 2005

Repassed by Senate July 26, 2005

.....
President of Senate

Received by Governor:

.....M,....., 2005

Approved:

.....M,....., 2005

.....
Governor

Filed in Office of Secretary of State:

.....M,....., 2005

.....
Secretary of State