

B-Engrossed
House Bill 3145

Ordered by the Senate July 1
Including House Amendments dated April 4 and Senate Amendments
dated July 1

Sponsored by Representative DALLUM

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.

Requires Oregon Department of Administrative Services to [*develop and implement standards, policies and procedures relating to security of information technology systems*] **establish, after consultation and collaborative development with agencies, statewide information systems security plan and associated standards, policies and procedures.**

Provides that Secretary of State, State Treasurer and Attorney General have sole discretion and authority over information systems security in their respective agencies.

Declares emergency, effective on passage.

A BILL FOR AN ACT

1
2 Relating to information management in state agencies; and declaring an emergency.

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

4 **SECTION 1. (1) As used in this section:**

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

6 (b) **"Information systems" means computers, hardware, software, storage media, net-**
7 **works, operational procedures and processes used in the collection, processing, storage,**
8 **sharing or distribution of information within, or with any access beyond ordinary public ac-**
9 **cess to, the state's shared computing and network infrastructure.**

10 (2) **The Oregon Department of Administrative Services has responsibility for and au-**
11 **thority over information systems security in the executive department, including taking all**
12 **measures reasonably necessary to protect the availability, integrity or confidentiality of in-**
13 **formation systems or the information stored in information systems. The Oregon Depart-**
14 **ment of Administrative Services shall, after consultation and collaborative development with**
15 **agencies, establish a state information systems security plan and associated standards, poli-**
16 **cies and procedures.**

17 (3) **The Oregon Department of Administrative Services, in its sole discretion, may:**

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

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

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

25 (4) **In collaboration with agencies, the Oregon Department of Administrative Services**

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.

1 shall develop and implement policies for responding to events that damage or threaten the
2 availability, integrity or confidentiality of information systems or the information stored in
3 information systems, whether those systems are within, interoperable with or outside the
4 state's shared computing and network infrastructure. In the policies, the department shall
5 prescribe actions reasonably necessary to:

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

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

10 (c) Implement forensic techniques and controls developed under subsection (5) of this
11 section;

12 (d) Evaluate the event for the purpose of possible improvements to the security of in-
13 formation systems; and

14 (e) Communicate and share information with agencies, using preexisting incident re-
15 sponse capabilities.

16 (5) After consultation and collaborative development with agencies, the Oregon Depart-
17 ment of Administrative Services shall implement forensic techniques and controls for the
18 security of information systems, whether those systems are within, interoperable with or
19 outside the state's shared computing and network infrastructure. The techniques and con-
20 trols must include the use of specialized expertise, tools and methodologies, to investigate
21 events that damage or threaten the availability, integrity or confidentiality of information
22 systems or the information stored in information systems. The department shall consult
23 with the Oregon State Police, the Office of Emergency Management, the Governor and oth-
24 ers as necessary in developing forensic techniques and controls under this section.

25 (6) The Oregon Department of Administrative Services shall ensure that reasonably ap-
26 propriate remedial actions are undertaken when the department finds that such actions are
27 reasonably necessary by reason of vulnerability assessments of information systems under
28 subsection (3) of this section, evaluation of events under subsection (4) of this section and
29 other evaluations and audits.

30 (7)(a) Agencies are responsible for the security of computers, hardware, software, stor-
31 age media, networks, operational procedures and processes used in the collection, processing,
32 storage, sharing or distribution of information outside the state's shared computing and
33 network infrastructure following information security standards, policies and procedures
34 established by the Oregon Department of Administrative Services and developed
35 collaboratively with agencies. Agencies may establish plans, standards and measures that are
36 more stringent than the standards established by the department to address specific agency
37 needs if those plans, standards and measures do not contradict or contravene the state in-
38 formation systems security plan. Independent agency security plans shall be developed within
39 the framework of the state information systems security plan.

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

43 (8) This section does not apply to:

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

1 University System; and

2 (b)(A) Gaming systems and networks operated by the Oregon State Lottery or its con-
3 tractors; or

4 (B) The results of Oregon State Lottery reviews, evaluations and vulnerability assess-
5 ments of computer systems outside the state's shared computing and network
6 infrastructure.

7 (9) The Oregon Department of Administrative Services shall adopt rules to carry out its
8 responsibilities under this section.

9 **SECTION 2.** (1) Notwithstanding section 1 of this 2005 Act, the Secretary of State, the
10 State Treasurer and the Attorney General have sole discretion and authority over informa-
11 tion systems security in their respective agencies, including taking all measures reasonably
12 necessary to protect the availability, integrity or confidentiality of information systems or
13 the information stored in information systems.

14 (2) The Secretary of State, the State Treasurer and the Attorney General may each es-
15 tablish an information systems security plan and associated standards, policies and proce-
16 dures in collaboration with the Oregon Department of Administrative Services as provided
17 in section 1 of this 2005 Act.

18 (3) If a plan is established under subsection (2) of this section, at a minimum the plan
19 must:

20 (a) Be compatible with the state information systems security plan and associated stan-
21 dards, policies and procedures established by the department under section 1 (2) of this 2005
22 Act;

23 (b) Assign responsibility for:

24 (A) Reviewing, monitoring and verifying the security of the agency's information sys-
25 tems; and

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

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

34 (d) Prescribe actions reasonably necessary to:

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

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

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

41 (D) Evaluate the event for the purpose of possible improvements to the security of in-
42 formation systems; and

43 (E) Communicate and share information with agencies, using preexisting incident re-
44 sponse capabilities; and

45 (e) Describe and implement forensic techniques and controls for the security of infor-

1 mation systems, whether those systems are within, interoperable with or outside the state's
2 shared computing and network infrastructure, including the use of specialized expertise,
3 tools and methodologies, to investigate events that damage or threaten the availability, in-
4 tegrity or confidentiality of information systems or the information stored in information
5 systems.

6 (4) The Secretary of State, the State Treasurer and the Attorney General may participate
7 in the planning process conducted by the department under section 1 (2) of this 2005 Act.

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

15 **SECTION 3.** This 2005 Act being necessary for the immediate preservation of the public
16 peace, health and safety, an emergency is declared to exist, and this 2005 Act takes effect
17 on its passage.