

SENATE AMENDMENTS TO A-ENGROSSED HOUSE BILL 3145

By COMMITTEE ON RULES

July 1

1 On page 1 of the printed A-engrossed bill, line 8, after “information” insert “within, or with any
2 access beyond ordinary public access to, the state’s shared computing and network infrastructure”.

3 In line 11, after “measures” insert “reasonably”.

4 In line 13, after “shall” delete the rest of the line and lines 14 through 23 and insert “, after
5 consultation and collaborative development with agencies, establish a state information systems se-
6 curity plan and associated standards, policies and procedures.

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

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

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

10 “(c) Conduct vulnerability assessments of agency information systems for the purpose of evalu-
11 ating and responding to the susceptibility of information systems to attack, disruption or any other
12 event that threatens the availability, integrity or confidentiality of information systems or the in-
13 formation stored in information systems.”.

14 In line 24, delete “(5)” and insert “(4) In collaboration with agencies,”.

15 In line 26, before the period insert “, whether those systems are within, interoperable with or
16 outside the state’s shared computing and network infrastructure”.

17 Delete line 27 and insert “In the policies, the department shall prescribe actions reasonably
18 necessary to:”.

19 On page 2, line 1, delete the second “the” and insert “an”.

20 In line 2, after “actions” insert “reasonably”.

21 In line 4, delete “(6)” and insert “(5)”.

22 In line 5, delete “and”.

23 In line 7, delete the period and insert “; and”.

24 Delete lines 8 and 9 and insert:

25 “(e) Communicate and share information with agencies, using preexisting incident response ca-
26 pabilities.

27 “(5) After consultation and collaborative development with agencies, the Oregon Department of
28 Administrative Services shall implement forensic techniques and controls for the security of infor-
29 mation systems, whether those systems are within, interoperable with or outside the state’s shared
30 computing and network infrastructure. The techniques and controls must include the use of spe-”.

31 In line 13, delete the first “and” and insert a comma and after “Governor” insert “and others
32 as necessary”.

33 Delete lines 15 and 16 and insert:

34 “(6) The Oregon Department of Administrative Services shall ensure that reasonably appropriate
35 remedial actions are undertaken when the department finds that such actions are reasonably nec-

1 essary by reason of vulnerability assessments of information”.

2 In line 17, delete “(5)” and insert “(4)”.

3 After line 18, insert:

4 “(7)(a) Agencies are responsible for the security of computers, hardware, software, storage me-
5 dia, networks, operational procedures and processes used in the collection, processing, storage,
6 sharing or distribution of information outside the state’s shared computing and network
7 infrastructure following information security standards, policies and procedures established by the
8 Oregon Department of Administrative Services and developed collaboratively with agencies. Agen-
9 cies may establish plans, standards and measures that are more stringent than the standards estab-
10 lished by the department to address specific agency needs if those plans, standards and measures
11 do not contradict or contravene the state information systems security plan. Independent agency
12 security plans shall be developed within the framework of the state information systems security
13 plan.

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

17 “(8) This section does not apply to:

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

21 “(b)(A) Gaming systems and networks operated by the Oregon State Lottery or its contractors;
22 or

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

25 In line 19, delete “(8)” and insert “(9)”.

26 After line 20, insert:

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

32 **“(2) The Secretary of State, the State Treasurer and the Attorney General may each**
33 **establish an information systems security plan and associated standards, policies and proce-**
34 **dures in collaboration with the Oregon Department of Administrative Services as provided**
35 **in section 1 of this 2005 Act.**

36 **“(3) If a plan is established under subsection (2) of this section, at a minimum the plan**
37 **must:**

38 **“(a) Be compatible with the state information systems security plan and associated**
39 **standards, policies and procedures established by the department under section 1 (2) of this**
40 **2005 Act;**

41 **“(b) Assign responsibility for:**

42 **“(A) Reviewing, monitoring and verifying the security of the agency’s information sys-**
43 **tems; and**

44 **“(B) Conducting vulnerability assessments of information systems for the purpose of**
45 **evaluating and responding to the susceptibility of information systems to attack, disruption**

1 or any other event that threatens the availability, integrity or confidentiality of information
2 systems or the information stored in information systems;

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

7 “(d) Prescribe actions reasonably necessary to:

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

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

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

14 “(D) Evaluate the event for the purpose of possible improvements to the security of in-
15 formation systems; and

16 “(E) Communicate and share information with agencies, using preexisting incident re-
17 sponse capabilities; and

18 “(e) Describe and implement forensic techniques and controls for the security of infor-
19 mation systems, whether those systems are within, interoperable with or outside the state’s
20 shared computing and network infrastructure, including the use of specialized expertise,
21 tools and methodologies, to investigate events that damage or threaten the availability, in-
22 tegrity or confidentiality of information systems or the information stored in information
23 systems.

24 “(4) The Secretary of State, the State Treasurer and the Attorney General may partic-
25 ipate in the planning process conducted by the department under section 1 (2) of this 2005
26 Act.

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

34 In line 21, delete “2” and insert “3”.