

---

SENATE BILL 6528

---

State of Washington

64th Legislature

2016 Regular Session

By Senators Brown, Sheldon, Dammeier, Parlette, Schoesler, Warnick, Honeyford, Braun, Angel, Hewitt, Miloscia, O'Ban, Becker, Rivers, and Rolfes

Read first time 01/25/16. Referred to Committee on Trade & Economic Development.

1 AN ACT Relating to promoting economic development through  
2 protection of information technology resources; amending RCW  
3 43.105.054; reenacting and amending RCW 43.105.020; and creating new  
4 sections.

5 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

6 NEW SECTION. **Sec. 1.** (1) Communication and information  
7 resources in the various public agencies of the state are strategic  
8 and vital assets belonging to the people of Washington and are an  
9 important component of maintaining a vibrant economy. Coordinated  
10 efforts and a sense of urgency are necessary to protect these assets  
11 against unauthorized access, disclosure, use, and modification or  
12 destruction, whether accidental or deliberate, as well as to assure  
13 the confidentiality, integrity, and availability of information.

14 (2) State government has a duty to Washington citizens to ensure  
15 that the information entrusted to public agencies is safe, secure,  
16 and protected from unauthorized access, unauthorized use, or  
17 destruction.

18 (3) Securing the state's communication and information resources  
19 is a statewide imperative requiring a coordinated and shared effort  
20 from all departments, agencies, and political subdivisions of the

1 state and a long-term commitment to state funding that ensures the  
2 success of such efforts.

3 (4) Risks to communication and information resources must be  
4 managed, and the integrity of data and the source, destination, and  
5 processes applied to data must be assured.

6 (5) Information security standards, policies, and guidelines must  
7 be adopted and implemented throughout public agencies to ensure the  
8 development and maintenance of minimum information security controls  
9 to protect communication and information resources that support the  
10 operations and assets of those agencies.

11 (6) Washington state must build upon its existing expertise in  
12 information technology including research and development facilities  
13 and workforce to become a national leader in cybersecurity.

14 **Sec. 2.** RCW 43.105.020 and 2015 3rd sp.s. c 1 s 102 are each  
15 reenacted and amended to read as follows:

16 The definitions in this section apply throughout this chapter  
17 unless the context clearly requires otherwise.

18 (1) "Agency" means the consolidated technology services agency.

19 (2) "Board" means the technology services board.

20 (3) "Customer agencies" means all entities that purchase or use  
21 information technology resources, telecommunications, or services  
22 from the consolidated technology services agency.

23 (4) "Director" means the state chief information officer, who is  
24 the director of the consolidated technology services agency.

25 (5) "Enterprise architecture" means an ongoing activity for  
26 translating business vision and strategy into effective enterprise  
27 change. It is a continuous activity. Enterprise architecture creates,  
28 communicates, and improves the key principles and models that  
29 describe the enterprise's future state and enable its evolution.

30 (6) "Equipment" means the machines, devices, and transmission  
31 facilities used in information processing, including but not limited  
32 to computers, terminals, telephones, wireless communications system  
33 facilities, cables, and any physical facility necessary for the  
34 operation of such equipment.

35 (7) "Information" includes, but is not limited to, data, text,  
36 voice, and video.

37 (8) "Information security" means the protection of communication  
38 and information resources from unauthorized access, use, disclosure,  
39 disruption, modification, or destruction in order to:

1 (a) Prevent improper information modification or destruction;

2 (b) Preserve authorized restrictions on information access and  
3 disclosure;

4 (c) Ensure timely and reliable access to and use of information;  
5 and

6 (d) Maintain the confidentiality, integrity, and availability of  
7 information.

8 (9) "Information technology" includes, but is not limited to, all  
9 electronic technology systems and services, automated information  
10 handling, system design and analysis, conversion of data, computer  
11 programming, information storage and retrieval, telecommunications,  
12 requisite system controls, simulation, electronic commerce, radio  
13 technologies, and all related interactions between people and  
14 machines.

15 ~~((9))~~ (10) "Information technology portfolio" or "portfolio"  
16 means a strategic management process documenting relationships  
17 between agency missions and information technology and  
18 telecommunications investments.

19 ~~((10))~~ (11) "K-20 network" means the network established in RCW  
20 43.41.391.

21 ~~((11))~~ (12) "Local governments" includes all municipal and  
22 quasi-municipal corporations and political subdivisions, and all  
23 agencies of such corporations and subdivisions authorized to contract  
24 separately.

25 ~~((12))~~ (13) "Office" means the office of the state chief  
26 information officer within the consolidated technology services  
27 agency.

28 ~~((13))~~ (14) "Oversight" means a process of comprehensive risk  
29 analysis and management designed to ensure optimum use of information  
30 technology resources and telecommunications.

31 ~~((14))~~ (15) "Proprietary software" means that software offered  
32 for sale or license.

33 ~~((15))~~ (16) "Public agency" means any agency of this state or  
34 another state; any political subdivision or unit of local government  
35 of this state or another state including, but not limited to,  
36 municipal corporations, quasi-municipal corporations, special purpose  
37 districts, and local service districts; any public benefit nonprofit  
38 corporation; any agency of the United States; and any Indian tribe  
39 recognized as such by the federal government.

1       ~~((16))~~ (17) "Public benefit nonprofit corporation" means a  
2 public benefit nonprofit corporation as defined in RCW 24.03.005 that  
3 is receiving local, state, or federal funds either directly or  
4 through a public agency other than an Indian tribe or political  
5 subdivision of another state.

6       ~~((17))~~ (18) "Public record" has the definitions in RCW  
7 42.56.010 and chapter 40.14 RCW and includes legislative records and  
8 court records that are available for public inspection.

9       ~~((18))~~ (19) "Security incident" means an accidental or  
10 deliberative event that results in or constitutes an imminent threat  
11 of the unauthorized access, loss, disclosure, modification,  
12 disruption, or destruction of communication and information  
13 resources.

14       (20) "State agency" means every state office, department,  
15 division, bureau, board, commission, or other state agency, including  
16 offices headed by a statewide elected official.

17       ~~((19))~~ (21) "Telecommunications" includes, but is not limited  
18 to, wireless or wired systems for transport of voice, video, and data  
19 communications, network systems, requisite facilities, equipment,  
20 system controls, simulation, electronic commerce, and all related  
21 interactions between people and machines.

22       ~~((20))~~ (22) "Utility-based infrastructure services" includes  
23 personal computer and portable device support, servers and server  
24 administration, security administration, network administration,  
25 telephony, email, and other information technology services commonly  
26 used by state agencies.

27       **Sec. 3.** RCW 43.105.054 and 2015 3rd sp.s. c 1 s 108 are each  
28 amended to read as follows:

29       (1) The director shall establish standards and policies to govern  
30 information technology in the state of Washington.

31       (2) The office shall have the following powers and duties related  
32 to information services:

33       (a) To develop statewide standards and policies governing the:

34       (i) Acquisition of equipment, software, and technology-related  
35 services;

36       (ii) Disposition of equipment;

37       (iii) Licensing of the radio spectrum by or on behalf of state  
38 agencies; and

39       (iv) Confidentiality of computerized data;

1 (b) To develop statewide and interagency technical policies,  
2 standards, and procedures;

3 (c) To review and approve standards and common specifications for  
4 new or expanded telecommunications networks proposed by agencies,  
5 public postsecondary education institutions, educational service  
6 districts, or statewide or regional providers of K-12 information  
7 technology services;

8 (d) With input from the legislature and the judiciary, (~~{tøt}~~)  
9 to provide direction concerning strategic planning goals and  
10 objectives for the state;

11 (e) To establish policies for the periodic review by the director  
12 of state agency performance which may include but are not limited to  
13 analysis of:

14 (i) Planning, management, control, and use of information  
15 services;

16 (ii) Training and education;

17 (iii) Project management; and

18 (iv) Cybersecurity;

19 (f) To coordinate with state agencies with an annual information  
20 technology expenditure that exceeds ten million dollars to implement  
21 a technology business management program to identify opportunities  
22 for savings and efficiencies in information technology expenditures  
23 and to monitor ongoing financial performance of technology  
24 investments; (~~and~~)

25 (g) In conjunction with the consolidated technology services  
26 agency, to develop statewide standards for agency purchases of  
27 technology networking equipment and services;

28 (h) To implement a process for detecting, reporting, and  
29 responding to security incidents consistent with the information  
30 security standards, policies, and guidelines adopted by the director;

31 (i) To develop plans and procedures to ensure the continuity of  
32 operations for information resources that support the operations and  
33 assets of public agencies in the event of a security incident; and

34 (j) To work with the department of commerce and other economic  
35 development stakeholders to facilitate the development of Washington  
36 as a national leader in cybersecurity.

37 (3) Statewide technical standards to promote and facilitate  
38 electronic information sharing and access are an essential component  
39 of acceptable and reliable public access service and complement

1 content-related standards designed to meet those goals. The office  
2 shall:

3 (a) Establish technical standards to facilitate electronic access  
4 to government information and interoperability of information  
5 systems, including wireless communications systems; and

6 (b) Require agencies to include an evaluation of electronic  
7 public access needs when planning new information systems or major  
8 upgrades of systems.

9 In developing these standards, the office is encouraged to  
10 include the state library, state archives, and appropriate  
11 representatives of state and local government.

12 NEW SECTION. **Sec. 4.** This act may be known and cited as the  
13 cybersecurity jobs act.

--- END ---