

SSB 6528 - S AMD 559
By Senator Brown

ADOPTED 02/11/2016

1 Strike everything after the enacting clause and insert the
2 following:

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

11 (2) State government has a duty to Washington citizens to ensure
12 that the information entrusted to state agencies is safe, secure, and
13 protected from unauthorized access, unauthorized use, or destruction.

14 (3) Securing the state's communication and information resources
15 is a statewide imperative requiring a coordinated and shared effort
16 from all departments, agencies, and political subdivisions of the
17 state and a long-term commitment to state funding that ensures the
18 success of such efforts.

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

22 (5) Information security standards, policies, and guidelines must
23 be adopted and implemented throughout state agencies to ensure the
24 development and maintenance of minimum information security controls
25 to protect communication and information resources that support the
26 operations and assets of those agencies.

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

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

1 The definitions in this section apply throughout this chapter
2 unless the context clearly requires otherwise.

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

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

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

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

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

15 (6) "Equipment" means the machines, devices, and transmission
16 facilities used in information processing, including but not limited
17 to computers, terminals, telephones, wireless communications system
18 facilities, cables, and any physical facility necessary for the
19 operation of such equipment.

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

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

25 (a) Prevent improper information modification or destruction;

26 (b) Preserve authorized restrictions on information access and
27 disclosure;

28 (c) Ensure timely and reliable access to and use of information;
29 and

30 (d) Maintain the confidentiality, integrity, and availability of
31 information.

32 (9) "Information technology" includes, but is not limited to, all
33 electronic technology systems and services, automated information
34 handling, system design and analysis, conversion of data, computer
35 programming, information storage and retrieval, telecommunications,
36 requisite system controls, simulation, electronic commerce, radio
37 technologies, and all related interactions between people and
38 machines.

39 ((+9)) (10) "Information technology portfolio" or "portfolio"
40 means a strategic management process documenting relationships

1 between agency missions and information technology and
2 telecommunications investments.

3 ~~((+10))~~ (11) "K-20 network" means the network established in RCW
4 43.41.391.

5 ~~((+11))~~ (12) "Local governments" includes all municipal and
6 quasi-municipal corporations and political subdivisions, and all
7 agencies of such corporations and subdivisions authorized to contract
8 separately.

9 ~~((+12))~~ (13) "Office" means the office of the state chief
10 information officer within the ~~((consolidated technology services
11 agency))~~ Washington technology solutions.

12 ~~((+13))~~ (14) "Oversight" means a process of comprehensive risk
13 analysis and management designed to ensure optimum use of information
14 technology resources and telecommunications.

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

17 ~~((+15))~~ (16) "Public agency" means any agency of this state or
18 another state; any political subdivision or unit of local government
19 of this state or another state including, but not limited to,
20 municipal corporations, quasi-municipal corporations, special purpose
21 districts, and local service districts; any public benefit nonprofit
22 corporation; any agency of the United States; and any Indian tribe
23 recognized as such by the federal government.

24 ~~((+16))~~ (17) "Public benefit nonprofit corporation" means a
25 public benefit nonprofit corporation as defined in RCW 24.03.005 that
26 is receiving local, state, or federal funds either directly or
27 through a public agency other than an Indian tribe or political
28 subdivision of another state.

29 ~~((+17))~~ (18) "Public record" has the definitions in RCW
30 42.56.010 and chapter 40.14 RCW and includes legislative records and
31 court records that are available for public inspection.

32 ~~((+18))~~ (19) "Security incident" means an accidental or
33 deliberative event that results in or constitutes an imminent threat
34 of the unauthorized access, loss, disclosure, modification,
35 disruption, or destruction of communication and information
36 resources.

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

1 (~~(19)~~) (21) "Telecommunications" includes, but is not limited
2 to, wireless or wired systems for transport of voice, video, and data
3 communications, network systems, requisite facilities, equipment,
4 system controls, simulation, electronic commerce, and all related
5 interactions between people and machines.

6 (~~(20)~~) (22) "Utility-based infrastructure services" includes
7 personal computer and portable device support, servers and server
8 administration, security administration, network administration,
9 telephony, email, and other information technology services commonly
10 used by state agencies.

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

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

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

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

18 (i) Acquisition of equipment, software, and technology-related
19 services;

20 (ii) Disposition of equipment;

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

23 (iv) Confidentiality of computerized data;

24 (b) To develop statewide and interagency technical policies,
25 standards, and procedures;

26 (c) To review and approve standards and common specifications for
27 new or expanded telecommunications networks proposed by agencies,
28 public postsecondary education institutions, educational service
29 districts, or statewide or regional providers of K-12 information
30 technology services;

31 (d) With input from the legislature and the judiciary, (~~{to}~~)
32 to provide direction concerning strategic planning goals and
33 objectives for the state;

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

37 (i) Planning, management, control, and use of information
38 services;

39 (ii) Training and education;

1 (iii) Project management; and

2 (iv) Cybersecurity;

3 (f) To coordinate with state agencies with an annual information
4 technology expenditure that exceeds ten million dollars to implement
5 a technology business management program to identify opportunities
6 for savings and efficiencies in information technology expenditures
7 and to monitor ongoing financial performance of technology
8 investments; (~~and~~)

9 (g) In conjunction with the consolidated technology services
10 agency, to develop statewide standards for agency purchases of
11 technology networking equipment and services;

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

15 (i) To develop plans and procedures to ensure the continuity of
16 commerce for information resources that support the operations and
17 assets of state agencies in the event of a security incident; and

18 (j) To work with the department of commerce and other economic
19 development stakeholders to facilitate the development of a strategy
20 that includes key local, state, and federal assets that will create
21 Washington as a national leader in cybersecurity. The office shall
22 collaborate with, including but not limited to, community colleges,
23 universities, the national guard, the department of defense, the
24 department of energy, and national laboratories to develop the
25 strategy.

26 (3) Statewide technical standards to promote and facilitate
27 electronic information sharing and access are an essential component
28 of acceptable and reliable public access service and complement
29 content-related standards designed to meet those goals. The office
30 shall:

31 (a) Establish technical standards to facilitate electronic access
32 to government information and interoperability of information
33 systems, including wireless communications systems; and

34 (b) Require agencies to include an evaluation of electronic
35 public access needs when planning new information systems or major
36 upgrades of systems.

37 In developing these standards, the office is encouraged to
38 include the state library, state archives, and appropriate
39 representatives of state and local government.

1 NEW SECTION. **Sec. 4.** This act may be known and cited as the
2 cybersecurity jobs act."

SSB 6528 - S AMD **559**
By Senator Brown

ADOPTED 02/11/2016

3 On page 1, line 2 of the title, after "resources;" strike the
4 remainder of the title and insert "amending RCW 43.105.054;
5 reenacting and amending RCW 43.105.020; and creating new sections."

EFFECT: Specifies that the Office of the Chief Information Officer and the Department of Commerce shall work with stakeholders to develop a strategy for making Washington State a national leader in cyber security. Limits legislative intent to state agencies and updates the name of the Consolidated Technology Services agency to Washington Technology Solutions.

--- END ---