

---

**SUBSTITUTE SENATE BILL 5662**

---

**State of Washington**

**66th Legislature**

**2019 Regular Session**

**By** Senate Environment, Energy & Technology (originally sponsored by Senators Palumbo, Carlyle, Rolfes, Mullet, Nguyen, Hobbs, Lias, Pedersen, and Braun)

1       AN ACT Relating to cloud computing solutions; amending RCW  
2   43.105.020; adding a new section to chapter 43.105 RCW; and repealing  
3   RCW 43.105.375.

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

5       **Sec. 1.** RCW 43.105.020 and 2017 c 92 s 2 are each amended to  
6   read as follows:

7       The definitions in this section apply throughout this chapter  
8   unless the context clearly requires otherwise.

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

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

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

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

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

1       (6) "Equipment" means the machines, devices, and transmission  
2 facilities used in information processing, including but not limited  
3 to computers, terminals, telephones, wireless communications system  
4 facilities, cables, and any physical facility necessary for the  
5 operation of such equipment.

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

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

11       (a) Prevent improper information modification or destruction;

12       (b) Preserve authorized restrictions on information access and  
13 disclosure;

14       (c) Ensure timely and reliable access to and use of information;  
15 and

16       (d) Maintain the confidentiality, integrity, and availability of  
17 information.

18       (9) "Information technology" includes, but is not limited to, all  
19 electronic technology systems and services, automated information  
20 handling, system design and analysis, conversion of data, computer  
21 programming, information storage and retrieval, telecommunications,  
22 requisite system controls, simulation, electronic commerce, radio  
23 technologies, and all related interactions between people and  
24 machines.

25       (10) "Information technology portfolio" or "portfolio" means a  
26 strategic management process documenting relationships between agency  
27 missions and information technology and telecommunications  
28 investments.

29       (11) "K-20 network" means the network established in RCW  
30 43.41.391.

31       (12) "Local governments" includes all municipal and quasi-  
32 municipal corporations and political subdivisions, and all agencies  
33 of such corporations and subdivisions authorized to contract  
34 separately.

35       (13) "Office" means the office of the state chief information  
36 officer within the consolidated technology services agency.

37       (14) "Oversight" means a process of comprehensive risk analysis  
38 and management designed to ensure optimum use of information  
39 technology resources and telecommunications.

1 (15) "Proprietary software" means that software offered for sale  
2 or license.

3 (16) "Public agency" means any agency of this state or another  
4 state; any political subdivision or unit of local government of this  
5 state or another state including, but not limited to, municipal  
6 corporations, quasi-municipal corporations, special purpose  
7 districts, and local service districts; any public benefit nonprofit  
8 corporation; any agency of the United States; and any Indian tribe  
9 recognized as such by the federal government.

10 (17) "Public benefit nonprofit corporation" means a public  
11 benefit nonprofit corporation as defined in RCW 24.03.005 that is  
12 receiving local, state, or federal funds either directly or through a  
13 public agency other than an Indian tribe or political subdivision of  
14 another state.

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

18 (19) "Public safety" refers to any entity or services that ensure  
19 the welfare and protection of the public.

20 (20) "Security incident" means an accidental or deliberative  
21 event that results in or constitutes an imminent threat of the  
22 unauthorized access, loss, disclosure, modification, disruption, or  
23 destruction of communication and information resources.

24 (21) "State agency" means every state office, department,  
25 division, bureau, board, commission, or other state agency, including  
26 offices headed by a statewide elected official.

27 (22) "Telecommunications" includes, but is not limited to,  
28 wireless or wired systems for transport of voice, video, and data  
29 communications, network systems, requisite facilities, equipment,  
30 system controls, simulation, electronic commerce, and all related  
31 interactions between people and machines.

32 (23) "Utility-based infrastructure services" includes personal  
33 computer and portable device support, servers and server  
34 administration, security administration, network administration,  
35 telephony, email, and other information technology services commonly  
36 used by state agencies.

37 (24) "Cloud computing" has the same meaning as provided by the  
38 special publication 800-145 issued by the national institute of  
39 standards and technology of the United States department of commerce  
40 as of September 2011.

1       (25) "Dislocated worker" has the same meaning as defined in RCW  
2       50.04.075.

3       NEW SECTION.     **Sec. 2.**   A new section is added to chapter 43.105  
4       RCW to read as follows:

5       (1) State agencies must adopt third-party, commercial cloud  
6       computing solutions for any new information technology or  
7       telecommunications investments except as provided in subsection (3)  
8       of this section. Prior to selecting and implementing a cloud  
9       computing solution, state agencies must evaluate:

10      (a) The ability of the cloud computing solution to meet security  
11      and compliance requirements for all workload types including low,  
12      moderate, and high impact data, leveraging defined federal  
13      authorization or accreditation programs to the fullest extent  
14      possible; and

15      (b) The portability of data, should the state agency choose to  
16      discontinue use of the cloud service.

17      (2) By December 31, 2020, state agencies must submit a cloud  
18      migration plan to the office that outlines its technology sourcing  
19      strategy, including prioritization and use of cloud computing  
20      solutions, and ways it can utilize cloud to reduce costs.

21      (3) State agencies with a service requirement that prohibits the  
22      utilization of a cloud computing solution must receive a waiver from  
23      the office.

24      (a) Waivers must be based on written justification from the  
25      requesting state agency citing specific services or performance  
26      requirements for not utilizing a cloud computing solution.

27      (b) Information on waiver applications must be included in the  
28      cloud migration report submitted to the legislature.

29      (4) State agencies are prohibited from installing and operating  
30      servers, storage, networking, and related hardware in agency-operated  
31      facilities unless a waiver is granted by the office or otherwise  
32      allowed by statewide policy.

33      (5) The office must conduct a statewide cloud computing readiness  
34      assessment to prepare for the migration of core services to cloud  
35      services, including ways it can leverage cloud computing to reduce  
36      costs. The assessment must:

37      (a) Inventory state agency assets, associated service contracts,  
38      and other relevant information;

1 (b) Identify impacts to state agency staffing resulting from the  
2 migration to cloud computing including: (i) Skill gaps between  
3 current on-premises computing practices and how cloud services are  
4 procured, secured, administered, maintained, and developed; and (ii)  
5 necessary retraining and ongoing training and development to ensure  
6 state agency staff maintain the skills necessary to effectively  
7 maintain information security and understand changes to enterprise  
8 architectures;

9 (c) Identify additional resources needed by the agency to enable  
10 sufficient cloud migration support to state agencies; and

11 (d) Support state agency migration of one hundred percent of  
12 server capacity by June 30, 2023, excluding capacity that has been  
13 granted a waiver under subsection (3) of this section.

14 (6) By June 30, 2020, the office must submit a report to the  
15 governor and the appropriate committees of the legislature that  
16 summarizes statewide cloud migration readiness and makes  
17 recommendations for any changes to migration goals.

18 (7) The office must submit a cloud migration progress report to  
19 the governor and the appropriate committees of the legislature every  
20 six months, with the first report due in January 2021.

21 (8) The agency must oversee and provide technical specifications  
22 to the department of enterprise services who must conduct competitive  
23 procurements processes to identify no more than three contracts per  
24 procurement to provide cloud computing services and to provide system  
25 migration support. The procurement process must be reopened and  
26 contracts must be renegotiated at a minimum every ten years.

27 (9) Starting June 30, 2020, state agency directors of human  
28 resources must report annually to the office and the employment  
29 security department on impacts to staffing related to state employees  
30 who could not be reassigned to other duties within the state agency  
31 as a result of the cloud migration.

32 (10) Subject to the availability of amounts appropriated for this  
33 specific purpose, there is created a training program for employees  
34 who could not be reassigned to other duties within the state agency  
35 as a result of the cloud migration. The state human resources  
36 department of the office of financial management, in coordination  
37 with the office and the employment security department, must oversee  
38 requests for training and allocation of moneys. Upon approval from  
39 the office of financial management, moneys may be used for early  
40 retirement packages for employees within five years of retirement age

1 on a voluntary basis and for other dislocated workers for retraining  
2 programs, certification, degrees, or classes with an emphasis on  
3 technical fields that complement the cloud migration strategy. By  
4 January 1, 2020, the employment security department, in coordination  
5 with the office of financial management, must develop a program to  
6 support employees and dislocated workers identified in this  
7 subsection and affected by the policies created in this section.

8 (11) This section does not apply to institutions of higher  
9 education.

10 NEW SECTION. **Sec. 3.** RCW 43.105.375 (Use of state data center—  
11 Business plan and migration schedule for state agencies—Exceptions)  
12 and 2015 3rd sp.s. c 1 s 219 & 2011 1st sp.s. c 43 s 735 are each  
13 repealed.

--- END ---