ENGROSSED SECOND SUBSTITUTE SENATE BILL 5662

State of Washington 66th Legislature 2019 Regular Session

By Senate Ways & Means (originally sponsored by Senators Palumbo, Carlyle, Rolfes, Mullet, Nguyen, Hobbs, Liias, Pedersen, and Braun)

READ FIRST TIME 03/01/19.

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

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

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

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

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

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

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

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

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

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

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

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

(a) Prevent improper information modification or destruction;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) State agencies must adopt third-party, commercial cloud computing solutions for any new information technology or telecommunications investments except as provided in subsection (2) of this section. Prior to selecting and implementing a cloud computing solution, state agencies must evaluate:

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

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

(2) State agencies must receive a waiver from the office if there is a service requirement that prohibits the adoption of a cloud computing solution, as required in subsection (1) of this section.

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

(b) Information on waiver applications, requested and granted, must be submitted by the office to the appropriate committees of the legislature by December 30th each calendar year.

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

(4) Subject to the availability of amounts appropriated for this specific purpose, the office must conduct a statewide cloud computing readiness assessment to prepare for the migration of core services to cloud services, including ways it can leverage cloud computing to reduce costs. The assessment must:

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

(b) Identify impacts to state agency staffing resulting from the migration to cloud computing including: (i) Skill gaps between current on-premises computing practices and how cloud services are procured, secured, administered, maintained, and developed; and (ii) necessary retraining and ongoing training and development to ensure state agency staff maintain the skills necessary to effectively

maintain information security and understand changes to enterprise architectures; and

(c) Identify additional resources needed by the agency to enable sufficient cloud migration support to state agencies.

(5) By June 30, 2020, the office must submit a report to the governor and the appropriate committees of the legislature that summarizes statewide cloud migration readiness and makes recommendations for migration goals.

(6) Subject to the availability of amounts appropriated for this specific purpose, the agency must oversee and provide technical specifications to the department of enterprise services who must conduct competitive procurements processes to identify no more than three contracts per procurement to provide cloud computing services and to provide system migration support. The procurement process must be reopened and contracts must be renegotiated at a minimum every five years.

(7) This section does not apply to institutions of higher education.

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

--- END ---