

**RCW 43.105.020 Definitions.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Agency" means Washington technology solutions.

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

(3) "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 or its successor publications.

(4) "Customer agencies" means all entities that purchase or use information technology resources, telecommunications, or services from Washington technology solutions.

(5) "Director" means the state chief information officer, who is the director of Washington technology solutions.

(6) "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.

(7) "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.

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

(9) "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.

(10) "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.

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

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

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

(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 24.03A.245 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) "Ransomware" means a type of malware that attempts to deny a user or organization access to data or systems, usually through encryption, until a sum of money or other currency is paid or the user or organization is forced to take a specific action.

(21) "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.

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

(23) "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.

(24) "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. [2024 c 54 s 3; 2023 c 124 s 1. Prior: 2021 c 176 s 5223; 2021 c 40 s 2; 2017 c 92 s 2; 2016 c 237 s 2; prior: 2015 3rd sp.s. c 1 s 102; 2011 1st sp.s. c 43 s 802; 2010 1st sp.s. c 7 s 64; prior: 2009 c 565 s 32; 2009 c 509 s 7; 2009 c 486 s 14; 2003 c 18 s 2; prior: 1999 c 285 s 1; 1999 c 80 s 1; 1993 c 280 s 78; 1990 c 208 s 3; 1987 c 504 s 3; 1973 1st ex.s. c 219 s 3; 1967 ex.s. c 115 s 2.]

**Effective date—2021 c 176:** See note following RCW 24.03A.005.

**Findings—Intent—2021 c 40:** See note following RCW 43.105.375.

**Short title—2016 c 237:** "This act may be known and cited as the cybersecurity jobs act of 2016." [2016 c 237 s 5.]

**Effective date—2015 3rd sp.s. c 1 ss 101-109, 201-224, 406-408, 410, 501-507, 601, and 602:** See note following RCW 43.105.007.

**Effective date—Purpose—2011 1st sp.s. c 43:** See notes following RCW 43.19.003.

**Effective date—2010 1st sp.s. c 26; 2010 1st sp.s. c 7:** See note following RCW 43.330.400.

**Findings—Intent—Purpose—Effective date—2009 c 509:** See notes following RCW 43.330.400.

**Conflict with federal requirements—Intent—2009 c 486:** See notes following RCW 28B.30.530.

**Intent—Finding—2003 c 18:** "It is the intent of the legislature to ensure that the state's considerable investment in radio communications facilities, and the radio spectrum that is licensed to government entities in the state, are managed in a way that promotes to the maximum extent the health and safety of the state's citizens and the economic efficiencies of coordinated planning, development, management, maintenance, accountability, and performance. The legislature finds that such coordination is essential for disaster preparedness, emergency management, and public safety, and that such coordination will result in more cost-effective use of state resources and improved government services." [2003 c 18 s 1.]

**Effective date—2003 c 18:** "This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect July 1, 2003." [2003 c 18 s 6.]

**Effective date—1993 c 280:** See RCW 43.330.902.

**Effective date—1967 ex.s. c 115:** "This act is necessary for the immediate preservation of the public peace, health and safety, the support of the state government and its existing public institutions, and shall take effect July 1, 1967." [1967 ex.s. c 115 s 8.]