Chapter 43.105 RCW
CONSOLIDATED TECHNOLOGY SERVICES AGENCY

Sections

RCW 43.105.006 Consolidated technology services agency—Purpose. To achieve maximum benefit from advances in information technology the state establishes a centralized provider and procurer of certain information technology services as an agency to support the needs of state agencies. This agency shall be known as the consolidated technology services agency. To ensure maximum benefit to the state, state agencies shall rely on the consolidated technology services agency for those services with a business case of broad use, uniformity, scalability, and price sensitivity to aggregation and volume.

To successfully meet agency needs and meet its obligation as the primary service provider for these services, the consolidated technology services agency must offer high quality services at the lowest possible price. It must be able to attract an adaptable and competitive workforce, be authorized to procure services where the business case justifies it, and be accountable to its customers for the efficient and effective delivery of critical business services.

The consolidated technology services agency is established as an agency in state government. The agency is established with clear accountability to the agencies it serves and to the public. This accountability will come through enhanced transparency in the agency's operation and performance. The agency is also established with broad flexibility to adapt its operations and service catalog to address the needs of customer agencies, and to do so in the most cost-effective ways. [2011 1st sp.s. c 43 § 801.]

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

RCW 43.105.007 Purpose. Information technology is a tool used by state agencies to improve their ability to deliver public services efficiently and effectively. Advances in information technology, including advances in hardware, software, and business processes for implementing and managing these resources, offer new opportunities to improve the level of support provided to citizens and state agencies and to reduce the per-transaction cost of these services. These advances are one component in the process of reengineering how government delivers services to citizens.

To fully realize the service improvements and cost efficiency from the effective application of information technology to its business processes, state government must establish decision-making

structures that connect business processes and information technology in an operating model. Many of these business practices transcend individual agency processes and should be worked at the enterprise level. To do this requires an effective partnership of executive management, business processes owners, and providers of support functions necessary to efficiently and effectively deliver services to citizens.

To maximize the potential for information technology to contribute to government business process reengineering, the state must establish clear central authority to plan, set enterprise policies and standards, and provide project oversight and management analysis of the various aspects of a business process.

Establishing a state chief information officer as the director of the consolidated technology services agency will provide state government with the cohesive structure necessary to develop improved operating models with agency directors and reengineer business process to enhance service delivery while capturing savings.

To achieve maximum benefit from advances in information technology, the state establishes a centralized provider and procurer of certain information technology services as an agency to support the needs of public agencies. This agency shall be known as the consolidated technology services agency. To ensure maximum benefit to the state, state agencies shall rely on the consolidated technology services agency for those services with a business case of broad use, uniformity, scalability, and price sensitivity to aggregation and volume.

To successfully meet public agency needs and meet its obligation as the primary service provider for these services, the consolidated technology services agency must offer high quality services at the best value. It must be able to attract an adaptable and competitive workforce, be authorized to procure services where the business case justifies it, and be accountable to its customers for the efficient and effective delivery of critical business services.

The consolidated technology services agency is established with clear accountability to the agencies it serves and to the public. This accountability will come through enhanced transparency in the agency's operation and performance. The agency is also established with broad flexibility to adapt its operations and service catalog to address the needs of customer agencies, and to do so in the most cost-effective ways. [2015 3rd sp.s. c 1 § 101; 2011 1st sp.s. c 43 § 701. Formerly RCW 43.41A.003.]

Effective date—2015 3rd sp.s. c 1 §§ 101-109, 201-224, 406-408, 410, 501-507, 601, and 602: "Sections 101 through 109, 201 through 224, 406 through 408, 410, 501 through 507, 601, and 602 of this act are necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and take effect July 1, 2015." [2015 3rd sp.s. c 1 § 604.]

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

RCW 43.105.020 Definitions. 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) "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 the consolidated technology services agency.

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

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

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

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

(17) "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.

(18) "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.

(19) "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.

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

(21) "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.

(22) "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.

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

(24) "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.

(25) "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. [2023 c 124 § 1. Prior: 2021 c 176 § 5223; 2021 c 40 § 2; 2017 c 92 § 2; 2016 c 237 § 2; prior: 2015 3rd sp.s. c 1 § 102; 2011 1st sp.s. c 43 § 802; 2010 1st sp.s. c 7 § 64; prior: 2009 c 565 § 32; 2009 c 509 § 7; 2009 c 486 § 14; 2003 c 18 § 2; prior: 1999 c 285 § 1; 1999 c 80 § 1; 1993 c 280 § 78; 1990 c 208 § 3; 1987 c 504 § 3; 1973 1st ex.s. c 219 § 3; 1967 ex.s. c 115 § 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 § 5.]

Effective date—2015 3rd sp.s. c 1 §§ 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 § 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 § 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 § 8.]

RCW 43.105.025 Agency created—Appointment of director—Director's duties. (1) There is created the consolidated technology services agency, an agency of state government. The agency shall be headed by a director, who is the state chief information officer. The director shall be appointed by the governor with the consent of the senate. The director shall serve at the governor's pleasure and shall receive such salary as determined by the governor. If a vacancy occurs in the position while the senate is not in session, the governor shall make a temporary appointment until the next meeting of the senate at which time he or she shall present to that body his or her nomination for the position.

(2) The director shall:

(a) Appoint a confidential secretary and such deputy and assistant directors as needed to administer the agency; and

(b) Appoint such professional, technical, and clerical assistants and employees as may be necessary to perform the duties imposed by this chapter in accordance with chapter 41.06 RCW, except as otherwise provided by law.

(3) The director may create such administrative structures as he or she deems appropriate and may delegate any power or duty vested in him or her by this chapter or other law.

(4) The director shall exercise all the powers and perform all the duties prescribed by law with respect to the administration of this chapter including:

(a) Reporting to the governor any matters relating to abuses and evasions of this chapter;

(b) Accepting and expending gifts and grants that are related to the purposes of this chapter;

(c) Applying for grants from public and private entities, and receiving and administering any grant funding received for the purpose and intent of this chapter; and

(d) Performing other duties as are necessary and consistent with law. [2015 3rd sp.s. c 1 § 103; 2011 1st sp.s. c 43 § 803; 1999 c 80 § 5; 1992 c 20 § 9; 1987 c 504 § 6. Formerly RCW 43.105.047.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

Severability—1992 c 20: "If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected." [1992 c 20 § 14.]

Captions not law—1992 c 20: "Captions used in this act do not constitute any part of the law." [1992 c 20 § 16.]

Civil service exemptions: RCW 41.06.094.

RCW 43.105.052 Powers and duties of agency. The agency shall:

(1) Make available information services to public agencies and public benefit nonprofit corporations;

(2) Establish rates and fees for services provided by the agency;

(3) Develop a billing rate plan for a two-year period to coincide with the budgeting process. The rate plan must be subject to review at least annually by the office of financial management. The rate plan must show the proposed rates by each cost center and show the components of the rate structure as mutually determined by the agency and the office of financial management. The rate plan and any adjustments to rates must be approved by the office of financial management;

(4) Develop a detailed business plan for any service or activity to be contracted under *RCW 41.06.142(7)(b);

(5) Develop plans for the agency's achievement of statewide goals and objectives set forth in the state strategic information technology plan required under RCW 43.105.220;

(6) Enable the standardization and consolidation of information technology infrastructure across all state agencies to support enterprise-based system development and improve and maintain service delivery; and

(7) Perform all other matters and things necessary to carry out the purposes and provisions of this chapter. [2015 3rd sp.s. c 1 § 104; 2011 1st sp.s. c 43 § 804; 2010 1st sp.s. c 7 § 16; 2000 c 180 § 1; 1999 c 80 § 6; 1993 c 281 § 53; 1992 c 20 § 10; 1990 c 208 § 7; 1987 c 504 § 8.]

***Reviser's note:** RCW 41.06.142 was amended by 2020 c 269 § 2, changing subsection (7) to subsection (11).

Effective date—2015 3rd sp.s. c 1 §§ 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 43.03.027.

Effective date—1993 c 281: See note following RCW 41.06.022.

Severability—Captions not law—1992 c 20: See notes following RCW 43.105.025.

RCW 43.105.054 Governing information technology—Standards and policies—Powers and duties of office. (1) The director shall establish standards and policies to govern information technology in the state of Washington.

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

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

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

(ii) Disposition of equipment;

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

(iv) Confidentiality of computerized data;

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

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

(d) With input from the legislature and the judiciary, to provide direction concerning strategic planning goals and objectives for the state;

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

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

(ii) Training and education;

(iii) Project management; and

(iv) Cybersecurity, in coordination with the office of cybersecurity;

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

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

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

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

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

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

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

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

In developing these standards, the office is encouraged to include the state library, state archives, and appropriate representatives of state and local government. [2021 c 291 § 9; 2016 c 237 § 3; 2015 3rd sp.s. c 1 § 108; 2013 2nd sp.s. c 33 § 1; 2011 1st sp.s. c 43 § 706. Formerly RCW 43.41A.025.]

Short title—2016 c 237: See note following RCW 43.105.020.

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.057 Rule-making authority. The agency shall adopt rules as necessary under chapter 34.05 RCW to implement the provisions of this chapter. [2011 1st sp.s. c 43 § 807; 1992 c 20 § 11; 1990 c 208 § 13.]

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

Severability—Captions not law—1992 c 20: See notes following RCW 43.105.025.

RCW 43.105.060 Contracts by state and local agencies with agency. State and local government agencies are authorized to enter into any contracts with the agency which may be necessary or desirable to effectuate the purposes and policies of this chapter or for maximum utilization of facilities and services which are the subject of this chapter. [2011 1st sp.s. c 43 § 808; 1987 c 504 § 10; 1973 1st ex.s. c 219 § 9; 1967 ex.s. c 115 § 6.]

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

Effective date—1967 ex.s. c 115: See note following RCW 43.105.020.

RCW 43.105.111 Performance targets—Plans for achieving goals—Quarterly reports to governor. The director shall set performance targets and approve plans for achieving measurable and specific goals for the agency. By January 2017, the appropriate organizational performance and accountability measures and performance targets shall be submitted to the governor. These measures and targets shall include measures of performance demonstrating specific and measurable improvements related to service delivery and costs, operational efficiencies, and overall customer satisfaction. The agency shall develop a dashboard of key performance measures that will be updated quarterly and made available on the agency public website.

The director shall report to the governor on agency performance at least quarterly. The reports shall be included on the agency's website and accessible to the public. [2015 3rd sp.s. c 1 § 105; 2011 1st sp.s. c 43 § 806.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.205 Office of the state chief information officer—Created—Powers, duties, and functions. (1) The office of the state chief information officer is created within the consolidated technology services agency.

(2) The primary duties of the office are:

(a) To prepare and lead the implementation of a strategic direction and enterprise architecture for information technology for state government;

(b) To establish standards and policies for the consistent and efficient operation of information technology services throughout state government;

(c) To establish statewide enterprise architecture that will serve as the organizing standard for information technology for state agencies;

(d) To educate and inform state managers and policymakers on technological developments, industry trends and best practices, industry benchmarks that strengthen decision making and professional development, and industry understanding for public managers and decision makers; and

(e) To perform all other matters and things necessary to carry out the purposes and provisions of this chapter.

(3) In the case of institutions of higher education, the powers of the office and the provisions of this chapter apply to business and administrative applications but do not apply to (a) academic and research applications; and (b) medical, clinical, and health care applications, including the business and administrative applications for such operations. However, institutions of higher education must disclose to the office any proposed academic applications that are enterprise-wide in nature relative to the needs and interests of other institutions of higher education. Institutions of higher education shall provide to the director sufficient data and information on proposed expenditures on business and administrative applications to permit the director to evaluate the proposed expenditures pursuant to RCW 43.88.092(3).

(4) The legislature and the judiciary, which are constitutionally recognized as separate branches of government, are strongly encouraged to coordinate with the office and participate in shared services initiatives and the development of enterprise-based strategies, where appropriate. Legislative and judicial agencies of the state shall submit to the director information on proposed information technology expenditures to allow the director to evaluate the proposed expenditures on an advisory basis. [2015 3rd sp.s. c 1 § 201; 2013 2nd sp.s. c 33 § 3; 2011 1st sp.s. c 43 § 702. Formerly RCW 43.41A.010.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.220 Strategic information technology plan—Biennial performance reports. (1) The office shall prepare a state strategic information technology plan which shall establish a statewide mission, goals, and objectives for the use of information technology, including goals for electronic access to government records, information, and services. The plan shall be developed in accordance with the standards and policies established by the office. The office shall seek the advice of the board in the development of this plan.

The plan shall be updated as necessary and submitted to the governor and the legislature.

(2) The office shall prepare a biennial state performance report on information technology based on state agency performance reports required under RCW 43.105.235 and other information deemed appropriate by the office. The report shall include, but not be limited to:

(a) An analysis, based upon agency portfolios, of the state's information technology infrastructure, including its value, condition, and capacity;

(b) An evaluation of performance relating to information technology;

(c) An assessment of progress made toward implementing the state strategic information technology plan, including progress toward electronic access to public information and enabling citizens to have two-way access to public records, information, and services; and

(d) An analysis of the success or failure, feasibility, progress, costs, and timeliness of implementation of major information technology projects under RCW 43.105.245. At a minimum, the portion of the report regarding major technology projects must include:

(i) The total cost data for the entire life-cycle of the project, including capital and operational costs, broken down by staffing costs, contracted service, hardware purchase or lease, software purchase or lease, travel, and training. The original budget must also be shown for comparison;

(ii) The original proposed project schedule and the final actual project schedule;

(iii) Data regarding progress towards meeting the original goals and performance measures of the project;

(iv) Discussion of lessons learned on the project, performance of any contractors used, and reasons for project delays or cost increases; and

(v) Identification of benefits generated by major information technology projects developed under RCW 43.105.245.

Copies of the report shall be distributed biennially to the governor and the legislature. The major technology section of the report must examine major information technology projects completed in the previous biennium. [2015 3rd sp.s. c 1 § 203; 2011 1st sp.s. c 43 § 707. Formerly RCW 43.41A.030.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.225 Managing information technology as a statewide portfolio. Management of information technology across state government requires managing resources and business processes across multiple agencies. It is no longer sufficient to pursue efficiencies within agency or individual business process boundaries. The state must manage the business process changes and information technology in support of business processes as a statewide portfolio. The director will use agency information technology portfolio planning as input to develop a statewide portfolio to guide resource allocation and prioritization decisions. [2015 3rd sp.s. c 1 § 204; 2011 1st sp.s. c 43 § 708. Formerly RCW 43.41A.035.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.230 State agency information technology portfolio—Basis for decisions and plans. A state agency information technology portfolio shall serve as the basis for making information technology decisions and plans which may include, but are not limited to:

(1) System refurbishment, acquisitions, and development efforts;

(2) Setting goals and objectives for using information technology;

(3) Assessments of information processing performance, resources, and capabilities;

(4) Ensuring the appropriate transfer of technological expertise for the operation of new systems developed using external resources;

(5) Guiding new investment demand, prioritization, selection, performance, and asset value of technology and telecommunications; and

(6) Progress toward providing electronic access to public information. [2015 3rd sp.s. c 1 § 205; 2011 1st sp.s. c 43 § 709. Formerly RCW 43.41A.040.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.235 State agency information technology portfolio—Exemptions. (1) Each state agency shall develop an information technology portfolio consistent with RCW 43.105.341. The superintendent of public instruction shall develop its portfolio in conjunction with educational service districts and statewide or regional providers of K-12 education information technology services.

(2) The director may exempt any state agency from any or all of the requirements of this section. [2015 3rd sp.s. c 1 § 206; 2011 1st sp.s. c 43 § 710. Formerly RCW 43.41A.045.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.240 Evaluation of agency information technology spending and budget requests. (1) Pursuant to RCW 43.88.092(3), at the request of the director of financial management, the office shall evaluate both state agency information technology current spending and technology budget requests, including those proposed by the superintendent of public instruction, in conjunction with educational service districts, or statewide or regional providers of K-12 education information technology services. The office shall submit recommendations for funding all or part of such requests to the director of financial management. The office shall also submit recommendations regarding consolidation and coordination of similar proposals or other efficiencies it finds in reviewing proposals.

(2) The office shall establish criteria, consistent with portfolio-based information technology management, for the evaluation of agency budget requests under this section. Technology budget

requests shall be evaluated in the context of the state's information technology portfolio; technology initiatives underlying budget requests are subject to review by the office. Criteria shall include, but not be limited to: Feasibility of the proposed projects, consistency with the state strategic information technology plan and the state enterprise architecture, consistency with information technology portfolios, appropriate provision for public electronic access to information, evidence of business process streamlining and gathering of business and technical requirements, services, duration of investment, costs, and benefits. [2015 3rd sp.s. c 1 § 207; 2011 1st sp.s. c 43 § 711. Formerly RCW 43.41A.050.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.245 Planning, implementation, and evaluation of major projects—Standards and policies. (1) The office shall establish standards and policies governing the planning, implementation, and evaluation of major information technology projects, including those proposed by the superintendent of public instruction, in conjunction with educational service districts, or statewide or regional providers of K-12 education information technology services. The standards and policies shall:

(a) Establish criteria to identify projects which are subject to this section. Such criteria shall include, but not be limited to, significant anticipated cost, complexity, or statewide significance of the project; and

(b) Establish a model process and procedures which state agencies shall follow in developing and implementing projects within their information technology portfolios. This process may include project oversight experts or panels, as appropriate. State agencies may propose, for approval by the office, a process and procedures unique to the agency. The office may accept or require modification of such agency proposals or the office may reject those proposals and require use of the model process and procedures established under this subsection. Any process and procedures developed under this subsection shall require (i) distinct and identifiable phases upon which funding may be based, (ii) user validation of products through system demonstrations and testing of prototypes and deliverables, and (iii) other elements identified by the office.

The director may suspend or terminate a major project, and direct that the project funds be placed into unallotted reserve status, if the director determines that the project is not meeting or is not expected to meet anticipated performance standards.

(2) The office of financial management shall establish policies and standards consistent with portfolio-based information technology management to govern the funding of projects developed under this section. The policies and standards shall provide for:

(a) Funding of a project under terms and conditions mutually agreed to by the director, the director of financial management, and the head of the agency proposing the project. However, the office of financial management may require incremental funding of a project on a

phase-by-phase basis whereby funds for a given phase of a project may be released only when the office of financial management determines, with the advice of the director, that the previous phase is satisfactorily completed; and

(b) Other elements deemed necessary by the office of financial management. [2015 3rd sp.s. c 1 § 208; 2011 1st sp.s. c 43 § 712. Formerly RCW 43.41A.055.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.255 Major technology projects and services—Approval. (1) Prior to making a commitment to purchase, acquire, or develop a major information technology project or service, state agencies must provide a proposal to the office outlining the business case of the proposed product or service, including the up-front and ongoing cost of the proposal.

(2) Within thirty days of receipt of a proposal, the office shall approve the proposal, reject it, or propose modifications.

(3) In reviewing a proposal, the office must determine whether the product or service is consistent with:

(a) The standards and policies developed by the director pursuant to RCW 43.105.054; and

(b) The state's enterprise-based strategy.

(4) If a substantially similar product or service is offered by the agency, the director may require the state agency to procure the product or service through the agency, if doing so would benefit the state as an enterprise.

(5) The office shall provide guidance to state agencies as to what threshold of information technology spending constitutes a major information technology product or service under this section. [2015 3rd sp.s. c 1 § 209; 2011 1st sp.s. c 43 § 713. Formerly RCW 43.41A.060.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.265 Enterprise-based strategy for information technology—Use of ongoing enterprise architecture program. (1) The office shall develop an enterprise-based strategy for information technology in state government informed by portfolio management planning and information technology expenditure information collected from state agencies pursuant to RCW 43.88.092.

(2)(a) The office shall develop an ongoing enterprise architecture program for translating business vision and strategy into effective enterprise change. This program will create, communicate, and improve the key principles and models that describe the enterprise's future state and enable its evolution, in keeping with

the priorities of government and the information technology strategic plan.

(b) The enterprise architecture program will facilitate business process collaboration among agencies statewide; improving the reliability, interoperability, and sustainability of the business processes that state agencies use.

In developing an enterprise-based strategy for the state, the office is encouraged to consider the following strategies as possible opportunities for achieving greater efficiency:

(i) Developing evaluation criteria for deciding which common enterprise-wide business processes should become managed as enterprise services;

(ii) Developing a road map of priorities for creating enterprise services;

(iii) Developing decision criteria for determining implementation criteria for centralized or decentralized enterprise services;

(iv) Developing evaluation criteria for deciding which technology investments to continue, hold, or drop; and

(v) Performing such other duties as may be needed to promote effective enterprise change.

(c) The office will establish performance measurement criteria for each of its initiatives; will measure the success of those initiatives; and will assess its quarterly results with the director to determine whether to continue, revise, or disband the initiative. [2015 3rd sp.s. c 1 § 210; 2011 1st sp.s. c 43 § 714. Formerly RCW 43.41A.065.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.285 Technology services board—Created—Composition. (1) The technology services board is created within the agency.

(2) The board shall be composed of thirteen members. Six members shall be appointed by the governor, three of whom shall be representatives of state agencies or institutions, and three of whom shall be representatives of the private sector. Of the state agency representatives, at least one of the representatives must have direct experience using the software projects overseen by the board or reasonably expect to use the new software developed under the oversight of the board. Two members shall represent the house of representatives and shall be selected by the speaker of the house of representatives with one representative chosen from each major caucus of the house of representatives; two members shall represent the senate and shall be appointed by the president of the senate with one representative chosen from each major caucus of the senate. One member shall be the director who shall be a voting member of the board and serve as chair. Two nonvoting members with information technology expertise must be appointed by the governor as follows:

(a) One member representing state agency bargaining units shall be selected from a list of three names submitted by each of the general government exclusive bargaining representatives; and

(b) One member representing local governments shall be selected from a list of three names submitted by commonly recognized local government organizations.
The governor may reject all recommendations and request new recommendations.

(3) Of the initial members, three must be appointed for a one-year term, three must be appointed for a two-year term, and four must be appointed for a three-year term. Thereafter, members must be appointed for three-year terms.

(4) Vacancies shall be filled in the same manner that the original appointments were made for the remainder of the member's term.

(5) Members of the board shall be reimbursed for travel expenses as provided in RCW 43.03.050 and 43.03.060.

(6) The office shall provide staff support to the board. [2015 3rd sp.s. c 1 § 211; 2011 1st sp.s. c 43 § 715. Formerly RCW 43.41A.070.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.287 Technology services board—Powers and duties. The board shall have the following powers and duties related to information services:

(1) To review and approve standards and policies, developed by the office, governing the acquisition and disposition of equipment, proprietary software, and purchased services, licensing of the radio spectrum by or on behalf of state agencies, and confidentiality of computerized data;

(2) To review and approve statewide or interagency technical policies and standards developed by the office;

(3) To review, approve, and provide oversight of major information technology projects to ensure that no major information technology project proposed by a state agency is approved or authorized funding by the board without consideration of the technical and financial business case for the project, including a review of:

(a) The total cost of ownership across the life of the project;

(b) All major technical options and alternatives analyzed, and reviewed, if necessary, by independent technical sources; and

(c) Whether the project is technically and financially justifiable when compared against the state's enterprise-based strategy, long-term technology trends, and existing or potential partnerships with private providers or vendors;

(4) To review and approve standards and common specifications for new or expanded telecommunications networks proposed by state agencies, public postsecondary education institutions, educational service districts, or statewide or regional providers of K-12 information technology services, and to assure the cost-effective development and incremental implementation of a statewide video telecommunications system to serve: Public schools; educational service districts; vocational-technical institutes; community

colleges; colleges and universities; state and local government; and the general public through public affairs programming;

(5) To develop a policy to determine whether a proposed project, product, or service should undergo an independent technical and financial analysis prior to submitting a request to the office of financial management for the inclusion in any proposed operating, capital, or transportation budget;

(6) To approve contracting for services and activities under *RCW 41.06.142(7) for the agency. To approve any service or activity to be contracted under *RCW 41.06.142(7)(b), the board must also review the proposed business plan and recommendation submitted by the office;

(7) To consider, on an ongoing basis, ways to promote strategic investments in enterprise-level information technology projects that will result in service improvements and cost efficiency;

(8) To provide a forum to solicit external expertise and perspective on developments in information technology, enterprise architecture, standards, and policy development; and

(9) To provide a forum where ideas and issues related to information technology plans, policies, and standards can be reviewed. [2015 3rd sp.s. c 1 § 212; 2011 1st sp.s. c 43 § 716. Formerly RCW 43.41A.075.]

***Reviser's note:** RCW 41.06.142 was amended by 2020 c 269 § 2, changing subsection (7) to subsection (11).

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.291 Technology services board security subcommittee. (1) The technology services board security subcommittee is created within the board. The membership of the technology services board security subcommittee is comprised of a subset of members appointed to the board, as determined by the chair of the technology services board. The chair may make additional appointments to the technology services board security subcommittee to ensure that relevant technology sectors are represented.

(2) The technology services board security subcommittee has the following powers and duties related to cybersecurity:

(a) Review emergent cyberattacks and threats to critical infrastructure sectors in order to identify existing gaps in state agency cybersecurity policies;

(b) Assess emerging risks to state agency information technology;

(c) Recommend a reporting and information sharing system to notify state agencies of new risks, risk treatment opportunities, and projected shortfalls in response and recovery;

(d) Recommend tabletop cybersecurity exercises, including data breach simulation exercises;

(e) Assist the office of cybersecurity created in RCW 43.105.450 in developing cybersecurity best practice recommendations for state agencies;

(f) Review the proposed policies and standards developed by the office of cybersecurity and recommend their approval to the full board;

(g) Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies; and

(h) Assist the agency and the military department in creating the state of cybersecurity report required in subsection (6) of this section.

(3) In providing staff support to the board, the agency shall work with the national institute of standards and technology and other federal agencies, private sector businesses, and private cybersecurity experts and bring their perspectives and guidance to the board for consideration in fulfilling its duties to ensure a holistic approach to cybersecurity in state government.

(4) To discuss sensitive security topics and information, the technology services board security subcommittee may hold a portion of its agenda in executive session closed to the public.

(5) The technology services board security subcommittee must meet quarterly. The technology services board security subcommittee must hold a joint meeting once a year with the cybersecurity advisory committee created in RCW 38.52.040(4).

(6) By December 1, 2023, and each December 1st thereafter, the military department and the agency are jointly responsible for providing a state of cybersecurity report to the governor and the appropriate committees of the legislature, consistent with RCW 43.01.036, specifying recommendations considered necessary to address cybersecurity in the state. The technology services board security subcommittee shall coordinate the implementation of any recommendations contained in the state of cybersecurity report. The technology services board security subcommittee may identify as confidential, and not subject to public disclosure, those portions of the report as the technology services board security subcommittee deems necessary to protect the security of public and private cyber systems.

(7) In fulfilling its duties under this section, the agency and the technology services board security subcommittee shall collaborate with the military department and the cybersecurity advisory committee created in RCW 38.52.040(4).

(8) The reports produced and information compiled pursuant to this section are confidential and may not be disclosed under chapter 42.56 RCW. [2023 c 124 § 3.]

RCW 43.105.331 State interoperability executive committee—Composition—Responsibilities. (1) The director shall appoint a state interoperability executive committee, the membership of which must include, but not be limited to, representatives of the military department, the Washington state patrol, the department of transportation, the office of the state chief information officer, the department of natural resources, the department of fish and wildlife, the department of health, the department of corrections, city and county governments, state and local fire chiefs, police chiefs, and sheriffs, state and local emergency management directors, tribal nations, and public safety answering points, commonly known as 911 call centers. The chair and legislative members of the board will

serve as nonvoting ex officio members of the committee. Voting membership may not exceed twenty-two members.

(2) The director shall appoint the chair of the committee from among the voting members of the committee.

(3) The state interoperability executive committee has the following responsibilities:

(a) Develop policies and make recommendations to the office for technical standards for state wireless radio communications systems, including emergency communications systems. The standards must address, among other things, the interoperability of systems, taking into account both existing and future systems and technologies;

(b) Coordinate and manage on behalf of the office the licensing and use of state-designated and state-licensed radio frequencies, including the spectrum used for public safety and emergency communications, and serve as the point of contact with the federal communications commission and the first responders network authority on matters relating to allocation, use, and licensing of radio spectrum;

(c) Coordinate the purchasing of all state wireless radio communications system equipment to ensure that:

(i) Any new trunked radio system shall be, at a minimum, project-25; and

(ii) Any new land-mobile radio system that requires advanced digital features shall be, at a minimum, project-25;

(d) Seek support, including possible federal or other funding, for state-sponsored wireless communications systems;

(e) Develop recommendations for legislation that may be required to promote interoperability of state wireless communications systems;

(f) Foster cooperation and coordination among public safety and emergency response organizations;

(g) Work with wireless communications groups and associations to ensure interoperability among all public safety and emergency response wireless communications systems; and

(h) Perform such other duties as may be assigned by the director to promote interoperability of wireless communications systems.

(4) The office shall provide administrative support to the committee. [2017 c 92 § 1; 2015 3rd sp.s. c 1 § 213; 2011 1st sp.s. c 43 § 717. Formerly RCW 43.41A.080.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.341 Information technology portfolios. Information technology portfolios shall reflect (1) links among an agency's objectives, business plan, and technology; (2) analysis of the effect of an agency's proposed new technology investments on its existing infrastructure and business functions; and (3) analysis of the effect of proposed information technology investments on the state's information technology infrastructure. [1999 c 80 § 2. Formerly RCW 43.41A.110, 43.105.172.]

RCW 43.105.342 Consolidated technology services revolving account—Independent technical and financial analysis of proposed projects by the board. (1) The consolidated technology services revolving account is created in the custody of the state treasurer. All receipts from agency fees and charges for services collected from public agencies must be deposited into the account. The account must be used for the:

(a) Acquisition of equipment, software, supplies, and services; and

(b) Payment of salaries, wages, and other costs incidental to the acquisition, development, maintenance, operation, and administration of: (i) Information services; (ii) telecommunications; (iii) systems; (iv) software; (v) supplies; and (vi) equipment, including the payment of principal and interest on debt by the agency and other users as determined by the office of financial management.

(2) The director or the director's designee, with the approval of the technology services board, is authorized to expend up to one million dollars per fiscal biennium for the technology services board to conduct independent technical and financial analysis of proposed information technology projects.

(3) Only the director or the director's designee may authorize expenditures from the account. The account is subject to allotment procedures under chapter 43.88 RCW, but no appropriation is required for expenditures except as provided in subsection (4) of this section.

(4) Expenditures for the strategic planning and policy component of the agency are subject to appropriation. [2015 3rd sp.s. c 1 § 501.]

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

RCW 43.105.351 Electronic access to public records—Findings—Intent. Based upon the recommendations of the public information access policy task force, the legislature finds that government records and information are a vital resource to both government operations and to the public that government serves. Broad public access to state and local government records and information has potential for expanding citizen access to that information and for improving government services. Electronic methods for locating and transferring information can improve linkages between and among citizens, organizations, businesses, and governments. Information must be managed with great care to meet the objectives of citizens and their governments.

It is the intent of the legislature to encourage state and local governments to develop, store, and manage their public records and information in electronic formats to meet their missions and objectives. Further, it is the intent of the legislature for state and local governments to set priorities for making public records widely available electronically to the public. [1996 c 171 § 1. Formerly RCW 43.41A.115, 43.105.250.]

RCW 43.105.355 Electronic access to public records—Costs and fees. Funding to meet the costs of providing access, including the building of the necessary information systems, the digitizing of

information, developing the ability to mask nondisclosable information, and maintenance and upgrade of information access systems should come primarily from state and local appropriations, federal dollars, grants, private funds, cooperative ventures among governments, nonexclusive licensing, and public/private partnerships.

State agencies and local governments are encouraged to pool resources and to form cooperative ventures to provide electronic access to government records and information. State agencies are encouraged to seek federal and private grants for projects that provide increased efficiency and improve government delivery of information and services. [2015 3rd sp.s. c 1 § 217; 1996 c 171 § 12. Formerly RCW 43.41A.130, 43.105.280.]

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

Captions not law—Effective dates—1996 c 171: See notes following RCW 2.68.050.

RCW 43.105.359 Electronic access to public records—Government information locator service pilot project. The state library, with the assistance of the office and the state archives, shall establish a pilot project to design and test an electronic information locator system, allowing members of the public to locate and access electronic public records. In designing the system, the following factors shall be considered: (1) Ease of operation by citizens; (2) access through multiple technologies, such as direct dial and toll-free numbers, kiosks, and the internet; (3) compatibility with private online services; and (4) capability of expanding the electronic public records included in the system. The pilot project may restrict the type and quality of electronic public records that are included in the system to test the feasibility of making electronic public records and information widely available to the public. [2011 1st sp.s. c 43 § 724; 1996 c 171 § 13. Formerly RCW 43.41A.135, 43.105.290.]

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

Captions not law—Effective dates—1996 c 171: See notes following RCW 2.68.050.

RCW 43.105.365 Accuracy, integrity, and privacy of records and information. State agencies and local governments that collect and enter information concerning individuals into electronic records and information systems that will be widely accessible by the public under RCW 42.56.010 shall ensure the accuracy of this information to the extent possible. To the extent possible, information must be collected directly from, and with the consent of, the individual who is the subject of the data. State agencies shall establish procedures for correcting inaccurate information, including establishing mechanisms for individuals to review information about themselves and recommend changes in information they believe to be inaccurate. The inclusion of personal information in electronic public records that is widely available to the public should include information on the date when

the database was created or most recently updated. If personally identifiable information is included in electronic public records that are made widely available to the public, state agencies must follow retention and archival schedules in accordance with chapter 40.14 RCW, retaining personally identifiable information only as long as needed to carry out the purpose for which it was collected. At least once every five years, each agency that collects information must review the information collected and justify why it is being collected and for what purpose. [2015 3rd sp.s. c 1 § 218; 2011 c 60 § 39; 1996 c 171 § 15. Formerly RCW 43.41A.140, 43.105.310.]

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

Effective date—2011 c 60: See RCW 42.17A.919.

Captions not law—Effective dates—1996 c 171: See notes following RCW 2.68.050.

RCW 43.105.369 Office of privacy and data protection. (1) The office of privacy and data protection is created within the office of the state chief information officer. The purpose of the office of privacy and data protection is to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection.

(2) The director shall appoint the chief privacy officer, who is the director of the office of privacy and data protection.

(3) The primary duties of the office of privacy and data protection with respect to state agencies are:

(a) To conduct an annual privacy review;

(b) To conduct an annual privacy training for state agencies and employees;

(c) To articulate privacy principles and best practices;

(d) To coordinate data protection in cooperation with the agency; and

(e) To participate with the office of the state chief information officer in the review of major state agency projects involving personally identifiable information.

(4) The office of privacy and data protection must serve as a resource to local governments and the public on data privacy and protection concerns by:

(a) Developing and promoting the dissemination of best practices for the collection and storage of personally identifiable information, including establishing and conducting a training program or programs for local governments; and

(b) Educating consumers about the use of personally identifiable information on mobile and digital networks and measures that can help protect this information.

(5) By December 1, 2016, and every four years thereafter, the office of privacy and data protection must prepare and submit to the legislature a report evaluating its performance. The office of privacy and data protection must establish performance measures in its 2016 report to the legislature and, in each report thereafter, demonstrate the extent to which performance results have been achieved. These

performance measures must include, but are not limited to, the following:

(a) The number of state agencies and employees who have participated in the annual privacy training;

(b) A report on the extent of the office of privacy and data protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity;

(c) A report on the implementation of data protection measures by state agencies attributable in whole or in part to the office of privacy and data protection's coordination of efforts; and

(d) A report on consumer education efforts, including but not limited to the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the office of privacy and data protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.

(6) Within one year of June 9, 2016, the office of privacy and data protection must submit to the joint legislative audit and review committee for review and comment the performance measures developed under subsection (5) of this section and a data collection plan.

(7) The office of privacy and data protection shall submit a report to the legislature on the: (a) Extent to which telecommunications providers in the state are deploying advanced telecommunications capability; and (b) existence of any inequality in access to advanced telecommunications infrastructure experienced by residents of tribal lands, rural areas, and economically distressed communities. The report may be submitted at a time within the discretion of the office of privacy and data protection, at least once every four years, and only to the extent the office of privacy and data protection is able to gather and present the information within existing resources. [2016 c 195 § 2.]

Findings—2016 c 195: "The legislature finds that the rapid expansion of digital technology and mobile networks is changing how citizens access and share personal data and communications. Data privacy, data protection, and access equity are of increasing concern for all residents of the state. State agencies and programs entrusted by citizens with sensitive personal information must serve as responsible custodians of this data. The state can also play an important role in educating local governments and consumers about measures that may help them protect this information and as an advocate for access equity. In an interconnected world, citizens who lack meaningful access to digital technology, including mobile networks and high-speed internet connections, lack the necessary tools for sharing in the state's technology, innovation, and economic development successes. For the forgoing reasons, the legislature finds that it is necessary and efficient to have a central point of contact for policy matters involving data privacy, data protection, and access equity." [2016 c 195 § 1.]

RCW 43.105.375 Use of state data center or commercial cloud computing services—Exceptions. (1) Except as provided by subsection (2) of this section, state agencies shall locate all existing and new information or telecommunications investments in the state data center or within third-party, commercial cloud computing services.

(2) State agencies with a service requirement that precludes them from complying with subsection (1) of this section must receive a waiver from the office. Waivers must be based upon written justification from the requesting state agency citing specific service or performance requirements for locating servers outside the state's common platform.

(3) The legislature and the judiciary, which are constitutionally recognized as separate branches of government, may enter into an interagency agreement with the office to migrate its servers into the state data center or third-party, commercial cloud computing services.

(5) [(4)] This section does not apply to institutions of higher education. [2021 c 40 § 3; 2015 3rd sp.s. c 1 § 219; 2011 1st sp.s. c 43 § 735. Formerly RCW 43.41A.150.]

Findings—Intent—2021 c 40: "(1) The legislature finds that the advent of the COVID-19 pandemic has increased the needs of the people of Washington for state services. From unemployment benefits to information on the incidence of disease in the state, Washingtonians have increasingly turned to state government for vital services and information.

(2) The legislature further finds that the state's information technology infrastructure is outdated and with insufficient capacity to handle the increased demand and has, in many cases, not been adequate to enable the state to provide the needed services effectively and efficiently.

(3) Therefore, the legislature intends to migrate the state's information technology toward cloud services, which will deliver the capacity, security, resiliency, disaster recovery capability, and data analytics necessary to allow the state to provide Washingtonians the services they require during this pandemic and in the future." [2021 c 40 § 1.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.385 Agency as central service provider for state agencies. (1) The office shall conduct a needs assessment and develop a migration strategy to ensure that, over time, all state agencies are moving towards using the agency as their central service provider for all utility-based infrastructure services, including centralized PC and infrastructure support. State agency-specific application services shall remain managed within individual agencies.

(2) The office shall develop short-term and long-term objectives as part of the migration strategy.

(3) This section does not apply to institutions of higher education. [2015 3rd sp.s. c 1 § 220; 2011 1st sp.s. c 43 § 736. Formerly RCW 43.41A.152.]

Effective date—2015 3rd sp.s. c 1 §§ 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.

RCW 43.105.450 Office of cybersecurity—State chief information security officer—State agency information technology security. (1) The office of cybersecurity is created within the office of the chief information officer.

(2) The director shall appoint a state chief information security officer, who is the director of the office of cybersecurity.

(3) The primary duties of the office of cybersecurity are:

(a) To establish security standards and policies to protect the state's information technology systems and infrastructure, to provide appropriate governance and application of the standards and policies across information technology resources used by the state, and to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure;

(b) To develop a centralized cybersecurity protocol for protecting and managing state information technology assets and infrastructure;

(c) To detect and respond to security incidents consistent with information security standards and policies;

(d) To create a model incident response plan for agency adoption, with the office of cybersecurity as the incident response coordinator for incidents that: (i) Impact multiple agencies; (ii) impact more than 10,000 citizens; (iii) involve a nation state actor; or (iv) are likely to be in the public domain;

(e) To ensure the continuity of state business and information resources that support the operations and assets of state agencies in the event of a security incident;

(f) To provide formal guidance to agencies on leading practices and applicable standards to ensure a whole government approach to cybersecurity, which shall include, but not be limited to, guidance regarding: (i) The configuration and architecture of agencies' information technology systems, infrastructure, and assets; (ii) governance, compliance, and oversight; and (iii) incident investigation and response;

(g) To serve as a resource for local and municipal governments in Washington in the area of cybersecurity;

(h) To develop a service catalog of cybersecurity services to be offered to state and local governments;

(i) To collaborate with state agencies in developing standards, functions, and services in order to ensure state agency regulatory environments are understood and considered as part of an enterprise cybersecurity response;

(j) To define core services that must be managed by agency information technology security programs; and

(k) To perform all other matters and things necessary to carry out the purposes of this chapter.

(4) In performing its duties, the office of cybersecurity must address the highest levels of security required to protect confidential information transacted, stored, or processed in the state's information technology systems and infrastructure that is specifically protected from disclosure by state or federal law and for which strict handling requirements are required.

(5) In executing its duties under subsection (3) of this section, the office of cybersecurity shall use or rely upon existing, industry standard, widely adopted cybersecurity standards, with a preference for United States federal standards.

(6) Each state agency, institution of higher education, the legislature, and the judiciary must develop an information technology security program consistent with the office of cybersecurity's standards and policies.

(7)(a) Each state agency information technology security program must adhere to the office of cybersecurity's security standards and policies. Each state agency must review and update its program annually, certify to the office of cybersecurity that its program is in compliance with the office of cybersecurity's security standards and policies, and provide the office of cybersecurity with a list of the agency's cybersecurity business needs and agency program metrics.

(b) The office of cybersecurity shall require a state agency to obtain an independent compliance audit of its information technology security program and controls at least once every three years to determine whether the state agency's information technology security program is in compliance with the standards and policies established by the agency and that security controls identified by the state agency in its security program are operating efficiently.

(c) If a review or an audit conducted under (a) or (b) of this subsection identifies any failure to comply with the standards and policies of the office of cybersecurity or any other material cybersecurity risk, the office of cybersecurity must require the state agency to formulate and implement a plan to resolve the failure or risk. On an annual basis, the office of cybersecurity must provide a confidential report to the governor and appropriate committees of the legislature identifying and describing the cybersecurity risk or failure to comply with the office of cybersecurity's security policy or implementing cybersecurity standards and policies, as well as the agency's plan to resolve such failure or risk. Risks that are not mitigated are to be tracked by the office of cybersecurity and reviewed with the governor and the chair and ranking member of the appropriate committees of the legislature on a quarterly basis.

(d) The reports produced, and information compiled, pursuant to this subsection (7) are confidential and may not be disclosed under chapter 42.56 RCW.

(8) In the case of institutions of higher education, the judiciary, and the legislature, each information technology security program must be comparable to the intended outcomes of the office of cybersecurity's security standards and policies. [2021 c 291 § 1.]

RCW 43.105.460 Office of cybersecurity—Catalog of services and functions—Report. (1) By July 1, 2022, the office of cybersecurity, in collaboration with state agencies, shall develop a catalog of cybersecurity services and functions for the office of cybersecurity to perform and submit a report to the legislature and governor. The report must include, but not be limited to:

(a) Cybersecurity services and functions to include in the office of cybersecurity's catalog of services that should be performed by the office of cybersecurity;

(b) Core capabilities and competencies of the office of cybersecurity;

(c) Security functions which should remain within agency information technology security programs;

(d) A recommended model for accountability of agency security programs to the office of cybersecurity; and

(e) The cybersecurity services and functions required to protect confidential information transacted, stored, or processed in the state's information technology systems and infrastructure that is specifically protected from disclosure by state or federal law and for which strict handling requirements are required.

(2) The office of cybersecurity shall update and publish its catalog of services and performance metrics on a biennial basis. The office of cybersecurity shall use data and information provided from agency security programs to inform the updates to its catalog of services and performance metrics.

(3) To ensure alignment with enterprise information technology security strategy, the office of cybersecurity shall develop a process for reviewing and evaluating agency proposals for additional cybersecurity services consistent with RCW 43.105.255. [2021 c 291 § 2.]

RCW 43.105.470 Office of cybersecurity—Major cybersecurity incidents—Reporting duties. (1) In the event of a major cybersecurity incident, as defined in policy established by the office of cybersecurity in accordance with RCW 43.105.450, state agencies must report that incident to the office of cybersecurity within 24 hours of discovery of the incident.

(2) State agencies must provide the office of cybersecurity with contact information for any external parties who may have material information related to the cybersecurity incident.

(3) Once a cybersecurity incident is reported to the office of cybersecurity, the office of cybersecurity must investigate the incident to determine the degree of severity and facilitate any necessary incident response measures that need to be taken to protect the enterprise.

(4) The chief information security officer or the chief information security officer's designee shall serve as the state's point of contact for all major cybersecurity incidents.

(5) The office of cybersecurity must create policy to implement this section. [2021 c 291 § 3.]

RCW 43.105.825 K-20 network—Oversight—Coordination of telecommunications planning. (1) In overseeing the technical aspects of the K-20 network, the board is not intended to duplicate the statutory responsibilities of the student achievement council, the superintendent of public instruction, the board, the state librarian, or the governing boards of the institutions of higher education.

(2) The board may not interfere in any curriculum or legally offered programming offered over the network.

(3) The responsibility to review and approve standards and common specifications for the network remains the responsibility of the board.

(4) The coordination of telecommunications planning for the common schools remains the responsibility of the superintendent of public instruction. The board may recommend, but not require,

revisions to the superintendent's telecommunications plans. [2015 3rd sp.s. c 1 § 106; 2012 c 229 § 588; 2004 c 275 § 62; 1999 c 285 § 7.]

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

Effective date—2012 c 229 §§ 101, 117, 401, 402, 501 through 594, 601 through 609, 701 through 708, 801 through 821, 902, and 904: See note following RCW 28B.77.005.

Part headings not law—2004 c 275: See note following RCW 28B.76.090.

RCW 43.105.904 Actions of telecommunications oversight and policy committee—Savings—1999 c 285. Actions of the telecommunications oversight and policy committee in effect on June 30, 1999, shall remain in effect thereafter unless modified or repealed by the *K-20 board. [1999 c 285 § 4.]

***Reviser's note:** RCW 43.105.800, which created the K-20 board, was repealed by 2010 1st sp.s. c 7 § 63.

RCW 43.105.905 Construction—2008 c 262. Nothing in this act may be construed as giving the *department of information services or any other entities any additional authority, regulatory or otherwise, over providers of telecommunications and information technology. [2008 c 262 § 4.]

***Reviser's note:** The "department of information services" was renamed the "consolidated technology services agency" by 2011 1st sp.s. c 43 § 803.

Findings—Intent—2008 c 262: "(1) The legislature finds and declares the following:

(a) The deployment and adoption of high-speed internet services and information technology has resulted in enhanced economic development and public safety for the state's communities, improved health care and educational opportunities, and a better quality of life for the state's residents;

(b) Continued progress in the deployment and adoption of high-speed internet services and other advanced telecommunications services, both land-based and wireless, is vital to ensuring Washington remains competitive and continues to create business and job growth; and

(c) That the state must encourage and support strategic partnerships of public, private, nonprofit, and community-based sectors in the continued growth and development of high-speed internet services and information technology for state residents and businesses.

(2) Therefore, in order to begin advancing the state towards further growth and development of high-speed internet in the state, and to ensure a better quality of life for all state residents, it is the legislature's intent to conduct a statewide needs assessment of broadband internet resources through an open dialogue with all interested parties, including providers, unions, businesses, community

organizations, local governments, and state agencies. The legislature intends to use this needs assessment in guiding future plans on how to ensure that every resident in Washington state may gain access to high-speed internet services and, as part of this effort, to address digital literacy and technology training needs of low-income and technology underserved residents of the state through state support of community technology programs." [2008 c 262 § 1.]

RCW 43.105.906 Conflict with federal requirements—2009 c 509. If any part of this act is found to be in conflict with federal requirements that are a prescribed condition to the allocation of federal funds to the state, the conflicting part of this act is inoperative solely to the extent of the conflict and with respect to the agencies directly affected, and this finding does not affect the operation of the remainder of this act in its application to the agencies concerned. Rules adopted under this act must meet federal requirements that are a necessary condition to the receipt of federal funds by the state. [2009 c 509 § 11.]

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

RCW 43.105.907 Transfer of certain powers, duties, and functions of the department of information services. (1) Those powers, duties, and functions of the department of information services being transferred to the consolidated technology services agency as set forth in *sections 801 through 816, chapter 43, Laws of 2011 1st sp. sess. are hereby transferred to the consolidated technology services agency.

(2)(a) All reports, documents, surveys, books, records, files, papers, or written material in the possession of the department of information services shall be delivered to the custody of the consolidated technology services agency. All cabinets, furniture, office equipment, motor vehicles, and other tangible property employed by the department of information services shall be made available to the consolidated technology services agency. All funds, credits, or other assets held by the department of information services shall be assigned to the consolidated technology services agency.

(b) Any appropriations made to the department of information services shall, on October 1, 2011, be transferred and credited to the consolidated technology services agency.

(c) If any question arises as to the transfer of any personnel, funds, books, documents, records, papers, files, equipment, or other tangible property used or held in the exercise of the powers and the performance of the duties and functions transferred, the director of financial management shall make a determination as to the proper allocation and certify the same to the state agencies concerned.

(3) All rules and all pending business before the department of information services pertaining to the powers, duties, and functions transferred shall be continued and acted upon by the consolidated technology services agency. All existing contracts and obligations shall remain in full force and shall be performed by the consolidated technology services agency.

(4) The transfer of the powers, duties, functions, and personnel of the department of information services shall not affect the validity of any act performed before October 1, 2011.

(5) If apportionments of budgeted funds are required because of the transfers directed by this section, the director of financial management shall certify the apportionments to the agencies affected, the state auditor, and the state treasurer. Each of these shall make the appropriate transfer and adjustments in funds and appropriation accounts and equipment records in accordance with the certification.

(6) All employees of the department of information services engaged in performing the powers, functions, and duties transferred to the consolidated technology services agency are transferred to the consolidated technology services agency. All employees classified under chapter 41.06 RCW, the state civil service law, are assigned to the consolidated technology services agency to perform their usual duties upon the same terms as formerly, without any loss of rights, subject to any action that may be appropriate thereafter in accordance with the laws and rules governing state civil service law.

(7) Unless or until modified by the public employment relations commission pursuant to RCW 41.80.911:

(a) The portions of the bargaining units of employees at the department of information services existing on October 1, 2011, shall be considered appropriate units at the consolidated technology services agency and will be so certified by the public employment relations commission.

(b) The exclusive bargaining representatives recognized as representing the portions of the bargaining units of employees at the department of information services existing on October 1, 2011, shall continue as the exclusive bargaining representatives of the transferred bargaining units without the necessity of an election. [2011 1st sp.s. c 43 § 1009. Formerly RCW 43.41A.900.]

***Reviser's note:** Sections 815 and 816, chapter 43, Laws of 2011 1st sp. sess. were vetoed.

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