S-0898.1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SENATE BILL 5455**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State of Washington 65th Legislature 2017 Regular Session**

**By** Senators Miloscia, Zeiger, and Pearson

AN ACT Relating to enhancing statewide cybersecurity performance through information assessment; amending RCW 43.105.020, 43.105.052, 43.105.111, and 43.105.220; adding a new section to chapter 43.105 RCW; and creating a new section.

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

NEW SECTION. **Sec.**  The legislature intends to develop world-class cybersecurity performance management and assessment systems that can be duplicated in other states. The legislature finds that this is best accomplished through coordination of a series of performance assessments by independent examiners and enhanced executive branch communication with the legislature regarding cybersecurity infrastructure, performance, and posture.

**Sec.**  RCW 43.105.020 and 2016 c 237 s 2 are each amended to read as follows:

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

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

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

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

(4) "Cybersecurity excellence assessment" means an assessment of enterprise cybersecurity operational performance using a framework approved by the national institutes of standards and technology, United States department of commerce.

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

((~~(5)~~)) (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.

((~~(6)~~)) (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.

((~~(7)~~)) (8) "Information" includes, but is not limited to, data, text, voice, and video.

((~~(8)~~)) (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.

((~~(9)~~)) (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.

((~~(10)~~)) (11) "Information technology portfolio" or "portfolio" means a strategic management process documenting relationships between agency missions and information technology and telecommunications investments.

((~~(11)~~)) (12) "K‑20 network" means the network established in RCW 43.41.391.

((~~(12)~~)) (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.

((~~(13)~~)) (14) "Office" means the office of the state chief information officer within the consolidated technology services agency.

((~~(14)~~)) (15) "Oversight" means a process of comprehensive risk analysis and management designed to ensure optimum use of information technology resources and telecommunications.

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

((~~(16)~~)) (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.

((~~(17)~~)) (18) "Public benefit nonprofit corporation" means a public benefit nonprofit corporation as defined in RCW 24.03.005 that is receiving local, state, or federal funds either directly or through a public agency other than an Indian tribe or political subdivision of another state.

((~~(18)~~)) (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.

((~~(19)~~)) (20) "Security incident" means an accidental or deliberative event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources.

((~~(20)~~)) (21) "State agency" means every state office, department, division, bureau, board, commission, or other state agency, including offices headed by a statewide elected official.

((~~(21)~~)) (22) "Telecommunications" includes, but is not limited to, wireless or wired systems for transport of voice, video, and data communications, network systems, requisite facilities, equipment, system controls, simulation, electronic commerce, and all related interactions between people and machines.

((~~(22)~~)) (23) "Utility-based infrastructure services" includes personal computer and portable device support, servers and server administration, security administration, network administration, telephony, email, and other information technology services commonly used by state agencies.

**Sec.**  RCW 43.105.052 and 2015 3rd sp.s. c 1 s 104 are each amended to read as follows:

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) Develop procedures for providing information about the state's cybersecurity infrastructure, performance, and posture with members of the state legislature to enable them to effectively perform their constitutional duties;

(7) 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)~~)) (8) Perform all other matters and things necessary to carry out the purposes and provisions of this chapter.

**Sec.**  RCW 43.105.111 and 2015 3rd sp.s. c 1 s 105 are each amended to read as follows:

The director shall set one-year and five-year performance ((~~targets~~)) projections and approve plans for achieving those measurable and specific ((~~goals~~)) projections for the agency. By January 2017, the appropriate organizational performance and accountability measures and performance ((~~targets~~)) projections shall be submitted to the governor. These measures and ((~~targets~~)) projections 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 web site.

The director shall report to the governor on agency performance at least quarterly and to the appropriate legislative committees on agency performance at least annually. The reports shall be included on the agency's web site and accessible to the public.

**Sec.**  RCW 43.105.220 and 2015 3rd sp.s. c 1 s 203 are each amended to read as follows:

(1) The office shall prepare a state strategic information technology plan which shall establish a statewide mission, ((~~goals~~)) one-year and five-year projections, and objectives for the use of information technology, including ((~~goals~~)) projections 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~~)) projections 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.

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

(1) The consolidated technology services agency must:

(a) Enter into a partnership with the national institutes of standards and technology, United States department of commerce to coordinate and schedule cybersecurity excellence assessments of the agency's operations every two years.

(b) Transmit completed cybersecurity excellence assessments and feedback reports to pertinent legislative committees and the office of the governor.

(2) The consolidated technology services agency's goal is to progress toward achieving world-class performance by achieving a sixty percent score within seven years of its first cybersecurity excellence assessment. When it achieves a sixty percent score, it shall apply for an award from the national institutes of standards and technology, United States department of commerce for its performance.

(3) If the consolidated technology services agency meets the goal in subsection (2) of this section, it is not required to conduct a cybersecurity excellence assessment every two years, but must conduct an excellence assessment every four years.

**--- END ---**