S-3441.1

# SENATE BILL 5834

**State of Washington 67th Legislature 2022 Regular Session**

**By** Senators Carlyle, Frockt, Nguyen, and Stanford

Read first time 01/12/22. Referred to Committee on Environment, Energy & Technology.

AN ACT Relating to implementing enterprise-wide technology policies in state government to ensure consistency, security, and responsible use of data; amending RCW 43.105.054 and 43.105.369; and creating a new section.

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

NEW SECTION. **Sec. 1.** (1) The legislature finds that Washington state values the highest level of quality for the use of technology to improve services for the public, provide for accessibility and cost savings, and meet the public's needs. This includes the smart use of the cloud technology, applications, and mobile technology and the like that meet the highest standards of quality. The high quality use of technology requires rigorously following evidence-based best practices, supporting the state workforce with continuous learning, and responsibly managing the public's data, privacy, and security.

(2) The legislature further finds that statewide data privacy and security policies have been in effect as recommendations for years, but the implementation of these policies has been sporadic, uncoordinated, and inconsistent. State agencies operate under a highly decentralized model and must design, develop, and implement their own programs in isolation and silos from others.

(3) Voluntary compliance with these policies has shown to be insufficient. It is now important to require a more coordinated, standardized approach. Therefore, the legislature intends to elevate the quality of the state's use of technology by ensuring enterprise-level best practices, standards, and policies and to emphasize the expectation that agencies will be more rigorous about adopting and implementing such best practices, standards, and policies.

**Sec. 2.** RCW 43.105.054 and 2021 c 291 s 9 are each amended to read as follows:

(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; and

(v) Privacy, in coordination with the office of privacy and data protection;

(f) To coordinate with state agencies with an annual information technology expenditure that exceeds ((~~ten million dollars~~)) $10,000,000 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.

**Sec. 3.** RCW 43.105.369 and 2016 c 195 s 2 are each amended to read as follows:

(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 and establish 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.

(8)(a) By July 31, 2022, the office of privacy and data protection must establish privacy principles and best practices. The privacy principles and best practices may be updated as needed.

(b) Beginning July 1, 2023, except as provided in (c) of this subsection, each state agency must adopt the privacy principles and best practices established by the office of privacy and data protection pursuant to subsection (3)(c) of this section through its privacy policies and procedures. Each state agency must review the policies and procedures annually to ensure they are current with the privacy principles and best practices established by the office of privacy and data protection.

(c) A state agency with a requirement that precludes it from complying with (b) of this subsection must receive a waiver from the office of privacy and data protection. Waivers must be based upon written justification from the requesting state agency citing specific service or performance requirements for needing a waiver, including an estimate of how much additional time is needed and what specific resources would assist the state agency in complying.

(d) The office of privacy and data protection must assist state agencies in meeting the requirements of this subsection.

(e) This subsection does not apply to institutions of higher education.

**--- END ---**