
SENATE BILL 5834

State of Washington

67th Legislature

2022 Regular Session

By Senator Carlyle

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

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

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

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

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

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

10 (1) The director shall establish standards and policies to govern
11 information technology in the state of Washington.

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

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

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

17 (ii) Disposition of equipment;

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

20 (iv) Confidentiality of computerized data;

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

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

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

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

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

36 (ii) Training and education;

37 (iii) Project management; (~~and~~)

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

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

3 (f) To coordinate with state agencies with an annual information
4 technology expenditure that exceeds (~~ten million dollars~~)
5 \$10,000,000 to implement a technology business management program to
6 identify opportunities for savings and efficiencies in information
7 technology expenditures and to monitor ongoing financial performance
8 of technology investments;

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

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

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

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

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

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

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

37 In developing these standards, the office is encouraged to
38 include the state library, state archives, and appropriate
39 representatives of state and local government.

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

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

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

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

12 (a) To conduct an annual privacy review;

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

15 (c) To articulate and establish privacy principles and best
16 practices;

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

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

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

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

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

32 (5) By December 1, 2016, and every four years thereafter, the
33 office of privacy and data protection must prepare and submit to the
34 legislature a report evaluating its performance. The office of
35 privacy and data protection must establish performance measures in
36 its 2016 report to the legislature and, in each report thereafter,
37 demonstrate the extent to which performance results have been
38 achieved. These performance measures must include, but are not
39 limited to, the following:

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

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

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

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

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

19 (7) The office of privacy and data protection shall submit a
20 report to the legislature on the: (a) Extent to which
21 telecommunications providers in the state are deploying advanced
22 telecommunications capability; and (b) existence of any inequality in
23 access to advanced telecommunications infrastructure experienced by
24 residents of tribal lands, rural areas, and economically distressed
25 communities. The report may be submitted at a time within the
26 discretion of the office of privacy and data protection, at least
27 once every four years, and only to the extent the office of privacy
28 and data protection is able to gather and present the information
29 within existing resources.

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

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

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

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

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

--- END ---