

---

**SENATE BILL 5957**

---

**State of Washington**

**68th Legislature**

**2024 Regular Session**

**By** Senators Boehnke, Dhingra, Dozier, Hasegawa, Liiias, Short, and Warnick

Prefiled 01/03/24. Read first time 01/08/24. Referred to Committee on Environment, Energy & Technology.

1 AN ACT Relating to requiring the office of privacy and data  
2 protection to develop guidelines for the use of artificial  
3 intelligence; and amending RCW 43.105.020 and 43.105.369.

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

5 **Sec. 1.** RCW 43.105.020 and 2023 c 124 s 1 are each amended to  
6 read as follows:

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

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

10 (2) "Artificial intelligence" means:

11 (a) A branch of computer science devoted to developing data  
12 processing systems that performs functions normally associated with  
13 human intelligence, such as reasoning, learning, and self-  
14 improvement; or

15 (b) The capability of a device to perform functions that are  
16 normally associated with human intelligence such as reasoning,  
17 learning, and self-improvement.

18 (3) "Board" means the technology services board.

19 ~~((3))~~ (4) "Cloud computing" has the same meaning as provided by  
20 the special publication 800-145 issued by the national institute of

1 standards and technology of the United States department of commerce  
2 as of September 2011 or its successor publications.

3 ~~((4))~~ (5) "Customer agencies" means all entities that purchase  
4 or use information technology resources, telecommunications, or  
5 services from the consolidated technology services agency.

6 ~~((5))~~ (6) "Director" means the state chief information officer,  
7 who is the director of the consolidated technology services agency.

8 ~~((6))~~ (7) "Enterprise architecture" means an ongoing activity  
9 for translating business vision and strategy into effective  
10 enterprise change. It is a continuous activity. Enterprise  
11 architecture creates, communicates, and improves the key principles  
12 and models that describe the enterprise's future state and enable its  
13 evolution.

14 ~~((7))~~ (8) "Equipment" means the machines, devices, and  
15 transmission facilities used in information processing, including but  
16 not limited to computers, terminals, telephones, wireless  
17 communications system facilities, cables, and any physical facility  
18 necessary for the operation of such equipment.

19 ~~((8))~~ (9) "Information" includes, but is not limited to, data,  
20 text, voice, and video.

21 ~~((9))~~ (10) "Information security" means the protection of  
22 communication and information resources from unauthorized access,  
23 use, disclosure, disruption, modification, or destruction in order  
24 to:

25 (a) Prevent improper information modification or destruction;

26 (b) Preserve authorized restrictions on information access and  
27 disclosure;

28 (c) Ensure timely and reliable access to and use of information;  
29 and

30 (d) Maintain the confidentiality, integrity, and availability of  
31 information.

32 ~~((10))~~ (11) "Information technology" includes, but is not  
33 limited to, all electronic technology systems and services, automated  
34 information handling, system design and analysis, conversion of data,  
35 computer programming, information storage and retrieval,  
36 telecommunications, requisite system controls, simulation, electronic  
37 commerce, radio technologies, and all related interactions between  
38 people and machines.

39 ~~((11))~~ (12) "Information technology portfolio" or "portfolio"  
40 means a strategic management process documenting relationships

1 between agency missions and information technology and  
2 telecommunications investments.

3 ~~((12))~~ (13) "K-20 network" means the network established in RCW  
4 43.41.391.

5 ~~((13))~~ (14) "Local governments" includes all municipal and  
6 quasi-municipal corporations and political subdivisions, and all  
7 agencies of such corporations and subdivisions authorized to contract  
8 separately.

9 ~~((14))~~ (15) "Office" means the office of the state chief  
10 information officer within the consolidated technology services  
11 agency.

12 ~~((15))~~ (16) "Oversight" means a process of comprehensive risk  
13 analysis and management designed to ensure optimum use of information  
14 technology resources and telecommunications.

15 ~~((16))~~ (17) "Proprietary software" means that software offered  
16 for sale or license.

17 ~~((17))~~ (18) "Public agency" means any agency of this state or  
18 another state; any political subdivision or unit of local government  
19 of this state or another state including, but not limited to,  
20 municipal corporations, quasi-municipal corporations, special purpose  
21 districts, and local service districts; any public benefit nonprofit  
22 corporation; any agency of the United States; and any Indian tribe  
23 recognized as such by the federal government.

24 ~~((18))~~ (19) "Public benefit nonprofit corporation" means a  
25 public benefit nonprofit corporation as defined in RCW 24.03A.245  
26 that is receiving local, state, or federal funds either directly or  
27 through a public agency other than an Indian tribe or political  
28 subdivision of another state.

29 ~~((19))~~ (20) "Public record" has the definitions in RCW  
30 42.56.010 and chapter 40.14 RCW and includes legislative records and  
31 court records that are available for public inspection.

32 ~~((20))~~ (21) "Public safety" refers to any entity or services  
33 that ensure the welfare and protection of the public.

34 ~~((21))~~ (22) "Ransomware" means a type of malware that attempts  
35 to deny a user or organization access to data or systems, usually  
36 through encryption, until a sum of money or other currency is paid or  
37 the user or organization is forced to take a specific action.

38 ~~((22))~~ (23) "Security incident" means an accidental or  
39 deliberative event that results in or constitutes an imminent threat  
40 of the unauthorized access, loss, disclosure, modification,

1 disruption, or destruction of communication and information  
2 resources.

3 ~~((23))~~ (24) "State agency" means every state office,  
4 department, division, bureau, board, commission, or other state  
5 agency, including offices headed by a statewide elected official.

6 ~~((24))~~ (25) "Telecommunications" includes, but is not limited  
7 to, wireless or wired systems for transport of voice, video, and data  
8 communications, network systems, requisite facilities, equipment,  
9 system controls, simulation, electronic commerce, and all related  
10 interactions between people and machines.

11 ~~((25))~~ (26) "Utility-based infrastructure services" includes  
12 personal computer and portable device support, servers and server  
13 administration, security administration, network administration,  
14 telephony, email, and other information technology services commonly  
15 used by state agencies.

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

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

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

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

27 (a) To conduct an annual privacy review;

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

30 (c) To articulate privacy principles and best practices;

31 (d) To develop guidelines for the use of artificial intelligence  
32 to ensure the ethical, transparent, accountable, and responsible  
33 implementation of the technology, and protection of personally  
34 identifiable information;

35 (e) To coordinate data protection in cooperation with the agency;  
36 and

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

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

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

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

11 (5) By December 1, 2016, and every four years thereafter, the  
12 office of privacy and data protection must prepare and submit to the  
13 legislature a report evaluating its performance. The office of  
14 privacy and data protection must establish performance measures in  
15 its 2016 report to the legislature and, in each report thereafter,  
16 demonstrate the extent to which performance results have been  
17 achieved. These performance measures must include, but are not  
18 limited to, the following:

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

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

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

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

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

37 (7) The office of privacy and data protection shall submit a  
38 report to the legislature on the: (a) Extent to which  
39 telecommunications providers in the state are deploying advanced  
40 telecommunications capability; and (b) existence of any inequality in

1 access to advanced telecommunications infrastructure experienced by  
2 residents of tribal lands, rural areas, and economically distressed  
3 communities. The report may be submitted at a time within the  
4 discretion of the office of privacy and data protection, at least  
5 once every four years, and only to the extent the office of privacy  
6 and data protection is able to gather and present the information  
7 within existing resources.

--- END ---