
SECOND SUBSTITUTE SENATE BILL 5518

State of Washington

68th Legislature

2023 Regular Session

By Senate Ways & Means (originally sponsored by Senators Boehnke, Stanford, MacEwen, Muzzall, Fortunato, Frame, Kuderer, Valdez, Warnick, and Wellman)

READ FIRST TIME 02/24/23.

1 AN ACT Relating to cybersecurity; amending RCW 43.21F.045;
2 reenacting and amending RCW 43.105.020 and 38.52.040; adding a new
3 section to chapter 43.105 RCW; and adding a new section to chapter
4 42.56 RCW.

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

6 **Sec. 1.** RCW 43.105.020 and 2021 c 176 s 5223 and 2021 c 40 s 2
7 are each reenacted and amended to read as follows:

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

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

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

12 (3) "Cloud computing" has the same meaning as provided by the
13 special publication 800-145 issued by the national institute of
14 standards and technology of the United States department of commerce
15 as of September 2011 or its successor publications.

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

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

1 (6) "Enterprise architecture" means an ongoing activity for
2 translating business vision and strategy into effective enterprise
3 change. It is a continuous activity. Enterprise architecture creates,
4 communicates, and improves the key principles and models that
5 describe the enterprise's future state and enable its evolution.

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

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

13 (9) "Information security" means the protection of communication
14 and information resources from unauthorized access, use, disclosure,
15 disruption, modification, or destruction in order to:

16 (a) Prevent improper information modification or destruction;

17 (b) Preserve authorized restrictions on information access and
18 disclosure;

19 (c) Ensure timely and reliable access to and use of information;
20 and

21 (d) Maintain the confidentiality, integrity, and availability of
22 information.

23 (10) "Information technology" includes, but is not limited to,
24 all electronic technology systems and services, automated information
25 handling, system design and analysis, conversion of data, computer
26 programming, information storage and retrieval, telecommunications,
27 requisite system controls, simulation, electronic commerce, radio
28 technologies, and all related interactions between people and
29 machines.

30 (11) "Information technology portfolio" or "portfolio" means a
31 strategic management process documenting relationships between agency
32 missions and information technology and telecommunications
33 investments.

34 (12) "K-20 network" means the network established in RCW
35 43.41.391.

36 (13) "Local governments" includes all municipal and quasi-
37 municipal corporations and political subdivisions, and all agencies
38 of such corporations and subdivisions authorized to contract
39 separately.

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

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

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

8 (17) "Public agency" means any agency of this state or another
9 state; any political subdivision or unit of local government of this
10 state or another state including, but not limited to, municipal
11 corporations, quasi-municipal corporations, special purpose
12 districts, and local service districts; any public benefit nonprofit
13 corporation; any agency of the United States; and any Indian tribe
14 recognized as such by the federal government.

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

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

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

25 (21) "Ransomware" means a type of malware that attempts to deny a
26 user or organization access to data or systems, usually through
27 encryption, until a sum of money or other currency is paid or the
28 user or organization is forced to take a specific action.

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

33 ~~((22))~~ (23) "State agency" means every state office,
34 department, division, bureau, board, commission, or other state
35 agency, including offices headed by a statewide elected official.

36 ~~((23))~~ (24) "Telecommunications" includes, but is not limited
37 to, wireless or wired systems for transport of voice, video, and data
38 communications, network systems, requisite facilities, equipment,
39 system controls, simulation, electronic commerce, and all related
40 interactions between people and machines.

1 (~~(24)~~) (25) "Utility-based infrastructure services" includes
2 personal computer and portable device support, servers and server
3 administration, security administration, network administration,
4 telephony, email, and other information technology services commonly
5 used by state agencies.

6 **Sec. 2.** RCW 38.52.040 and 2021 c 233 s 1 and 2021 c 122 s 4 are
7 each reenacted and amended to read as follows:

8 (1) There is hereby created the emergency management council
9 (hereinafter called the council), to consist of not more than 21
10 members who shall be appointed by the adjutant general. The
11 membership of the council shall include, but not be limited to,
12 representatives of city and county governments, two representatives
13 of federally recognized tribes, sheriffs and police chiefs, county
14 coroners and medical examiners, the Washington state patrol, the
15 military department, the department of ecology, state and local fire
16 chiefs, seismic safety experts, state and local emergency management
17 directors, search and rescue volunteers, medical professions who have
18 expertise in emergency medical care, building officials, private
19 industry, and the office of the superintendent of public instruction.
20 The representatives of private industry shall include persons
21 knowledgeable in emergency and hazardous materials management. The
22 councilmembers shall elect a chair from within the council
23 membership. The members of the council shall serve without
24 compensation, but may be reimbursed for their travel expenses
25 incurred in the performance of their duties in accordance with RCW
26 43.03.050 and 43.03.060 as now existing or hereafter amended.

27 (2) The emergency management council shall advise the governor
28 and the director on all matters pertaining to state and local
29 emergency management. The council may appoint such ad hoc committees,
30 subcommittees, and working groups as are required to develop specific
31 recommendations for the improvement of emergency management
32 practices, standards, policies, or procedures. The council shall
33 ensure that the governor receives an annual assessment of statewide
34 emergency preparedness including, but not limited to, specific
35 progress on hazard mitigation and reduction efforts, implementation
36 of seismic safety improvements, reduction of flood hazards,
37 mitigation of cybersecurity risks to critical infrastructure, and
38 coordination of hazardous materials planning and response activities.
39 The council shall review administrative rules governing state and

1 local emergency management practices and recommend necessary
2 revisions to the director.

3 (3) The council or a council subcommittee shall serve and
4 periodically convene in special session as the state emergency
5 response commission required by the emergency planning and community
6 right-to-know act (42 U.S.C. Sec. 11001 et seq.). The state emergency
7 response commission shall conduct those activities specified in
8 federal statutes and regulations and state administrative rules
9 governing the coordination of hazardous materials policy including,
10 but not limited to, review of local emergency planning committee
11 emergency response plans for compliance with the planning
12 requirements in the emergency planning and community right-to-know
13 act (42 U.S.C. Sec. 11001 et seq.). Committees shall annually review
14 their plans to address changed conditions, and submit their plans to
15 the state emergency response commission for review when updated, but
16 not less than at least once every five years. The department may
17 employ staff to assist local emergency planning committees in the
18 development and annual review of these emergency response plans, with
19 an initial focus on the highest risk communities through which trains
20 that transport oil in bulk travel. By March 1, 2018, the department
21 shall report to the governor and legislature on progress towards
22 compliance with planning requirements. The report must also provide
23 budget and policy recommendations for continued support of local
24 emergency planning.

25 (4) (a) The cybersecurity advisory committee is created and is a
26 subcommittee of the emergency management council. The purpose of the
27 cybersecurity advisory committee is to provide advice and
28 recommendations that strengthen cybersecurity in both industry and
29 public sectors across all critical infrastructure sectors.

30 (b) The cybersecurity advisory committee shall bring together
31 organizations with expertise and responsibility for cybersecurity and
32 incident response among local government, tribes, state agencies,
33 institutions of higher education, the technology sector, and first
34 responders with the goal of providing recommendations on building and
35 sustaining the state's capability to identify and mitigate
36 cybersecurity risk and to respond to and recover from cybersecurity-
37 related incidents, including but not limited to ransomware incidents.
38 With respect to critical infrastructure, the cybersecurity advisory
39 committee shall work with relevant federal agencies, state agencies,

1 institutions of higher education as defined in chapter 28B.92 RCW,
2 industry experts, and technical specialists to:

3 (i) Identify which local, tribal, and industry infrastructure
4 sectors are at the greatest risk of cyberattacks and need the most
5 enhanced cybersecurity measures;

6 (ii) Use federal guidance to analyze categories of critical
7 infrastructure in the state that could reasonably result in
8 catastrophic consequences if unauthorized cyber access to the
9 infrastructure occurred;

10 (iii) Recommend cyber incident response exercises that relate to
11 risk and risk mitigation in the water, transportation,
12 communications, health care, elections, agriculture, energy, and
13 higher education sectors, or other sectors as the cybersecurity
14 advisory committee deems appropriate, in consultation with
15 appropriate state agencies including, but not limited to, the energy
16 resilience and emergency management office at the department of
17 commerce and the secretary of state's office; and

18 (iv) Examine the inconsistencies between state and federal law
19 regarding cybersecurity.

20 (c) In fulfilling its duties under this section, the military
21 department and the cybersecurity advisory committee shall collaborate
22 with the consolidated technology services agency and the technology
23 services board security subcommittee created in section 3 of this
24 act.

25 (d) In order to protect sensitive security topics and
26 information, the cybersecurity advisory committee must follow 6
27 C.F.R. Part 29, as it existed on the effective date of this section,
28 procedures for handling critical infrastructure information. The
29 reports produced, and information compiled, pursuant to this
30 subsection are confidential and may not be disclosed under chapter
31 42.56 RCW.

32 (e) The cybersecurity advisory committee must contribute, as
33 appropriate, to the emergency management council annual report and
34 must meet quarterly. The cybersecurity advisory committee shall hold
35 a joint meeting once a year with the technology services board
36 security subcommittee created in section 3 of this act.

37 (f) For the purpose of this subsection, "ransomware" has the same
38 meaning as in RCW 43.105.020.

39 (5)(a) The intrastate mutual aid committee is created and is a
40 subcommittee of the emergency management council. The intrastate

1 mutual aid committee consists of not more than five members who must
2 be appointed by the council chair from council membership. The chair
3 of the intrastate mutual aid committee is the military department
4 representative appointed as a member of the council. Meetings of the
5 intrastate mutual aid committee must be held at least annually.

6 (b) In support of the intrastate mutual aid system established in
7 chapter 38.56 RCW, the intrastate mutual aid committee shall develop
8 and update guidelines and procedures to facilitate implementation of
9 the intrastate mutual aid system by member jurisdictions, including
10 but not limited to the following: Projected or anticipated costs;
11 checklists and forms for requesting and providing assistance;
12 recordkeeping; reimbursement procedures; and other implementation
13 issues. These guidelines and procedures are not subject to the rule-
14 making requirements of chapter 34.05 RCW.

15 ~~((+5))~~ (6) On emergency management issues that involve early
16 learning, kindergarten through twelfth grade, or higher education,
17 the emergency management council must consult with representatives
18 from the following organizations: The department of children, youth,
19 and families; the office of the superintendent of public instruction;
20 the state board for community and technical colleges; and an
21 association of public baccalaureate degree-granting institutions.

22 NEW SECTION. **Sec. 3.** A new section is added to chapter 43.105
23 RCW to read as follows:

24 (1) The technology services board security subcommittee is
25 created within the board. The membership of the technology services
26 board security subcommittee is comprised of a subset of members
27 appointed to the board, as determined by the chair of the technology
28 services board. The chair may make additional appointments to the
29 technology services board security subcommittee to ensure that
30 relevant technology sectors are represented.

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

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

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

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

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

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

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

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

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

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

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

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

28 (6) By December 1, 2023, and each December 1st thereafter, the
29 military department and the agency are jointly responsible for
30 providing a state of cybersecurity report to the governor and the
31 appropriate committees of the legislature, consistent with RCW
32 43.01.036, specifying recommendations considered necessary to address
33 cybersecurity in the state. The technology services board security
34 subcommittee shall coordinate the implementation of any
35 recommendations contained in the state of cybersecurity report. The
36 technology services board security subcommittee may identify as
37 confidential, and not subject to public disclosure, those portions of
38 the report as the technology services board security subcommittee
39 deems necessary to protect the security of public and private cyber
40 systems.

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

5 (8) The reports produced and information compiled pursuant to
6 this section are confidential and may not be disclosed under chapter
7 42.56 RCW.

8 NEW SECTION. **Sec. 4.** A new section is added to chapter 42.56
9 RCW to read as follows:

10 The reports and information, or any portions thereof, that are
11 designated confidential by the cybersecurity advisory committee under
12 RCW 38.52.040(4) and the technology services board security
13 subcommittee under section 3 of this act are confidential and may not
14 be disclosed under this chapter.

15 **Sec. 5.** RCW 43.21F.045 and 2015 c 225 s 73 are each amended to
16 read as follows:

17 (1) The department shall supervise and administer energy-related
18 activities as specified in RCW 43.330.904 and shall advise the
19 governor and the legislature with respect to energy matters affecting
20 the state.

21 (2) In addition to other powers and duties granted to the
22 department, the department shall have the following powers and
23 duties:

24 (a) Prepare and update contingency plans for securing energy
25 infrastructure against all physical and cybersecurity threats, and
26 for implementation in the event of energy shortages or emergencies.
27 The plans shall conform to chapter 43.21G RCW and shall include
28 procedures for determining when these shortages or emergencies exist,
29 the state officers and agencies to participate in the determination,
30 and actions to be taken by various agencies and officers of state
31 government in order to reduce hardship and maintain the general
32 welfare during these emergencies. The department shall coordinate the
33 activities undertaken pursuant to this subsection with other persons.
34 The components of plans that require legislation for their
35 implementation shall be presented to the legislature in the form of
36 proposed legislation at the earliest practicable date. The department
37 shall report to the governor and the legislature on probable,
38 imminent, and existing energy shortages, and shall administer energy

1 allocation and curtailment programs in accordance with chapter 43.21G
2 RCW.

3 (b) Establish and maintain a central repository in state
4 government for collection of existing data on energy resources,
5 including:

6 (i) Supply, demand, costs, utilization technology, projections,
7 and forecasts;

8 (ii) Comparative costs of alternative energy sources, uses, and
9 applications; and

10 (iii) Inventory data on energy research projects in the state
11 conducted under public and/or private auspices, and the results
12 thereof.

13 (c) Coordinate federal energy programs appropriate for state-
14 level implementation, carry out such energy programs as are assigned
15 to it by the governor or the legislature, and monitor federally
16 funded local energy programs as required by federal or state
17 regulations.

18 (d) Develop energy policy recommendations for consideration by
19 the governor and the legislature.

20 (e) Provide assistance, space, and other support as may be
21 necessary for the activities of the state's two representatives to
22 the Pacific northwest electric power and conservation planning
23 council. To the extent consistent with federal law, the director
24 shall request that Washington's councilmembers request the
25 administrator of the Bonneville power administration to reimburse the
26 state for the expenses associated with the support as provided in the
27 Pacific Northwest Electric Power Planning and Conservation Act (P.L.
28 96-501).

29 (f) Cooperate with state agencies, other governmental units, and
30 private interests in the prioritization and implementation of the
31 state energy strategy elements and on other energy matters.

32 (g) Serve as the official state agency responsible for
33 coordinating implementation of the state energy strategy.

34 (h) No later than December 1, 1982, and by December 1st of each
35 even-numbered year thereafter, prepare and transmit to the governor
36 and the appropriate committees of the legislature a report on the
37 implementation of the state energy strategy and other important
38 energy issues, as appropriate.

1 (i) Provide support for increasing cost-effective energy
2 conservation, including assisting in the removal of impediments to
3 timely implementation.

4 (j) Provide support for the development of cost-effective energy
5 resources including assisting in the removal of impediments to timely
6 construction.

7 (k) Adopt rules, under chapter 34.05 RCW, necessary to carry out
8 the powers and duties enumerated in this chapter.

9 (l) Provide administrative assistance, space, and other support
10 as may be necessary for the activities of the energy facility site
11 evaluation council, as provided for in RCW 80.50.030.

12 (m) Appoint staff as may be needed to administer energy policy
13 functions and manage energy facility site evaluation council
14 activities. These employees are exempt from the provisions of chapter
15 41.06 RCW.

16 (3) To the extent the powers and duties set out under this
17 section relate to energy education, applied research, and technology
18 transfer programs they are transferred to Washington State
19 University.

20 (4) To the extent the powers and duties set out under this
21 section relate to energy efficiency in public buildings they are
22 transferred to the department of enterprise services.

--- END ---