
SENATE BILL 5619

State of Washington

68th Legislature

2023 Regular Session

By Senators Lias, Boehnke, Hunt, Nguyen, and Torres

Read first time 01/30/23. Referred to Committee on Environment,
Energy & Technology.

1 AN ACT Relating to establishing a cybersecurity governance
2 framework within state government; reenacting and amending RCW
3 38.52.040; adding a new section to chapter 43.105 RCW; and adding a
4 new section to chapter 42.56 RCW.

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

6 **Sec. 1.** 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

1 councilmembers shall elect a chair from within the council
2 membership. The members of the council shall serve without
3 compensation, but may be reimbursed for their travel expenses
4 incurred in the performance of their duties in accordance with RCW
5 43.03.050 and 43.03.060 as now existing or hereafter amended.

6 (2) The emergency management council shall advise the governor
7 and the director on all matters pertaining to state and local
8 emergency management. The council may appoint such ad hoc committees,
9 subcommittees, and working groups as are required to develop specific
10 recommendations for the improvement of emergency management
11 practices, standards, policies, or procedures. The council shall
12 ensure that the governor receives an annual assessment of statewide
13 emergency preparedness including, but not limited to, specific
14 progress on hazard mitigation and reduction efforts, implementation
15 of seismic safety improvements, reduction of flood hazards, and
16 coordination of hazardous materials planning and response activities.
17 The council shall review administrative rules governing state and
18 local emergency management practices and recommend necessary
19 revisions to the director.

20 (3) The council or a council subcommittee shall serve and
21 periodically convene in special session as the state emergency
22 response commission required by the emergency planning and community
23 right-to-know act (42 U.S.C. Sec. 11001 et seq.). The state emergency
24 response commission shall conduct those activities specified in
25 federal statutes and regulations and state administrative rules
26 governing the coordination of hazardous materials policy including,
27 but not limited to, review of local emergency planning committee
28 emergency response plans for compliance with the planning
29 requirements in the emergency planning and community right-to-know
30 act (42 U.S.C. Sec. 11001 et seq.). Committees shall annually review
31 their plans to address changed conditions, and submit their plans to
32 the state emergency response commission for review when updated, but
33 not less than at least once every five years. The department may
34 employ staff to assist local emergency planning committees in the
35 development and annual review of these emergency response plans, with
36 an initial focus on the highest risk communities through which trains
37 that transport oil in bulk travel. By March 1, 2018, the department
38 shall report to the governor and legislature on progress towards
39 compliance with planning requirements. The report must also provide

1 budget and policy recommendations for continued support of local
2 emergency planning.

3 (4) (a) The cybersecurity advisory committee is created and is a
4 subcommittee of the emergency management council. The purpose of this
5 cybersecurity advisory committee is to provide advice and
6 recommendations that strengthen cybersecurity in both industry and
7 public sectors across all critical infrastructure sectors.

8 (b) The cybersecurity advisory committee shall bring together
9 organizations with expertise and responsibility for cybersecurity and
10 incident response among local government, tribes, state agencies,
11 institutions of higher education, the technology sector, and first
12 responders with the goal of providing recommendations on building and
13 sustaining the state's capability to identify and mitigate
14 cybersecurity risk and to respond to and recover from cybersecurity-
15 related incidents. With respect to critical infrastructure, the
16 cybersecurity advisory committee shall work with relevant federal
17 agencies, institutions of higher education as defined in chapter
18 28B.92 RCW, industry experts, and technical specialists to:

19 (i) Assess critical infrastructure not covered by federal law, to
20 identify which local, tribal, and industry infrastructure sectors are
21 at the greatest risk of cyberattacks and need the most enhanced
22 cybersecurity measures;

23 (ii) Use federal guidance to identify categories of critical
24 infrastructure as critical cyber infrastructure if cyber damage or
25 unauthorized cyber access to the infrastructure could reasonably
26 result in catastrophic consequences;

27 (iii) Recommend cyber incident response exercises that relates
28 risk and risk mitigation in the water, transportation,
29 communications, health care elections, agriculture, and higher
30 education sectors; and

31 (iv) Examine the inconsistencies between state and federal law
32 regarding cybersecurity.

33 (c) In fulfilling its duties under this section, the military
34 department and the cybersecurity advisory committee shall collaborate
35 with the consolidated technology services agency and the technology
36 services board security subcommittee created in section 2 of this
37 act.

38 (d) In order to discuss sensitive security topics and
39 information, the cybersecurity advisory committee may hold a portion
40 of its agenda in executive session closed to the public. The reports

1 produced, and information compiled, pursuant to this subsection are
2 confidential and may not be disclosed under chapter 42.56 RCW.

3 (e) The cybersecurity advisory committee shall meet quarterly.
4 The cybersecurity advisory committee shall hold a joint meeting once
5 a year with the technology services board security subcommittee
6 created in section 2 of this act.

7 (5)(a) The intrastate mutual aid committee is created and is a
8 subcommittee of the emergency management council. The intrastate
9 mutual aid committee consists of not more than five members who must
10 be appointed by the council chair from council membership. The chair
11 of the intrastate mutual aid committee is the military department
12 representative appointed as a member of the council. Meetings of the
13 intrastate mutual aid committee must be held at least annually.

14 (b) In support of the intrastate mutual aid system established in
15 chapter 38.56 RCW, the intrastate mutual aid committee shall develop
16 and update guidelines and procedures to facilitate implementation of
17 the intrastate mutual aid system by member jurisdictions, including
18 but not limited to the following: Projected or anticipated costs;
19 checklists and forms for requesting and providing assistance;
20 recordkeeping; reimbursement procedures; and other implementation
21 issues. These guidelines and procedures are not subject to the rule-
22 making requirements of chapter 34.05 RCW.

23 ~~((+5))~~ (6) On emergency management issues that involve early
24 learning, kindergarten through twelfth grade, or higher education,
25 the emergency management council must consult with representatives
26 from the following organizations: The department of children, youth,
27 and families; the office of the superintendent of public instruction;
28 the state board for community and technical colleges; and an
29 association of public baccalaureate degree-granting institutions.

30 NEW SECTION. Sec. 2. A new section is added to chapter 43.105
31 RCW to read as follows:

32 (1) The technology services board security subcommittee is
33 created within the board. The membership of the technology services
34 board security subcommittee is comprised of a subset of members
35 appointed to the board, as determined by the chair of the technology
36 services board security subcommittee. The chair may make additional
37 appointments to the technology services board security subcommittee
38 to ensure that relevant technology sectors are represented.

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

3 (a) Review emergent cyberattacks and threats to critical
4 infrastructure sectors in order to identify existing gaps in state
5 agency cybersecurity policies;

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

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

10 (d) Recommend tabletop cybersecurity exercises, including data
11 breach simulation exercises;

12 (e) Assist the office of cybersecurity created in RCW 43.105.450
13 in developing cybersecurity best practice recommendations for state
14 agencies;

15 (f) Review the proposed policies and standards developed by the
16 office of cybersecurity and recommend their approval to the full
17 board;

18 (g) Review information relating to cybersecurity incidents and
19 ransomware incidents to determine commonalities and develop best
20 practice recommendations for public agencies; and

21 (h) Assist the agency and the military department in creating the
22 state of cybersecurity report required in subsection (6) of this
23 section.

24 (3) In providing staff support to the board, the agency shall
25 work with the national institute of standards and technology and
26 other federal agencies, private sector businesses, and private
27 cybersecurity experts and bring their perspectives and guidance to
28 the board for consideration in fulfilling its duties to ensure a
29 holistic approach to cybersecurity in state government.

30 (4) To discuss sensitive security topics and information, the
31 technology services board security subcommittee may hold a portion of
32 its agenda in executive session closed to the public. Time reserved
33 for executive session may not comprise greater than one-half of the
34 agenda time of a given meeting.

35 (5) The technology services board security subcommittee must meet
36 quarterly. The technology services board security subcommittee must
37 hold a joint meeting once a year with the cybersecurity advisory
38 committee created in RCW 38.52.040(4).

39 (6) By December 1, 2023, and each December 1st thereafter, the
40 military department and the agency are jointly responsible for

1 providing a state of cybersecurity report to the governor and the
2 appropriate committees of the legislature, consistent with RCW
3 43.01.036, specifying recommendations considered necessary to address
4 cybersecurity in the state. The technology services board security
5 subcommittee may identify as confidential, and not subject to public
6 disclosure, those portions of the report as the technology services
7 board security subcommittee deems necessary to protect the security
8 of public and private cyber systems.

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

13 (8) The reports produced and information compiled pursuant to
14 this section are confidential and may not be disclosed under chapter
15 42.56 RCW.

16 NEW SECTION. **Sec. 3.** A new section is added to chapter 42.56
17 RCW to read as follows:

18 The reports and information, or those portions thereof that are
19 designated confidential by the cybersecurity advisory committee under
20 RCW 38.52.040(4) and the technology services board security
21 subcommittee under section 2 of this act, are confidential and may
22 not be disclosed under this chapter.

--- END ---