S-0076.2

SENATE BILL 5619

State of Washington 68th Legislature 2023 Regular Session

By Senators Liias and Boehnke

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

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

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

(1) There is hereby created the emergency management council (hereinafter called the council), to consist of not more than 21 members who shall be appointed by the adjutant general. The membership of the council shall include, but not be limited to, representatives of city and county governments, two representatives of federally recognized tribes, sheriffs and police chiefs, county coroners and medical examiners, the Washington state patrol, the military department, the department of ecology, state and local fire chiefs, seismic safety experts, state and local emergency management directors, search and rescue volunteers, medical professions who have expertise in emergency medical care, building officials, private industry, and the office of the superintendent of public instruction. The representatives of private industry shall include persons knowledgeable in emergency and hazardous materials management. The

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

--- END ---