CERTIFICATION OF ENROLLMENT

SECOND SUBSTITUTE SENATE BILL 5518

Chapter 124, Laws of 2023

68th Legislature
2023 Regular Session

CYBERSECURITY—VARIOUS PROVISIONS

EFFECTIVE DATE: July 23, 2023

Passed by the Senate March 2, 2023
Yeas 49 Nays 0

DENNY HECK

President of the Senate

Passed by the House April 6, 2023
Yeas 97 Nays 0

LAURIE JINKINS

Speaker of the House of Representatives

Approved April 20, 2023 10:32 AM

JAY INSLEE

Governor of the State of Washington

CERTIFICATE

I, Sarah Bannister, Secretary of the Senate of the State of Washington, do hereby certify that the attached is **SECOND SUBSTITUTE SENATE BILL 5518** as passed by the Senate and the House of Representatives on the dates hereon set forth.

SARAH BANNISTER

Secretary

FILED

April 21, 2023

Secretary of State
State of Washington

SECOND SUBSTITUTE SENATE BILL 5518

Passed Legislature - 2023 Regular Session

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.

AN ACT Relating to cybersecurity; amending RCW 43.21F.045; reenacting and amending RCW 43.105.020 and 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 43.105.020 and 2021 c 176 s 5223 and 2021 c 40 s 2 are each reenacted and amended to read as follows:

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

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

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

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

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

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

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

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

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

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

(a) Prevent improper information modification or destruction;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 2. 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, mitigation of cybersecurity risks to critical infrastructure, 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 the 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, including but not limited to ransomware incidents. With respect to critical infrastructure, the cybersecurity advisory committee shall work with relevant federal agencies, state agencies,

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

(i) 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 analyze categories of critical infrastructure in the state that could reasonably result in catastrophic consequences if unauthorized cyber access to the infrastructure occurred;

(iii) Recommend cyber incident response exercises that relate to risk and risk mitigation in the water, transportation, communications, health care, elections, agriculture, energy, and higher education sectors, or other sectors as the cybersecurity advisory committee deems appropriate, in consultation with appropriate state agencies including, but not limited to, the energy resilience and emergency management office at the department of commerce and the secretary of state's office; 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 3 of this act.

(d) In order to protect sensitive security topics and information, the cybersecurity advisory committee must follow 6 C.F.R. Part 29, as it existed on the effective date of this section, procedures for handling critical infrastructure information. 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 must contribute, as appropriate, to the emergency management council annual report and must meet quarterly. The cybersecurity advisory committee shall hold a joint meeting once a year with the technology services board security subcommittee created in section 3 of this act.

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

(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. 3.** 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. 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.

(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 shall coordinate the implementation of any recommendations contained in the state of cybersecurity report. 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. 4.** A new section is added to chapter 42.56 RCW to read as follows:

The reports and information, or any 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 3 of this act are confidential and may not be disclosed under this chapter.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Passed by the Senate March 2, 2023.
Passed by the House April 6, 2023.
Approved by the Governor April 20, 2023.
Filed in Office of Secretary of State April 21, 2023.

--- END ---