S-0375.2

SENATE BILL 5518

State of Washington 68th Legislature 2023 Regular Session

By Senators Boehnke, Stanford, MacEwen, Muzzall, Fortunato, Frame, Kuderer, Valdez, Warnick, and Wellman

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

AN ACT Relating to the protection of critical constituent and state operational data against the financial and personal harm caused by ransomware and other malicious cyber activities; amending RCW 43.105.220 and 43.105.342; reenacting and amending RCW 43.105.020; adding a new section to chapter 43.105 RCW; adding a new section to chapter 42.56 RCW; and creating new sections.

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

NEW SECTION. **Sec. 1.** The legislature finds that Washington state branches of government, agencies, boards, and commissions manage and protect highly sensitive data to best serve constituents. The data managed by public entities is a high value target for domestic and international perpetrators of for-profit ransomware and other malicious cyber activities. Breaches in data security prevent state agencies from protecting confidential and sensitive information stored in technology systems.

In the absence of immutable data protection capabilities and reliable disaster recovery practices, the legislature finds that a breach of state agency information technology systems may result in the reduction of critical constituent services and increased risk of financial harm related to identity theft.

The legislature finds that state agencies have implemented enterprise technology programs, standards, and policies for data backup and recovery practices to protect confidential and sensitive information contained in enterprise and individual state agencies' information technology systems. The legislature further finds that combining these data protection practices with preventative practices, such as an enterprise identity management solution, the active promotion of cybersecurity awareness practices, and maintaining the readiness of state resources for incident management is the best protection that the state can offer to combat the effects of ransomware and other malicious cyber activities.

The legislature recognizes that action must be taken at each state agency to ensure data protection and disaster recovery practices are consistent with enterprise technology standards and is aware that additional investments in technology, training, and personnel will be needed. The legislature further recognizes that adequate funding must be provided to support agency efforts to protect confidential and sensitive data stored in technology systems.

Sec. 2. 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) "Immutable" means to provide state agencies with recovery capabilities. A native immutable information protection solution must demonstrate characteristics that do not permit, unless scheduled to do so by a predefined process, the editing or removing of any protected information.

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

((~~(9)~~)) (10) "Information protection" includes backups and other methods to allow the preservation and recovery of information.

(11) "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)~~)) (12) "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)~~)) (13) "Information technology portfolio" or "portfolio" means a strategic management process documenting relationships between agency missions and information technology and telecommunications investments.

((~~(12)~~)) (14) "K-20 network" means the network established in RCW 43.41.391.

((~~(13)~~)) (15) "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)~~)) (16) "Malicious cyber activities" means activities, other than those authorized by or in accordance with state and federal law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information residing on those systems.

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

((~~(15)~~)) (18) "Oversight" means a process of comprehensive risk analysis and management designed to ensure optimum use of information technology resources and telecommunications.

((~~(16)~~)) (19) "Proprietary software" means that software offered for sale or license.

((~~(17)~~)) (20) "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)~~)) (21) "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)~~)) (22) "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)~~)) (23) "Public safety" refers to any entity or services that ensure the welfare and protection of the public.

((~~(21)~~)) (24) "Ransomware" includes any type of malicious software code, executable, application, payload, or digital content designed to encrypt, steal, exfiltrate, delete, destroy, or deny access to any data, databases, systems, applications, networks, data centers, cloud computing environment, cloud service, or other mission critical or business essential infrastructure.

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

((~~(23)~~)) (27) "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)~~)) (28) "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.

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

(1) The office shall design, develop, and implement enterprise technology standards specific to malware and ransomware protection, backup, and recovery, as well as prevention education for state employees and constituents who use state technology services. The office shall refer to the national institute of standards and technology (NIST) ransomware profile contained in the NIST ransomware *Risk Management: A Cybersecurity Framework Profile* published February 2022, or its successor publication, as guidance to support the prevention of, response to, and recovery from, ransomware events.

(2)(a) The office shall establish a ransomware education and outreach program dedicated to educating public agencies on the prevention, response, and remediation of malware and ransomware.

(b) The office shall document, publish, and distribute malware and ransomware response educational materials specifically for chief executive officers, chief financial officers, chief information officers, and chief information security officers, or their equivalents, to each state agency, which outlines specific steps to take in the event of a malware attack that destroys, encrypts, exfiltrates, obfuscates, or otherwise prevents the owning organization from accessing their data.

(3) Each state agency must ensure that all mission critical applications, business essential applications, and other resources containing category 3 or category 4 data as defined in enterprise technology standards developed pursuant to RCW 43.105.054, have immutable backups.

(4) By September 30, 2023, and biannually thereafter, each state agency shall review all of its mission critical applications, business essential applications, and other resources containing category 3 or category 4 data, as described in the enterprise technology standards developed pursuant to RCW 43.105.054, and report to the office:

(a) The total size of managed data;

(b) A list of mission critical applications and business essential applications, containing category 3 or category 4 data, as described in the enterprise technology standards developed pursuant to RCW 43.105.054;

(c) A list of the applications described in (b) of this subsection that do not have immutable backup; and

(d) A list of prioritized applications based on mission criticality and impact to constituents in the event of system failure or data loss.

(5)(a) By March 31, 2024, except as provided in (b) of this subsection, state agencies shall:

(i) Ensure that all mission critical applications, business essential applications, and other resources containing category 3 or category 4 data, as described in enterprise technology standards developed under RCW 43.105.054, are compliant with subsection (3) of this section; and

(ii) Report to the office whether they are in compliance with this subsection (5)(a).

(b) If any state agency reasonably anticipates that it cannot comply with (a) of this subsection by March 31, 2024, it shall submit a plan by March 31, 2024, to the office detailing steps it will take to comply with the requirement in (a) of this subsection.

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

(7) This section does not apply to institutions of higher education.

Sec. 4. RCW 43.105.220 and 2015 3rd sp.s. c 1 s 203 are each amended to read as follows:

(1)(a) The office shall prepare a state strategic information technology plan which shall establish a statewide mission, goals, and objectives for the use of information technology, including goals for electronic access to government records, information, and services. The plan shall be developed in accordance with the standards and policies established by the office. The office shall seek the advice of the board in the development of this plan.

(b) The plan shall be updated as necessary and submitted to the governor and the legislature.

(2)(a) The office shall prepare a biennial state performance report on information technology based on state agency performance reports required under RCW 43.105.235 and other information deemed appropriate by the office. The report shall include, but not be limited to:

((~~(a)~~)) (i) An analysis, based upon agency portfolios, of the state's information technology infrastructure, including its value, condition, and capacity;

((~~(b)~~)) (ii) An evaluation of performance relating to information technology;

((~~(c)~~)) (iii) An assessment of progress made toward implementing the state strategic information technology plan, including progress toward electronic access to public information and enabling citizens to have two-way access to public records, information, and services; and

((~~(d)~~)) (iv) An analysis of the success or failure, feasibility, progress, costs, and timeliness of implementation of major information technology projects under RCW 43.105.245. At a minimum, the portion of the report regarding major technology projects must include:

((~~(i)~~)) (A) The total cost data for the entire life-cycle of the project, including capital and operational costs, broken down by staffing costs, contracted service, hardware purchase or lease, software purchase or lease, travel, and training. The original budget must also be shown for comparison;

((~~(ii)~~)) (B) The original proposed project schedule and the final actual project schedule;

((~~(iii)~~)) (C) Data regarding progress towards meeting the original goals and performance measures of the project;

((~~(iv)~~)) (D) Discussion of lessons learned on the project, performance of any contractors used, and reasons for project delays or cost increases; and

((~~(v)~~)) (E) Identification of benefits generated by major information technology projects developed under RCW 43.105.245.

(b) Copies of the report shall be distributed biennially to the governor and the legislature. The major technology section of the report must examine major information technology projects completed in the previous biennium.

(3)(a) By December 31, 2024, and biannually thereafter, the office shall provide an oral report to the members of the technology services board during an executive session which is closed to the public, the chairs and ranking members of the appropriate fiscal committees of the senate and house of representatives, and the appropriate policy staff in the office of the governor which must include the following information based on the data reported by state agencies pursuant to section 3(4) of this act:

(i) The total number of mission critical applications within state agencies;

(ii) The total number of mission critical applications within state agencies with immutable backups;

(iii) The total number of business essential applications within state agencies;

(iv) The total number of business essential applications held by state agencies with immutable backups;

(v) The total number of applications held by state agencies containing either category 3 data or category 4 data, or both;

(vi) The total number of applications held by state agencies containing either category 3 data or category 4 data, or both, with immutable backups;

(vii) The breadth of threat landscape;

(viii) A prioritized list of applications within each state agency requiring immutable backups;

(ix) The cost of implementing immutable backups for each prioritized application;

(x) The number of full-time equivalents required to manage malware prevention and response policies and state agency incident response assistance;

(xi) Progress toward protection compared with the last submitted report; and

(xii) Recommendations for further work to protect critical state systems.

(b) The oral report provided under (a) of this subsection may not be recorded. The information described in (a) of this subsection is confidential and may not be disclosed under chapter 42.56 RCW.

NEW SECTION. **Sec. 5.** A new section is added to chapter 42.56 RCW to read as follows:

The reports and information compiled pursuant to section 3 of this act and RCW 43.105.220(3) are confidential, and may not be disclosed under this chapter.

Sec. 6. RCW 43.105.342 and 2015 3rd sp.s. c 1 s 501 are each amended to read as follows:

(1) The consolidated technology services revolving account is created in the custody of the state treasurer. All receipts from agency fees and charges for services collected from public agencies must be deposited into the account. The account must be used for the:

(a) Acquisition of equipment, software, supplies, and services; and

(b) Payment of salaries, wages, and other costs incidental to the acquisition, development, maintenance, operation, and administration of: (i) Information services; (ii) telecommunications; (iii) systems; (iv) software; (v) supplies; and (vi) equipment, including the payment of principal and interest on debt by the agency and other users as determined by the office of financial management.

(2) The director or the director's designee, with the approval of the technology services board, is authorized to expend ((~~up to one million dollars~~)):

(a) Up to $1,000,000 per fiscal biennium for the technology services board to conduct independent technical and financial analysis of proposed information technology projects; and

(b) Up to $5,000,000 per fiscal biennium for the board to provide funding to state agencies for the purposes of procuring immutable data backup and disaster recovery services for mission critical applications, business essential applications, or other critical information technology systems, containing category 3 or category 4 data as described in enterprise technology standards developed under RCW 43.105.054. When selecting state agencies to receive funding under this subsection, the board must consider the agency's

prioritized application list under section 3 of this act, in order to ensure that funding is allocated to protecting the most vulnerable systems containing the most sensitive public information.

(3) Only the director or the director's designee may authorize expenditures from the account. The account is subject to allotment procedures under chapter 43.88 RCW, but no appropriation is required for expenditures except as provided in subsection (4) of this section.

(4) Expenditures for the strategic planning and policy component of the agency are subject to appropriation.

NEW SECTION. **Sec. 7.** This act may be known and cited as the Washington state ransomware protection act.

--- END ---