S-3646.2

SENATE BILL 5916

State of Washington 67th Legislature 2022 Regular Session

By Senators Mullet, Conway, Fortunato, Nguyen, and Wagoner

Read first time 01/20/22. 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 43.105.054 and 43.105.220; reenacting and amending RCW 43.105.020; adding new sections to chapter 43.105 RCW; adding a new section to chapter 42.56 RCW; creating new sections; and making an appropriation.

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

NEW SECTION. **Sec. 1.** Washington state branches of government, agencies, boards, and commissions manage and protect highly sensitive data in order 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 backup capabilities and reliable disaster recovery practices, state agency information technology systems are vulnerable to such breaches in security. The legislature finds that enterprise technology programs, standards, and policies have been developed for data backup and recovery practices that agencies must implement to protect

confidential and sensitive information contained in enterprise and individual agencies' information technology systems. The legislature further finds that the availability of an enterprise identity management solution, the active promotion of cybersecurity awareness practices, readiness of state resources for incident management, and the availability of immutable data backups of critical, sensitive, and confidential data are the best protection that the state can offer to combat ransomware and other malicious cyber activities. The legislature recognizes that action must be taken at each state agency to ensure data backup and disaster recovery practices are consistent with enterprise technology standards and is aware that additional investments in technology, training, and personnel will be needed.

NEW SECTION. **Sec. 2.** 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 using state technology services, incident reporting, and incident response management and remediation. Enterprise technology standards must be reviewed annually.

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

(b) The office shall document, publish, and distribute 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, board, and commission, which outlines specific steps to take in the event of a malware attack. Distribution of materials must be determined at the discretion of the office.

(3) Except as provided in subsection (4) of this section, each state agency as defined within enterprise technology standards developed pursuant to RCW 43.105.054 must comply with the enterprise technology standards implemented pursuant to subsection (1) of this section.

(4) A state agency with a requirement that precludes it from complying with subsection (3) of this section must receive a waiver from the office. Waivers must be based upon a written business justification from the requesting state agency, board, or commission.

Waiver requests must be signed by the chief executive, chief financial officer, and risk manager of the requesting state agency, board, or commission. Such a waiver request, and all relevant data used to inform the waiver, or its consideration, are exempt from disclosure under the public records act, chapter 42.56 RCW.

(5) Each state agency must execute and analyze monthly vulnerability scans, making data available to the office of cybersecurity, the office of the state chief information officer, and the office of the state auditor upon request.

(6) Each state agency must ensure that all mission critical applications, business essential applications, and other resources containing data that requires special handling, as defined in enterprise technology standards developed pursuant to RCW 43.105.054, must be protected to the maximum extent feasible.

(7)(a) Each state agency must perform an assessment of all their applications and resources containing data and report to the office the sizing of managed data to include identifying mission critical applications, business essential applications, and categorizing all data attributes, as defined in enterprise technology standards developed pursuant to RCW 43.105.054, and develop a list of prioritized applications based on mission criticality and impact to constituents in the event of system failure or data loss and submit the list to the office.

(b) Each state agency must submit the sizing of managed data and the list required in (a) of this subsection to the office by September 1, 2022.

(8)(a) The office must analyze and aggregate data reported pursuant to subsection (7) of this section.

(b) By October 31, 2023, the office must submit a report to the governor and the appropriate committees of the legislature on the following:

(i) The total number of mission critical applications, the total amount of data associated with each mission critical application, the percentage of mission critical applications with immutable backups, the estimated annual data change and growth rates for each mission critical application, the percentage of mission critical applications that undergo annual continuity of operations exercises, and the percentage that meet enterprise technology standards;

(ii) The total number of business essential applications, the total amount of data associated with each business essential

application, the estimated annual data change and growth rates for each business essential application, the percentage of business essential applications with immutable backups, the percentage of business essential applications that undergo annual continuity of operations exercises, and the percentage that meet backup and recovery standards of the office;

(iii) The percentage of applications with catalogued and categorized data;

(iv) Each state agency that received waivers pursuant to subsection (4) of this section;

(v) Prioritized applications identified by each state agency as required in subsection (7)(a) of this section; and

(vi) Recommendations for further legislation, rules, and policy that will increase protections against ransomware.

(9) Agencies must ensure that all mission critical applications, business essential applications, and other resources containing category 3 and category 4 data are protected in accordance with enterprise technology standards developed under RCW 43.105.054.

(10) The office of financial management, department of enterprise services, and consolidated technology services agency must ensure that all mission critical and business essential information technology systems, in accordance with enterprise technology standards developed under RCW 43.105.054, are compliant with the provisions of this act and are supported by immutable backups by December 31, 2025.

(11) The office shall modify existing portfolio reporting mechanisms already in place to support the collection of relevant data necessary to baseline and monitor risk associated with malware and ransomware protections. This data must be analyzed for risk and must be used to prioritize a list of mission critical applications that need additional protections, which may require additional investment by the legislature in future biennia.

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

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

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

Ransomware protection, data security, and continuity of operations are considered critical success factors of state managed technology projects. Each technology project submitted for risk assessment by the office must include an indication of the agency's intent to incorporate data backup and recovery for the purposes of data security and continuity of operations within the project scope. Technology budgets analyzed as part of gated funding must include discreet separate line items for backup and recovery services where applicable. Exit criteria for each applicable project must include confirmation of an immutable backup solution as well as a successful test of application and data recovery.

NEW SECTION. **Sec. 4.** A new section is added to chapter 43.105 RCW to read as follows:

The information technology security account is created in the state treasury. All receipts directed to the account must be deposited in the account. Moneys in the account may be spent only after appropriation. Expenditures from the account may only be used for the purposes of protecting critical state agency information technology systems for which data backup and recovery are essential. Moneys in the account must supplement, and may supplant, existing funding to the consolidated technology services agency or the office of the state chief information officer.

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 2 (7) and (8)(b) of this act and the report submitted pursuant to RCW 43.105.220(3)(a) are confidential and may not be disclosed under this chapter.

Sec. 6. 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) "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) "State agency" means every state office, department, division, bureau, board, commission, or other state agency, including offices headed by a statewide elected official.

(23) "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) "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.

(25) "Immutable" means data that is stored unchanged over time or unable to be changed. For the purposes of backups, this means that, once ingested, no external or internal operation can modify the data and must never be available in a read/write state to the client. "Immutable" specifically applies to the characteristics and attributes of a backup system's file system and may not be applied to temporary systems state, time-bound or expiring configurations, or temporary conditions created by a physical air gap as is implemented in most legacy systems. An immutable file system must demonstrate characteristics that do not permit the editing or changing of any data backed up to provide agencies with absolute recovery capabilities.

(26) "Malicious cyber activities" means activities, other than those authorized by or in accordance with United States 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 resident thereon.

(27) "Ransomware" means 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 essential or business critical infrastructure.

Sec. 7. RCW 43.105.054 and 2021 c 291 s 9 are each amended to read as follows:

(1) The director shall establish standards and policies to govern information technology in the state of Washington.

(2) The office shall have the following powers and duties related to information services:

(a) To develop statewide standards and policies governing the:

(i) Acquisition of equipment, software, and technology-related services;

(ii) Disposition of equipment;

(iii) Licensing of the radio spectrum by or on behalf of state agencies; and

(iv) Confidentiality of computerized data;

(b) To develop statewide and interagency technical policies, standards, and procedures;

(c) To review and approve standards and common specifications for new or expanded telecommunications networks proposed by agencies, public postsecondary education institutions, educational service districts, or statewide or regional providers of K-12 information technology services;

(d) With input from the legislature and the judiciary, to provide direction concerning strategic planning goals and objectives for the state;

(e) To establish policies for the periodic review by the director of state agency performance which may include but are not limited to analysis of:

(i) Planning, management, control, and use of information services;

(ii) Training and education;

(iii) Project management; and

(iv) Cybersecurity, in coordination with the office of cybersecurity;

(f) To coordinate with state agencies with an annual information technology expenditure that exceeds ten million dollars to implement a technology business management program to identify opportunities for savings and efficiencies in information technology expenditures and to monitor ongoing financial performance of technology investments;

(g) In conjunction with the consolidated technology services agency, to develop statewide standards for agency purchases of technology networking equipment and services;

(h) To implement a process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines adopted by the director;

(i) To develop plans and procedures to ensure the continuity of commerce for information resources that support the operations and assets of state agencies in the event of a security incident; ((~~and~~))

(j) To design, develop, and implement enterprise technology standards specific to malware and ransomware protection, backup, and recovery; and

(k) To work with the office of cybersecurity, department of commerce, and other economic development stakeholders to facilitate the development of a strategy that includes key local, state, and federal assets that will create Washington as a national leader in cybersecurity. The office shall collaborate with, including but not limited to, community colleges, universities, the national guard, the department of defense, the department of energy, and national laboratories to develop the strategy.

(3) Statewide technical standards to promote and facilitate electronic information sharing and access are an essential component of acceptable and reliable public access service and complement content-related standards designed to meet those goals. The office shall:

(a) Establish technical standards to facilitate electronic access to government information and interoperability of information systems, including wireless communications systems; and

(b) Require agencies to include an evaluation of electronic public access needs when planning new information systems or major upgrades of systems.

In developing these standards, the office is encouraged to include the state library, state archives, and appropriate representatives of state and local government.

Sec. 8. 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, the office shall initiate a biannual report to the legislature, governor, and technology services board sharing information garnered from the agency reports that includes:

(i) The number of mission critical applications;

(ii) The number of mission critical applications with immutable backups;

(iii) The number of business essential applications;

(iv) The number of business essential applications with backups meeting enterprise technology standards;

(v) The number of applications containing either category 3 data or category 4 data, or both;

(vi) The number of applications 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 systems within the enterprise 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 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) These additional reporting requirements are not subject to public disclosure under chapter 42.56 RCW.

NEW SECTION. **Sec. 9.** A new section is added to chapter 43.105 RCW to read as follows:

The office must apply for any federal grant or other financial assistance program, excluding loans, that meets the purposes of this act. Any federal revenues received from these grants or programs that may be used to provide security and protection to critical state agency information technology systems must be deposited into the information technology security account created in section 4 of this act.

NEW SECTION. **Sec. 10.** The sum of $5,000,000, or as much thereof as may be necessary, is appropriated for the fiscal year ending June 30, 2023, from the general fund to the information technology security account created in section 4 of this act for the purposes of this act.

NEW SECTION. **Sec. 11.** This act may be known and cited as the Washington state ransomware protection act.

--- END ---