

---

**HOUSE BILL 1464**

---

**State of Washington**

**68th Legislature**

**2023 Regular Session**

**By** Representatives Hackney, Barnard, Walen, Jacobsen, and Ormsby

1 AN ACT Relating to the protection of critical constituent and  
2 state operational data against the financial and personal harm caused  
3 by ransomware and other malicious cyber activities; amending RCW  
4 43.105.220 and 43.105.342; reenacting and amending RCW 43.105.020;  
5 adding a new section to chapter 43.105 RCW; adding a new section to  
6 chapter 42.56 RCW; and creating new sections.

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

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

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

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

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

19       **Sec. 2.** RCW 43.105.020 and 2021 c 176 s 5223 and 2021 c 40 s 2  
20 are each reenacted and amended to read as follows:

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

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

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

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

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

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

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

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

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

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

13 ~~((9))~~ (10) "Information protection" includes backups and other  
14 methods to allow the preservation and recovery of information.

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

18 (a) Prevent improper information modification or destruction;

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

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

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

25 ~~((10))~~ (12) "Information technology" includes, but is not  
26 limited to, all electronic technology systems and services, automated  
27 information handling, system design and analysis, conversion of data,  
28 computer programming, information storage and retrieval,  
29 telecommunications, requisite system controls, simulation, electronic  
30 commerce, radio technologies, and all related interactions between  
31 people and machines.

32 ~~((11))~~ (13) "Information technology portfolio" or "portfolio"  
33 means a strategic management process documenting relationships  
34 between agency missions and information technology and  
35 telecommunications investments.

36 ~~((12))~~ (14) "K-20 network" means the network established in RCW  
37 43.41.391.

38 ~~((13))~~ (15) "Local governments" includes all municipal and  
39 quasi-municipal corporations and political subdivisions, and all

1 agencies of such corporations and subdivisions authorized to contract  
2 separately.

3 ~~((14))~~ (16) "Malicious cyber activities" means activities,  
4 other than those authorized by or in accordance with state and  
5 federal law, that seek to compromise or impair the confidentiality,  
6 integrity, or availability of computers, information or  
7 communications systems, networks, physical or virtual infrastructure  
8 controlled by computers or information systems, or information  
9 residing on those systems.

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

12 ~~((15))~~ (18) "Oversight" means a process of comprehensive risk  
13 analysis and management designed to ensure optimum use of information  
14 technology resources and telecommunications.

15 ~~((16))~~ (19) "Proprietary software" means that software offered  
16 for sale or license.

17 ~~((17))~~ (20) "Public agency" means any agency of this state or  
18 another state; any political subdivision or unit of local government  
19 of this state or another state including, but not limited to,  
20 municipal corporations, quasi-municipal corporations, special purpose  
21 districts, and local service districts; any public benefit nonprofit  
22 corporation; any agency of the United States; and any Indian tribe  
23 recognized as such by the federal government.

24 ~~((18))~~ (21) "Public benefit nonprofit corporation" means a  
25 public benefit nonprofit corporation as defined in RCW 24.03A.245  
26 that is receiving local, state, or federal funds either directly or  
27 through a public agency other than an Indian tribe or political  
28 subdivision of another state.

29 ~~((19))~~ (22) "Public record" has the definitions in RCW  
30 42.56.010 and chapter 40.14 RCW and includes legislative records and  
31 court records that are available for public inspection.

32 ~~((20))~~ (23) "Public safety" refers to any entity or services  
33 that ensure the welfare and protection of the public.

34 ~~((21))~~ (24) "Ransomware" includes any type of malicious  
35 software code, executable, application, payload, or digital content  
36 designed to encrypt, steal, exfiltrate, delete, destroy, or deny  
37 access to any data, databases, systems, applications, networks, data  
38 centers, cloud computing environment, cloud service, or other mission  
39 critical or business essential infrastructure.

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

5        ~~((22))~~ (26) "State agency" means every state office,  
6 department, division, bureau, board, commission, or other state  
7 agency, including offices headed by a statewide elected official.

8        ~~((23))~~ (27) "Telecommunications" includes, but is not limited  
9 to, wireless or wired systems for transport of voice, video, and data  
10 communications, network systems, requisite facilities, equipment,  
11 system controls, simulation, electronic commerce, and all related  
12 interactions between people and machines.

13        ~~((24))~~ (28) "Utility-based infrastructure services" includes  
14 personal computer and portable device support, servers and server  
15 administration, security administration, network administration,  
16 telephony, email, and other information technology services commonly  
17 used by state agencies.

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

20        (1) The office shall design, develop, and implement enterprise  
21 technology standards specific to malware and ransomware protection,  
22 backup, and recovery, as well as prevention education for state  
23 employees and constituents who use state technology services. The  
24 office shall refer to the national institute of standards and  
25 technology (NIST) ransomware profile contained in the NIST ransomware  
26 *Risk Management: A Cybersecurity Framework Profile* published February  
27 2022, or its successor publication, as guidance to support the  
28 prevention of, response to, and recovery from, ransomware events.

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

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

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

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

12 (a) The total size of managed data;

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

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

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

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

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

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

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

35 (6) The reports produced and information compiled pursuant to  
36 this section are confidential, and may not be disclosed under chapter  
37 42.56 RCW.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

31        (vii) The breadth of threat landscape;

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

--- END ---