

---

**HOUSE BILL 2044**

---

**State of Washington**

**67th Legislature**

**2022 Regular Session**

**By** Representatives Boehnke, Hackney, Fitzgibbon, Kloba, Ormsby, Sutherland, Ramel, and Young

Read first time 01/19/22. Referred to Committee on State Government & Tribal Relations.

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 43.105.054 and 43.105.220; reenacting and amending RCW 43.105.020;  
5 adding new sections to chapter 43.105 RCW; adding a new section to  
6 chapter 42.56 RCW; creating new sections; and making an  
7 appropriation.

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

9 NEW SECTION. **Sec. 1.** Washington state branches of government,  
10 agencies, boards, and commissions manage and protect highly sensitive  
11 data in order to best serve constituents. The data managed by public  
12 entities is a high value target for domestic and international  
13 perpetrators of for-profit ransomware and other malicious cyber  
14 activities. Breaches in data security prevent state agencies from  
15 protecting confidential and sensitive information stored in  
16 technology systems. In the absence of immutable data backup  
17 capabilities and reliable disaster recovery practices, state agency  
18 information technology systems are vulnerable to such breaches in  
19 security. The legislature finds that enterprise technology programs,  
20 standards, and policies have been developed for data backup and  
21 recovery practices that agencies must implement to protect

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

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

15 (1) The office shall design, develop, and implement enterprise  
16 technology standards specific to malware and ransomware protection,  
17 backup, and recovery, as well as prevention education for state  
18 employees and constituents using state technology services, incident  
19 reporting, and incident response management and remediation.  
20 Enterprise technology standards must be reviewed annually.

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

24 (b) The office shall document, publish, and distribute ransomware  
25 response educational materials specifically for chief executive  
26 officers, chief financial officers, chief information officers, and  
27 chief information security officers, or their equivalents, to each  
28 state agency, board, and commission, which outlines specific steps to  
29 take in the event of a malware attack. Distribution of materials must  
30 be determined at the discretion of the office.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 The reports and information compiled pursuant to section 2 (7)  
26 and (8)(b) of this act are confidential and may not be disclosed  
27 under this chapter.

28 **Sec. 6.** RCW 43.105.020 and 2021 c 176 s 5223 and 2021 c 40 s 2  
29 are each reenacted and amended to read as follows:

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

- 32 (1) "Agency" means the consolidated technology services agency.  
33 (2) "Board" means the technology services board.  
34 (3) "Cloud computing" has the same meaning as provided by the  
35 special publication 800-145 issued by the national institute of  
36 standards and technology of the United States department of commerce  
37 as of September 2011 or its successor publications.

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

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

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

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

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

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

21 (a) Prevent improper information modification or destruction;

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

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

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

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

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

39 (12) "K-20 network" means the network established in RCW  
40 43.41.391.

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

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

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

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

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

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

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

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

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

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

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

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

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

18 (26) "Malicious cyber activities" means activities, other than  
19 those authorized by or in accordance with United States law, that  
20 seek to compromise or impair the confidentiality, integrity, or  
21 availability of computers, information or communications systems,  
22 networks, physical or virtual infrastructure controlled by computers  
23 or information systems, or information resident thereon.

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

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

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

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

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

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

39 (ii) Disposition of equipment;



1 (iii) Licensing of the radio spectrum by or on behalf of state  
2 agencies; and  
3 (iv) Confidentiality of computerized data;  
4 (b) To develop statewide and interagency technical policies,  
5 standards, and procedures;  
6 (c) To review and approve standards and common specifications for  
7 new or expanded telecommunications networks proposed by agencies,  
8 public postsecondary education institutions, educational service  
9 districts, or statewide or regional providers of K-12 information  
10 technology services;  
11 (d) With input from the legislature and the judiciary, to provide  
12 direction concerning strategic planning goals and objectives for the  
13 state;  
14 (e) To establish policies for the periodic review by the director  
15 of state agency performance which may include but are not limited to  
16 analysis of:  
17 (i) Planning, management, control, and use of information  
18 services;  
19 (ii) Training and education;  
20 (iii) Project management; and  
21 (iv) Cybersecurity, in coordination with the office of  
22 cybersecurity;  
23 (f) To coordinate with state agencies with an annual information  
24 technology expenditure that exceeds ten million dollars to implement  
25 a technology business management program to identify opportunities  
26 for savings and efficiencies in information technology expenditures  
27 and to monitor ongoing financial performance of technology  
28 investments;  
29 (g) In conjunction with the consolidated technology services  
30 agency, to develop statewide standards for agency purchases of  
31 technology networking equipment and services;  
32 (h) To implement a process for detecting, reporting, and  
33 responding to security incidents consistent with the information  
34 security standards, policies, and guidelines adopted by the director;  
35 (i) To develop plans and procedures to ensure the continuity of  
36 commerce for information resources that support the operations and  
37 assets of state agencies in the event of a security incident; ~~(and)~~  
38 (j) To design, develop, and implement enterprise technology  
39 standards specific to malware and ransomware protection, backup, and  
40 recovery; and

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

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

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

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

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

23        **Sec. 8.** RCW 43.105.220 and 2015 3rd sp.s. c 1 s 203 are each  
24 amended to read as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

34       (3) (a) By December 31, 2024, the office shall initiate a biannual  
35 report to the legislature, governor, and technology services board  
36 sharing information garnered from the agency reports that includes:

37       (i) The number of mission critical applications;

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

40       (iii) The number of business essential applications;

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

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

5 (vi) The number of applications containing either category 3 data  
6 or category 4 data, or both, with immutable backups;

7 (vii) The breadth of threat landscape;

8 (viii) A prioritized list of systems within the enterprise  
9 requiring immutable backups;

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

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

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

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

19 (b) These additional reporting requirements are not subject to  
20 public disclosure under chapter 42.56 RCW.

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

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

30 NEW SECTION. Sec. 10. The sum of \$5,000,000, or as much thereof  
31 as may be necessary, is appropriated for the fiscal year ending June  
32 30, 2023, from the general fund to the information technology  
33 security account created in section 4 of this act for the purposes of  
34 this act.

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

--- **END** ---