

---

**SUBSTITUTE SENATE BILL 5432**

---

**State of Washington**

**67th Legislature**

**2021 Regular Session**

**By** Senate Environment, Energy & Technology (originally sponsored by Senators Carlyle, Nguyen, Conway, Das, Dhingra, Keiser, Lias, Nobles, and Randall; by request of Office of the Governor)

READ FIRST TIME 02/12/21.

1 AN ACT Relating to cybersecurity in state government; adding new  
2 sections to chapter 43.105 RCW; adding a new section to chapter 39.26  
3 RCW; adding a new section to chapter 39.34 RCW; adding a new section  
4 to chapter 42.56 RCW; creating a new section; repealing RCW  
5 43.105.215; and providing an expiration date.

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

7 NEW SECTION. **Sec. 1.** A new section is added to chapter 43.105  
8 RCW to read as follows:

9 (1) The office of cybersecurity is created within the office of  
10 the chief information officer.

11 (2) The director shall appoint a state chief information security  
12 officer, who is the director of the office of cybersecurity.

13 (3) The primary duties of the office of cybersecurity are:

14 (a) To establish security standards and policies to protect the  
15 state's information technology systems and infrastructure, to provide  
16 appropriate governance and application of the standards and policies  
17 across information technology resources used by the state, and to  
18 ensure the confidentiality, availability, and integrity of the  
19 information transacted, stored, or processed in the state's  
20 information technology systems and infrastructure;

1 (b) To develop a centralized cybersecurity protocol for  
2 protecting and managing state information technology assets and  
3 infrastructure;

4 (c) To detect and respond to levels of security incidents  
5 consistent with information security standards and policies;

6 (d) To create a model incident response plan for agency adoption,  
7 with the office of cybersecurity as the incident response coordinator  
8 for incidents that: (i) Impact multiple agencies; (ii) impact more  
9 than 10,000 citizens; (iii) involve a nation state actor; or (iv) are  
10 likely to be in the public domain;

11 (e) To ensure the continuity of state business and information  
12 resources that support the operations and assets of state agencies in  
13 the event of a security incident;

14 (f) To provide formal guidance to agencies on leading practices  
15 and applicable standards to ensure a whole government approach to  
16 cybersecurity, which shall include, but not be limited to, guidance  
17 regarding: (i) The configuration and architecture of agencies'  
18 information technology systems, infrastructure, and assets; (ii)  
19 governance, compliance, and oversight; and (iii) incident  
20 investigation and response;

21 (g) To serve as a resource for local and municipal governments in  
22 Washington in the area of cybersecurity;

23 (h) To develop a service catalog of cybersecurity services to be  
24 offered to state and local governments;

25 (i) To collaborate with state agencies in developing standards,  
26 functions, and services in order to ensure state agency regulatory  
27 environments are understood and considered as part of an enterprise  
28 cybersecurity response;

29 (j) To define core services that must be managed by agency  
30 information technology security programs; and

31 (k) To perform all other matters and things necessary to carry  
32 out the purposes of this chapter.

33 (4) In performing its duties, the office of cybersecurity must  
34 address the highest levels of security required to protect  
35 confidential information transacted, stored, or processed in the  
36 state's information technology systems and infrastructure that is  
37 specifically protected from disclosure by state or federal law and  
38 for which strict handling requirements are required.

39 (5) In executing its duties under subsection (3) of this section,  
40 the office of cybersecurity shall use or rely upon existing, industry

1 standard, widely adopted cybersecurity standards, with a preference  
2 for United States federal standards.

3 (6) Each state agency, institution of higher education, the  
4 legislature, and the judiciary must develop an information technology  
5 security program consistent with the office of cybersecurity's  
6 standards and policies.

7 (7) (a) Each state agency information technology security program  
8 must adhere to the office of cybersecurity's security standards and  
9 policies. Each state agency must review and update its program  
10 annually, certify to the office of cybersecurity that its program is  
11 in compliance with the office of cybersecurity's security standards  
12 and policies, and provide the office of cybersecurity with a list of  
13 the agency's cybersecurity business needs and agency program metrics.

14 (b) The office of cybersecurity shall require a state agency to  
15 obtain an independent compliance audit of its information technology  
16 security program and controls at least once every three years to  
17 determine whether the state agency's information technology security  
18 program is in compliance with the standards and policies established  
19 by the agency and that security controls identified by the state  
20 agency in its security program are operating efficiently.

21 (c) If a review or an audit conducted under (a) or (b) of this  
22 subsection identifies any failure to comply with the standards and  
23 policies of the office of cybersecurity or any other material  
24 cybersecurity risk, the office of cybersecurity must require the  
25 state agency to formulate and implement a plan to resolve the failure  
26 or risk. On an annual basis, the office of cybersecurity must provide  
27 a confidential report to the governor identifying and describing the  
28 cybersecurity risk or failure to comply with the office of  
29 cybersecurity's security policy or implementing cybersecurity  
30 standards and policies, as well as the agency's plan to resolve such  
31 failure or risk. Risks that are not mitigated are to be tracked by  
32 the office of cybersecurity and reviewed with the governor on a  
33 quarterly basis. The report to the governor under this subsection is  
34 confidential and exempt from public inspection and copying under  
35 chapter 42.56 RCW.

36 (8) In the case of institutions of higher education, the  
37 judiciary, and the legislature, each information technology security  
38 program must be comparable to the intended outcomes of the office of  
39 cybersecurity's security standards and policies.

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

3        (1)    By July 1, 2022, the office of cybersecurity, in  
4 collaboration with state agencies, shall develop a catalog of  
5 cybersecurity services and functions for the office of cybersecurity  
6 to perform and submit a report to the legislature and governor. The  
7 report must include, but not be limited to:

8        (a)    Cybersecurity services and functions to include in the office  
9 of cybersecurity's catalog of services that should be performed by  
10 the office of cybersecurity;

11       (b)    Core capabilities and competencies of the office of  
12 cybersecurity;

13       (c)    Security functions which should remain within agency  
14 information technology security programs;

15       (d)    A recommended model for accountability of agency security  
16 programs to the office of cybersecurity; and

17       (e)    The cybersecurity services and functions required to protect  
18 confidential information transacted, stored, or processed in the  
19 state's information technology systems and infrastructure that is  
20 specifically protected from disclosure by state or federal law and  
21 for which strict handling requirements are required.

22       (2)    The office of cybersecurity shall update and publish its  
23 catalog of services and performance metrics on a biennial basis. The  
24 office of cybersecurity shall use data and information provided from  
25 agency security programs to inform the updates to its catalog of  
26 services and performance metrics.

27       (3)    To ensure alignment with enterprise information technology  
28 security strategy, the office of cybersecurity shall develop a  
29 process for reviewing and evaluating agency proposals for additional  
30 cybersecurity services consistent with RCW 43.105.255.

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

33       (1)    In the event of a major cybersecurity incident, state  
34 agencies must report that incident to the office of cybersecurity  
35 within 24 hours of discovery of the incident.

36       (2)    State agencies must provide the office of cybersecurity with  
37 contact information for any external parties who have material  
38 information related to the cybersecurity incident.

1 (3) Once a cybersecurity incident is reported to the office of  
2 cybersecurity, the office of cybersecurity must investigate the  
3 incident to determine the degree of severity and facilitate an  
4 enterprise incident response to the extent permitted by other state  
5 and federal requirements.

6 (4) The chief information security officer or the chief  
7 information security officer's designee shall serve as the state's  
8 point of contact for all major cybersecurity incidents to the extent  
9 permitted by other state and federal requirements.

10 (5) The office of cybersecurity must create policy to implement  
11 this section.

12 NEW SECTION. **Sec. 4.** (1) The office of cybersecurity, in  
13 collaboration with the office of privacy and data protection and the  
14 office of the attorney general, shall research and examine existing  
15 best practices for data governance, data protection, the sharing of  
16 data relating to cybersecurity, and the protection of state and local  
17 governments' information technology systems and infrastructure  
18 including, but not limited to, model terms for data sharing contracts  
19 and adherence to privacy principles.

20 (2) The office of cybersecurity must submit a report of its  
21 findings and identify specific recommendations to the governor and  
22 the appropriate committees of the legislature by December 1, 2021.

23 (3) This section expires December 31, 2021.

24 NEW SECTION. **Sec. 5.** A new section is added to chapter 39.26  
25 RCW to read as follows:

26 (1) Before an agency sharing category 3 or higher data as defined  
27 in policy authorized under RCW 43.105.054, with another agency, a  
28 written data sharing agreement must be in place. Such agreements  
29 shall conform to the policies for data sharing specified by the  
30 office of cybersecurity under the authority of RCW 43.105.054.

31 (2) Nothing in this chapter shall be construed as limiting audit  
32 authorities under chapter 43.09 RCW.

33 NEW SECTION. **Sec. 6.** A new section is added to chapter 39.34  
34 RCW to read as follows:

35 (1) If a public agency is requesting from another public agency  
36 category 3 or higher data as defined in policy authorized under RCW  
37 43.105.054, the requesting agency shall provide for a written

1 agreement between the agencies that conforms to the policies of the  
2 office of cybersecurity.

3 (2) Nothing in this chapter shall be construed as limiting audit  
4 authorities under chapter 43.09 RCW.

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

7 Reports submitted by the office of cybersecurity to the  
8 governor's office in accordance with the requirements under section 1  
9 (7)(c) of this act are exempt from disclosure under this chapter.

10 NEW SECTION. **Sec. 8.** RCW 43.105.215 (Security standards and  
11 policies—State agencies' information technology security programs)  
12 and 2015 3rd sp.s. c 1 s 202 & 2013 2nd sp.s. c 33 s 8 are each  
13 repealed.

--- END ---