

CERTIFICATION OF ENROLLMENT
ENGROSSED SUBSTITUTE SENATE BILL 5432

Chapter 291, Laws of 2021

67th Legislature
2021 Regular Session

OFFICE OF CYBERSECURITY

EFFECTIVE DATE: July 25, 2021

Passed by the Senate April 15, 2021
Yeas 48 Nays 0

DENNY HECK

President of the Senate

Passed by the House April 6, 2021
Yeas 83 Nays 15

Laurie Jinkins

**Speaker of the House of
Representatives**

Approved May 12, 2021 3:12 PM

JAY INSLEE

Governor of the State of Washington

CERTIFICATE

I, Brad Hendrickson, Secretary of the Senate of the State of Washington, do hereby certify that the attached is **ENGROSSED SUBSTITUTE SENATE BILL 5432** as passed by the Senate and the House of Representatives on the dates hereon set forth.

BRAD HENDRICKSON

Secretary

FILED

May 12, 2021

**Secretary of State
State of Washington**

ENGROSSED SUBSTITUTE SENATE BILL 5432

AS AMENDED BY THE HOUSE

Passed Legislature - 2021 Regular Session

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; amending
2 RCW 43.105.054; adding new sections to chapter 43.105 RCW; adding a
3 new section to chapter 39.26 RCW; adding a new section to chapter
4 39.34 RCW; adding a new section to chapter 42.56 RCW; creating new
5 sections; repealing RCW 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 security incidents consistent with
5 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 and appropriate committees of
28 the legislature identifying and describing the cybersecurity risk or
29 failure to comply with the office of cybersecurity's security policy
30 or implementing cybersecurity standards and policies, as well as the
31 agency's plan to resolve such failure or risk. Risks that are not
32 mitigated are to be tracked by the office of cybersecurity and
33 reviewed with the governor and the chair and ranking member of the
34 appropriate committees of the legislature on a quarterly basis.

35 (d) The reports produced, and information compiled, pursuant to
36 this subsection (7) are confidential and may not be disclosed under
37 chapter 42.56 RCW.

38 (8) In the case of institutions of higher education, the
39 judiciary, and the legislature, each information technology security

1 program must be comparable to the intended outcomes of the office of
2 cybersecurity's security standards and policies.

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

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

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

13 (b) Core capabilities and competencies of the office of
14 cybersecurity;

15 (c) Security functions which should remain within agency
16 information technology security programs;

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

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

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

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

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

35 (1) In the event of a major cybersecurity incident, as defined in
36 policy established by the office of cybersecurity in accordance with
37 section 1 of this act, state agencies must report that incident to

1 the office of cybersecurity within 24 hours of discovery of the
2 incident.

3 (2) State agencies must provide the office of cybersecurity with
4 contact information for any external parties who may have material
5 information related to the cybersecurity incident.

6 (3) Once a cybersecurity incident is reported to the office of
7 cybersecurity, the office of cybersecurity must investigate the
8 incident to determine the degree of severity and facilitate any
9 necessary incident response measures that need to be taken to protect
10 the enterprise.

11 (4) The chief information security officer or the chief
12 information security officer's designee shall serve as the state's
13 point of contact for all major cybersecurity incidents.

14 (5) The office of cybersecurity must create policy to implement
15 this section.

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

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

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

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

30 (1) Before an agency shares with a contractor category 3 or
31 higher data, as defined in policy established in accordance with RCW
32 43.105.054, a written data-sharing agreement must be in place. Such
33 agreements shall conform to the policies for data sharing specified
34 by the office of cybersecurity under the authority of RCW 43.105.054.

35 (2) Nothing in this section shall be construed as limiting audit
36 authorities under chapter 43.09 RCW.

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

3 (1) If a public agency is requesting from another public agency
4 category 3 or higher data, as defined in policy established in
5 accordance with RCW 43.105.054, the requesting agency shall provide
6 for a written agreement between the agencies that conforms to the
7 policies of the office of cybersecurity.

8 (2) Nothing in this section shall be construed as limiting audit
9 authorities under chapter 43.09 RCW.

10 NEW SECTION. **Sec. 7.** (1) The office of cybersecurity shall
11 contract for an independent security assessment of the state agency
12 information technology security program audits, required under
13 section 1 of this act, that have been conducted since July 1, 2015.
14 The independent assessment must be conducted in accordance with
15 subsection (2) of this section. To the greatest extent practicable,
16 the office of cybersecurity must contract for the independent
17 security assessment using a department of enterprise services master
18 contract or the competitive solicitation process described under
19 chapter 39.26 RCW. If the office of cybersecurity conducts a
20 competitive solicitation, the office of cybersecurity shall work with
21 the department of enterprise services, office of minority and women's
22 business enterprises, and the department of veterans affairs to
23 engage in outreach to Washington small businesses, as defined in RCW
24 39.26.010, and certified veteran-owned businesses, as described in
25 RCW 43.60A.190, and encourage these entities to submit a bid.

26 (2) The assessment must, at a minimum:

27 (a) Review the state agency information technology security
28 program audits, required under section 1 of this act, performed since
29 July 1, 2015;

30 (b) Assess the content of any audit findings and evaluate the
31 findings relative to industry standards at the time of the audit;

32 (c) Evaluate the state's performance in taking action upon audit
33 findings and implementing recommendations from the audit;

34 (d) Evaluate the policies and standards established by the office
35 of cybersecurity pursuant to section 1 of this act and provide
36 recommendations for ways to improve the policies and standards; and

37 (e) Include recommendations, based on best practices, for both
38 short-term and long-term programs and strategies designed to
39 implement audit findings.

1 (3) A report detailing the elements of the assessment described
2 under subsection (2) of this section must be submitted to the
3 governor and appropriate committees of the legislature by August 31,
4 2022. The report is confidential and may not be disclosed under
5 chapter 42.56 RCW.

6 NEW SECTION. **Sec. 8.** A new section is added to chapter 42.56
7 RCW to read as follows:

8 The reports and information compiled pursuant to sections 1 and 7
9 of this act are confidential and may not be disclosed under this
10 chapter.

11 **Sec. 9.** RCW 43.105.054 and 2016 c 237 s 3 are each amended to
12 read as follows:

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

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

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

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

20 (ii) Disposition of equipment;

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

23 (iv) Confidentiality of computerized data;

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

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

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

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

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

1 (ii) Training and education;

2 (iii) Project management; and

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

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

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

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

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

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

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

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

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

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

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

Passed by the Senate April 15, 2021.

Passed by the House April 6, 2021.

Approved by the Governor May 12, 2021.

Filed in Office of Secretary of State May 12, 2021.

--- END ---