CERTIFICATION OF ENROLLMENT

ENGROSSED SUBSTITUTE SENATE BILL 5432

67th Legislature
2021 Regular Session

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

President of the Senate

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

Speaker of the House of Representatives

Approved

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.

Secretary

FILED

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, Liias, Nobles, and Randall; by request of Office of the Governor)

READ FIRST TIME 02/12/21.

AN ACT Relating to cybersecurity in state government; amending RCW 43.105.054; adding new sections to chapter 43.105 RCW; adding a new section to chapter 39.26 RCW; adding a new section to chapter 39.34 RCW; adding a new section to chapter 42.56 RCW; creating new sections; repealing RCW 43.105.215; and providing an expiration date.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(c) If a review or an audit conducted under (a) or (b) of this subsection identifies any failure to comply with the standards and policies of the office of cybersecurity or any other material cybersecurity risk, the office of cybersecurity must require the state agency to formulate and implement a plan to resolve the failure or risk. On an annual basis, the office of cybersecurity must provide a confidential report to the governor and appropriate committees of the legislature identifying and describing the cybersecurity risk or failure to comply with the office of cybersecurity's security policy or implementing cybersecurity standards and policies, as well as the agency's plan to resolve such failure or risk. Risks that are not mitigated are to be tracked by the office of cybersecurity and reviewed with the governor and the chair and ranking member of the appropriate committees of the legislature on a quarterly basis.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) This section expires December 31, 2021.

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

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

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

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

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

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

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

(2) The assessment must, at a minimum:

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

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

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

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

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

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

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

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

Sec. 9. RCW 43.105.054 and 2016 c 237 s 3 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 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.

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

--- END ---