ENGROSSED 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, 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; 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 new sections 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 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 on a quarterly basis. The report to the governor under this subsection is confidential and exempt from public inspection and copying 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, 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 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 category 3 or higher data as defined in policy authorized under RCW 43.105.054, with a contractor, 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 authorized under 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 financial management shall contract for an independent security evaluation audit of state agency information technology in the state of Washington. The independent third party must audit the security and protection of digital assets for the state of Washington to test and assess the overall security posture including, but not limited to, cybersecurity.

(2) The audit must, at a minimum:

(a) Define threats, and include recommendations to mitigate the threats to include real-time security assessments of applications, systems, and networks to identify and assess risks and determine if they could be exploited by bad actors;

(b) Review security protocols and identify flaws in both physical and digital systems, to include data transfers;

(c) Assess the current security performance of existing security structures, to include penetration testing;

(d) Prioritize and complete risk scoring of identified threats and risks; and

(e) Formulate security solutions with estimated costs, to include what can be achieved in the short term, or less than 12 months, and what can be achieved in the mid to long term.

(3) The independent audit team must include the chair and ranking member of the senate environment, energy, and technology committee and two members of the house of representatives in executive briefings throughout the audit, and the four members must be updated, at least monthly, on the progress of the audit.

(4) The security evaluation audit report must be submitted to the fiscal committees of the legislature by August 31, 2022.

(5) Reports shared and submitted by the independent audit team, the office of financial management, and the office of cybersecurity to the members identified in subsections (3) and (4) of this section are exempt from disclosure under chapter 42.56 RCW.

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

Reports shared and submitted by the independent audit team, the office of financial management, and the office of cybersecurity to the members identified in section 7 (3) and (4) of this act in accordance with the requirements in section 7 of this act are exempt from disclosure under this chapter.

NEW SECTION. **Sec. 9.** A new section is added to chapter 42.56 RCW to read as follows:

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

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 ---