Z-0236.3

SENATE BILL 5432

State of Washington 67th Legislature 2021 Regular Session

By Senators Carlyle, Nguyen, Conway, Das, Dhingra, Keiser, Liias, Nobles, and Randall; by request of Office of the Governor

Read first time 02/08/21. Referred to Committee on Environment, Energy & Technology.

AN ACT Relating to cybersecurity in state government; adding new sections to chapter 43.105 RCW; creating a new section; 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 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;

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

(d) 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;

(e) To provide formal guidance to agencies on leading practices and standards to ensure a whole government approach to cybersecurity;

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

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

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

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

(4) Each state agency, institution of higher education, the legislature, and the judiciary must develop an information technology security program.

(5)(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 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.

(6) 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; and

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

(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 coordinate incident response.

(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 cybersecurity incidents.

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

NEW SECTION. **Sec. 4.** (1) The office of privacy and data protection, in collaboration with the office of the attorney general, shall research and examine existing best practices for data governance and data protection including but not limited to model terms for data sharing contracts and adherence to privacy principles.

(2) The office of privacy and data protection 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.** 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 ---