SENATE BILL REPORT
ESSB 5432

As Amended by House, April 6, 2021

Title: An act relating to cybersecurity in state government.

Brief Description: Concerning cybersecurity and data sharing in Washington state government.

Sponsors: Senate Committee on Environment, Energy & Technology (originally sponsored by Senators Carlyle, Nguyen, Conway, Das, Dhingra, Keiser, Liias, Nobles and Randall; by request of Office of the Governor).

Brief History:

Committee Activity: Environment, Energy & Technology: 2/09/21, 2/11/21 [DPS-WM, DNP].

Floor Activity: Passed Senate: 2/24/21, 49-0.
Passed House: 4/6/21, 83-15.

Brief Summary of Engrossed First Substitute Bill

- Creates the Office of Cybersecurity within the Office of the Chief Information Officer.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Majority Report: That Substitute Senate Bill No. 5432 be substituted therefor, and the substitute bill do pass and be referred to Committee on Ways & Means.

Signed by Senators Carlyle, Chair; Lovelett, Vice Chair; Das, Fortunato, Hobbs, Liias, Nguyen, Sheldon, Short, Stanford and Wellman.

Minority Report: Do not pass.
Signed by Senator Ericksen, Ranking Member.

Staff: Angela Kleis (786-7469)

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

Background: State Information Technology. *General.* The Consolidated Technology Services Agency, also known as WaTech, supports state agencies as a centralized provider and procurer of information technology (IT) services. The director of WaTech is the state Chief Information Officer (CIO). Within WaTech, the Office of the Chief Information Officer (OCIO) has primary duties related to IT for state government, which include establishing statewide enterprise architecture and standards.

Cybersecurity. The OCIO establishes security standards and policies to ensure the integrity of the information processed in the state's IT systems. The CIO appoints the state Chief Information Security Officer (CISO). Each institution of higher education, the Legislature, and the judiciary must develop an IT security program (program) that is comparable to the intended outcomes of OCIO security standards and policies. Each state agency must develop a program, ensure it adheres to OCIO security standards and policies, and obtain an independent compliance audit of the program at least once every three years.

Office of the Chief Information Officer Policies. The OCIO policy on securing IT assets requires agencies to implement common IT security standards. A component of this policy outlines data security requirements such as data classification. Agencies must classify data based on the sensitivity of the data. Data must be translated to the following classification categories:

- category 1: public information;
- category 2: sensitive information;
- category 3: confidential information; and
- category 4: confidential information requiring special handling.

Agencies must ensure any sharing of data with the public complies with OCIO policies and other applicable regulations. When sharing category 3 and above data outside of the agency, an agreement must be in place unless otherwise prescribed by law. Encryption standards for category 3 and 4 data are specified. Agencies must appropriately protect information transmitted electronically.

Summary of Engrossed First Substitute Bill: Office of Cybersecurity. The Office of Cybersecurity (OCS) is created within the OCIO. The CIO appoints the CISO. The primary duties of the OCS are specified, such as establishing security standards and policies and developing a centralized cybersecurity protocol for managing state IT assets.

Programs required under current law must adhere to or be comparable to security standards and policies established by the OCS rather than the OCIO. Current independent compliance audit requirements are maintained. If the audit identifies any failure to comply with standards or any other material cybersecurity risk, the OCS must require the agency to implement a plan to resolve the failure and monitor compliance.

Catalog of Services. By July 1, 2022, the OCS, in collaboration with state agencies, must develop a catalog of cybersecurity services and functions for the OCS to perform, and

submit a report to the Governor and the Legislature. The OCS shall update and publish its catalog of services and performance metrics on a biennial basis.

Incident Response. In the event of a major cybersecurity incident, state agencies must report that incident to the OCS within 24 hours of discovery of the incident. State agencies must provide the OCS with contact information for any external parties with material information related to the incident. The OCS must investigate the incident to determine the degree of severity and must serve as the state's point of contact for all major cybersecurity incidents.

Report on Data Governance. The OCS, in collaboration with the Office of Privacy and Data Protection and the Office of the Attorney General, shall research existing best practices for data governance and data protection, including model terms for data sharing contracts, and submit a report to the Legislature by December 1, 2021.

Data Sharing Agreements. Before an agency shares or requests category 3 or higher data, a written data sharing agreement that conforms to OCS policies must be in place. This requirement does not limit audit authorities of the State Auditor.

Independent Security Audit. The Office of Financial Management must contract for an independent security evaluation audit of state agency IT. The independent audit team must include legislative members, who must be updated on the progress of the audit. The security evaluation must be submitted to the fiscal committees of the Legislature by August 31, 2022.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony on Original Bill: *The committee recommended a different version of the bill than what was heard.* PRO: Cybersecurity should not be decentralized. This bill provides a strong new tool for privacy protections that will not interfere with Constitutional requirements relative to audits. This bill enables collaboration and improves the state's cybersecurity posture by providing clear guidelines and targets.

Persons Testifying: PRO: Senator Reuven Carlyle, Prime Sponsor; Scott Nelson, State Auditor's Office; Sheri Sawyer, Governor's Policy Office; James Weaver, WaTech.

Persons Signed In To Testify But Not Testifying: No one.

EFFECT OF HOUSE AMENDMENT(S):

- Modifies the entities that receive the reports and briefings relating to agency information technology security program audits to include appropriate committees of the Legislature.
- Specifies a "major cybersecurity incident" is defined in policy established by the OCS.
- Removes the requirement that the Office of Financial Management contract for an independent security audit of state agency information technology, and instead requires the OCS to contract for an independent security assessment of the state agency information technology security program audits that have been conducted since July 1, 2015.
- Requires the OCS, in contracting for the assessment, to use a Department of Enterprise Services master contract or the competitive solicitation process.
- Requires the OCS, if engaging in a competitive solicitation process to contract for the assessment, to work with certain agencies to engage in outreach to veteran-owned businesses and small businesses, including minority and women owned businesses, and encourage these entities to submit a bid.
- Requires a report summarizing findings and recommendations from the assessment of state agency information technology security program audits to be submitted to the Governor and appropriate committees of the Legislature by August 31, 2022.
- Specifies information, in addition to the reports, compiled pertaining to the state agency information technology security program reviews and audits are confidential and may not be disclosed under the Public Records Act (PRA); and the reports and information compiled pertaining to the assessments of the state agency information technology security program audits are confidential and may not be disclosed under the PRA.