SENATE BILL REPORT
SB 5432

As of February 9, 2021

Title: An act relating to cybersecurity in state government.

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

Sponsors: 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.

Brief Summary of Bill

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

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Staff: Angela Kleis (786-7469)

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.

State Privacy Office. Within the OCIO, the Office of Privacy and Data Protection (OPDP) serves as a central point of contact for state agencies on policy matters involving data privacy and data protection. The OPDP also serves as a resource to local governments and the public on data privacy and protection concerns.

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.

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.

Summary of 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.

Each institution of higher education, the Legislature, and the judiciary must develop a program that is comparable to the intended outcomes of OCS security standards and policies. Each state agency must develop a program, ensure it adheres to OCS security standards and policies, and obtain an independent compliance audit of the program at least once every three years.

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 cybersecurity incidents.

Report on Data Governance. The OPDP, in collaboration with 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.

Appropriation: None.

Fiscal Note: Requested on February 6, 2021.

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: 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.