FINAL BILL REPORT
ESSB 5432

C 291 L 21
Synopsis as Enacted

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).

Senate Committee on Environment, Energy & Technology
House Committee on State Government & Tribal Relations
House Committee on Appropriations

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) 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;

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.

- 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.

Procurement. The Department of Enterprise Services (DES) is responsible for the development and oversight of policy for the procurement of goods and services by all state agencies, including procurement processes for IT goods and services.

The DES Director (Director) must adopt rules, policies, and guidelines governing procurement. The Director has the sole authority to:

- enter into master contracts on behalf of the state; and
- delegate authorization to purchase goods and services to agencies:
    1. Such authorization must specify restrictions as to dollar amount or specific types of goods and services, based on a risk assessment process.
    2. Delegation does not exempt the agency from conformance to the policies established by the Director.

DES also adopts uniform policies and procedures for the effective and efficient management of contracts by all state agencies. All contracts for purchases of goods and services must be based on a competitive solicitation process. DES may grant exemptions from competitive solicitation, including emergency contracts, sole source contracts, and direct buy purchases.

Summary: 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 protecting and 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 Assessment. The OCS must contract for an independent security assessment (assessment) of the statutorily required program audits conducted since July 1, 2015. Minimum assessment requirements are specified such as assessing the context of any audit findings and evaluating the findings relative to industry standards at the time of the audit, evaluating the state's performance in taking action upon audit findings, and evaluating policies and standards established by the OCS.

A report of the assessment must be submitted to the Governor and Legislature by August 31, 2022. The report is confidential and not subject to public disclosure. To the greatest extent practicable, the OCS must contract for the assessment using a DES master contract or the competitive solicitation process described under current law. If the OCS conducts a competitive solicitation, it must work with DES, the Office of Minority and Women's Business Enterprises, and the Department of Veteran's Affairs to engage outreach to small businesses and certified veteran-owned businesses and encourage these entities to submit a bid.

Votes on Final Passage:

Senate	49	0	
House	83	15	(House amended)
Senate	48	0	(Senate concurred)

Effective: July 25, 2021