SENATE BILL REPORT
SB 5518

As of February 2, 2023

Title: An act relating to the protection of critical constituent and state operational data against the financial and personal harm caused by ransomware and other malicious cyber activities.

Brief Description: Concerning the protection of critical constituent and state operational data against the financial and personal harm caused by ransomware and other malicious cyber activities.

Sponsors: Senators Boehnke, Stanford, MacEwen, Muzzall, Fortunato, Frame, Kuderer, Valdez, Warnick and Wellman.

Brief History:
Committee Activity: Environment, Energy & Technology: 2/03/23.

Brief Summary of Bill

- Requires the Office of the Chief Information Officer (OCIO) to implement enterprise technology standards specific to malware and ransomware protection, backup, and recovery; establish a ransomware education and outreach program; and distribute malware and ransomware response educational materials to each state agency.
- Requires each state agency to ensure all mission critical applications, business essential applications, and other resources containing category 3 or category 4 data have immutable backups and report specified data to the OCIO.
- Authorizes the state chief information officer, with the approval of the Technology Services Board, to expend up to $5,000,000 per fiscal biennium to provide funding to state agencies for procuring immutable data backup and disaster recovery services for mission critical application, business essential applications, or other critical information technology systems, containing category 3 or category 4 data.

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.

Staff: Angela Kleis (786-7469)

Background: State Information Technology. *General.* The Consolidated Technology Services Agency, also known as Washington Technology Services (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.

Policy and Standard. OCIO policy and standard on securing IT assets require 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 its sensitivity. 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.

Another component of this policy specifies data and program backup requirements such as implementing procedures for periodic tests to restore agency data from backup media, testing recovery procedure for critical systems as specified in the agency IT Security Program, and establishing methods to secure their backup media.

Technology Services Board. The Technology Services Board (TSB) is created within WaTech. Membership is composed of legislators and representatives from state and local government and the private sector. The TSB has specified powers and duties related to information services including to review and approve standards and policies developed by the OCIO and provide oversight of major IT projects.

Public Records Act. Under the Public Records Act (PRA), all state and local agencies must make all public records available for public inspection and copying, unless a specific exemption in the PRA or another statute applies. The PRA must be liberally construed and its exemptions narrowly construed to promote a general public policy favoring disclosure.

Summary of Bill: The Office of the Chief Information Officer's Responsibilities. The OCIO:

- must implement enterprise technology standards specific to malware and ransomware protection, backup, and recovery;
- establish a ransomware education and outreach program dedicated to educating public agencies;
- must distribute malware and ransomware response educational materials to each state agency as specified.

State Agency Responsibilities. Each state agency, excluding institutions of higher education, must ensure all mission critical applications, business essential applications, and other resources containing category 3 or category 4 data have immutable backups.

By September 30, 2023, and biannually thereafter, each state agency must review all of its mission critical applications, business essential applications, and other resources containing category 3 or category 4 data and report to the OCIO the certain data, such as a list of applications, that have and do not have immutable backup.

By March 31, 2024, state agencies must ensure all mission critical applications, business essential applications, and other resources containing category 3 or category 4 data are compliant with the reporting requirement and report to the OCIO whether they are in compliance. If any state agency reasonably anticipates it cannot comply with this requirement, it must submit a plan to the OCIO by March 31, 2024, detailing steps it will take to comply.

Report to the Technology Service Board. By December 31, 2024, and biannually thereafter, the OCIO must provide an oral report to the members of the TSB during an executive session which is closed to the public, the chairs and ranking members of the appropriate fiscal committees of the Legislature, and the appropriate policy staff in the Office of the Governor. The oral report must include certain information regarding mission critical applications, business essential applications, and other resources containing category 3 or category 4 data.

Consolidated Technology Services Revolving Account. In addition to current statutory authority to approve expenditures from the Consolidated Technology Services Revolving Account, the state CIO, with the approval of the TSB, is authorized to expend up to $5,000,000 per fiscal biennium for the TSB to provide funding to state agencies for procuring immutable data backup and disaster recovery services for mission critical application, business essential applications, or other critical IT systems, containing category 3 or category 4 data.

Public Records Act Exemption. The reports produced and information compiled pursuant to this act are confidential and may not be disclosed under the PRA.

Appropriation: None.

Fiscal Note: Requested on January 22, 2023.

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

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