SENATE BILL REPORT
SB 5518

As of February 20, 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. [**Revised for 1st Substitute:** Concerning cybersecurity.]

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

Brief History:
Committee Activity: Environment, Energy & Technology: 2/03/23, 2/14/23 [DPS-WM]. Ways & Means: 2/20/23.

Brief Summary of First Substitute Bill

- Establishes the Cybersecurity Advisory Committee as a subcommittee of the Emergency Management Council.
- Creates the Technology Services Board Security Subcommittee within the Technology Services Board.
- Expands the Department of Commerce's authority regarding energy-related activities to include preparing and updating contingency plans for securing energy infrastructure against all physical and cybersecurity threats.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Majority Report: That Substitute Senate Bill No. 5518 be substituted therefor, and the substitute bill do pass and be referred to Committee on Ways & Means.

Signed by Senators Nguyen, Chair; Lovelett, Vice Chair; MacEwen, Ranking Member;

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.

Boehnke, Lovick, Short, Trudeau and Wellman.

Staff: Angela Kleis (786-7469)

SENATE COMMITTEE ON WAYS & MEANS

Staff: Sarian Scott (786-7729)

Background: Emergency Management Council. The Emergency Management Council (EMC), established within the state Military Department, advises the Governor and the adjutant general on all matters pertaining to state and local emergency management. The EMC must ensure the Governor receives an annual assessment of statewide emergency preparedness and review administrative rules governing state and local emergency management practices and recommend necessary revisions to the adjutant general.

Technology Services Board. 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. Within WaTech, the Office of the Chief Information Officer (OCIO) has primary duties related to IT for state government such as establishing statewide enterprise architecture and standards.

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.

Department of Commerce. The Department of Commerce (Commerce) must supervise and administer energy-related activities as specified under current law. Commerce's authority includes preparing and updating contingency plans for implementation in the event of energy shortages or emergencies and serving as the official state agency responsible for coordinating implementation of the state energy strategy.

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 (First Substitute): Advisory Committee. The Cybersecurity Advisory Committee (committee) is established within the EMC to provide advice and recommendations that strengthen cybersecurity in both industry and public sectors across all critical infrastructure sectors. The committee must bring together organizations with expertise and responsibility for cybersecurity and incident response. The committee must meet quarterly.

With regards to critical infrastructure, the committee must work with relevant federal agencies, institutions of higher education, industry experts, and technical specialists for specified purposes such as assessing critical infrastructure not covered by federal law to identify which sectors are at the greatest risk and examining the inconsistencies between state and federal law regarding cybersecurity.

Security Subcommittee. The TSB Security Subcommittee (subcommittee) is created. Membership of the subcommittee is comprised of a subset of members appointed to the TSB. The chair may make additional appointments to ensure relevant technology sectors are represented. The subcommittee must meet quarterly.

The specified powers and duties of the subcommittee include reviewing emergent cyberattacks and threats to critical infrastructure sectors in order to identify existing gaps in state agency cybersecurity policies and assessing emerging risks to state agency IT. When providing staff support, WaTech must work with certain entities representing technology and government sectors to ensure a holistic approach to cybersecurity in state government.

Collaboration and Joint Report. When fulfilling the duties specified in the bill, the Military Department, the committee, WaTech, and the subcommittee must collaborate with each other. Once a year, the committee and subcommittee must hold a joint meeting.

By December 1, 2023, and each December 1st thereafter, the Military Department and WaTech are jointly responsible for providing a state of cybersecurity report to the Governor and the appropriate committees of the Legislature specifying recommendations considered necessary to address cybersecurity in the state.

Commerce Authority. Commerce's authority regarding energy-related activities is expanded to include preparing and updating contingency plans for securing energy infrastructure against all physical and cybersecurity threats.

Confidentiality. In order to discuss sensitive security topics and information, the committee and subcommittee may hold a portion of its agendas in executive session closed to the public. The reports produced and information compiled by the committee and subcommittee are confidential and may not be disclosed under the PRA.

EFFECT OF CHANGES MADE BY ENVIRONMENT, ENERGY & TECHNOLOGY COMMITTEE (First Substitute):

- Changes the title.
- Removes all provisions of the underlying bill.
- Provides a definition for ransomware.
- Establishes the Cybersecurity Advisory Committee within the Emergency Management Council.

- Establishes the TSB Security Subcommittee within WaTech.
- Requires the Military Department, the Cybersecurity Advisory Committee, WaTech, and the TSB Security Subcommittee to collaborate.
- Specifies the Military Department and WaTech are jointly responsible for providing a state of cybersecurity report specifying recommendations considered necessary to address cybersecurity in the state.
- Expands Commerce's authority regarding energy-related activities to include preparing and updating contingency plans for securing energy infrastructure against all physical and cybersecurity threats.
- Makes technical corrections.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: Yes.

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

Staff Summary of Public Testimony on Original Bill (Environment, Energy & Technology): *The committee recommended a different version of the bill than what was heard.* PRO: This bill establishes an internal process based on best practices to prevent ransomware attacks that devastate local communities and protect the collection and security of constituent's data. It creates an area where we can support WaTech and the work it is doing. A recent auditor's report identified gaps in agency compliance with current security policies. We are a data and technology leading state, and we need transparency and funding to address the issues included in the report.

OTHER: The use of backups and their role in disaster recovery are important parts of an IT organization's operating model and provide many benefits and protections to ensure availability of state services in the event of a cybersecurity incident. To meet the deadlines and reporting requirements, WaTech may have to reprioritize some of its statewide program initiatives.

Persons Testifying (Environment, Energy & Technology): PRO: Senator Matt Boehnke, Prime Sponsor.

OTHER: Derek Puckett, Consolidated Technology Services (WaTech).

Persons Signed In To Testify But Not Testifying (Environment, Energy & Technology): No one.

Staff Summary of Public Testimony (Ways & Means): PRO: Cybersecurity is a big effort. There are disconnects across state policy. Centralize and work on plans given

increases in cybersecurity events. The state of Washington would like to close the gaps and refine the technology with other agencies to protect everyone from cybersecurity threats.

Persons Testifying (Ways & Means): PRO: Senator Matt Boehnke, Prime Sponsor.

Persons Signed In To Testify But Not Testifying (Ways & Means): No one.