HOUSE BILL REPORT
2SSB 5518

As Reported by House Committee On:
State Government & Tribal Relations

Title: An act relating to cybersecurity.

Brief Description: Concerning cybersecurity.

Sponsors: Senate Committee on Ways & Means (originally sponsored by Senators Boehnke, Stanford, MacEwen, Muzzall, Fortunato, Frame, Kuderer, Valdez, Warnick and Wellman).

Brief History:
Committee Activity:
State Government & Tribal Relations: 3/14/23, 3/22/23 [DP].

Brief Summary of Second Substitute Bill

- Establishes the Cybersecurity Advisory Committee as a subcommittee of the Emergency Management Council to provide advice and recommendations that strengthen cybersecurity in both private and public sectors across all critical infrastructure sectors.
- Creates the Technology Services Board Security Subcommittee within the Technology Services Board to make various assessments and recommendations related to state cybersecurity policy, developing a shared notification system, and data breach training exercises.
- Expands the duties and powers of the Department of Commerce to include preparing and updating contingency plans for securing energy infrastructure against all physical and cybersecurity threats.

HOUSE COMMITTEE ON STATE GOVERNMENT & TRIBAL RELATIONS

Majority Report: Do pass. Signed by 7 members: Representatives Ramos, Chair; Stearns, Vice Chair; Abbarno, Ranking Minority Member; Christian, Assistant Ranking

---

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.

Minority Member; Gregerson, Low and Mena.

Staff: Desiree Omli (786-7105).

Background:

Emergency Management Council.
The Emergency Management Council (Council) advises the Governor and Adjutant General on all matters pertaining to state and local emergency management. The Council provides the Governor with an annual assessment of statewide emergency preparedness including progress on hazard mitigation and reduction efforts, seismic safety improvements, reduction of flood hazards, and coordination of hazardous materials planning and response. The Council is composed of 21 members appointed by the Adjutant General, including representatives from local governments, representatives from federally recognized tribes, sheriffs and police chiefs, medical examiners, the Military Department, and various medical and safety experts.

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) sits 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 reviewing and approving standards and policies developed by the OCIO and providing oversight of major information technology projects.

Department of Commerce.
The Department of Commerce (Commerce) must supervise and administer energy-related activities as specified under current law. Commerce's duties and 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.

Summary of Bill:

Emergency Management Council.
As part of its annual assessment of statewide emergency preparedness, the Council must provide the Governor with an update on mitigation of cybersecurity risks to critical infrastructure.

The Cybersecurity Advisory Committee (Committee) is created as a subcommittee of the Council to provide advice and recommendations that strengthen cybersecurity in both private and public sectors across all critical infrastructure sectors. The Committee must meet quarterly and collaborate with organizations with expertise and responsibility for cybersecurity and incident response in various sectors to provide recommendations on building and sustaining the state's capability to identify and mitigate cybersecurity risk and to respond to and recover from cybersecurity incidents including ransomware incidents.

The Committee must work with federal agencies, state agencies, institutions of higher education, industry experts, and technical specialists to:

- identify which local, tribal, and industry infrastructure sectors are at the greatest risk of cyberattacks and need the most enhanced cybersecurity measures;
- use federal guidance to analyze categories of critical infrastructure that may result in catastrophic consequences if unauthorized cyber access occurred;
- recommend, in consultation with the Energy Resilience and Emergency Management Office at Commerce, cyber incident response exercises related to risk mitigation in various sectors such as the water, transportation, communications, health care, elections, energy, agriculture, and higher education sectors; and
- examine inconsistencies between state and federal law pertaining to cybersecurity.

The reports produced and information compiled by the Committee in fulfilling its duties under the act are confidential and may not be disclosed under the Public Records Act (PRA).

Technology Services Board.

The Technology Services Board Security Subcommittee (TSBSS) is created with the TSB. It must meet quarterly and hold a joint meeting once a year with the Committee. The Chair of the TSB appoints members of the TSB to the TSBSS and may appoint representatives from relevant technology sectors. In collaboration with the Military Department and the Committee, the TSBSS is responsible for:

- reviewing emergent cyberattacks and threats to critical infrastructure sectors to identify existing gaps in state agency cybersecurity policies;
- assessing emerging risks to state agency IT;
- recommending a reporting and information sharing system to notify state agencies of new risks, risk treatment opportunities, and projected shortfalls in response and recovery;
- recommending security exercises including data breach simulations;
- assisting the OCIO in developing best practices relating to cybersecurity;
- reviewing the proposed policies and standards developed by the OCIO and recommending their approval to the TSB;
- reviewing cybersecurity and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies; and
- assisting WaTech and the Military Department in producing a report on the state of

cybersecurity described below.

WaTech must work with the National Institute of Standards and Technology and other federal agencies, private sector businesses, and private cybersecurity experts to bring their perspective and guidance to the TSB for full consideration to ensure a holistic approach to cybersecurity in state government.

Each December 1, beginning in 2023, the Military Department and WaTech must jointly provide the Governor and Legislature with a report on the state of cybersecurity. The report must specify recommendations necessary to address cybersecurity in the state. The TSBSS must coordinate the implementation of any recommendations in the report and may identify the portions of the report that it deems necessary to protect the security of public and private cybersecurity systems.

The reports and information compiled to meet the foregoing requirements are confidential and may not be disclosed under the PRA. The TSBSS may hold a portion of its agenda in executive session closed to the public to discuss sensitive security information.

Department of Commerce.
The duties and powers of Commerce are expanded to include preparing and updating contingency plans for security energy infrastructure against all physical and cybersecurity threats.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) Cybersecurity risks threaten various infrastructures including emergency communications, critical manufacturing, emergency services, transportation, water and wastewater treatment, food processing, and agriculture. There is a gap in steps the state is taking around cybersecurity and protecting its data infrastructure, energy sector, and physical structures that are experiencing an increasing amount of digit attacks. This act requires the TSB, Governor's Office, and Council to combine their efforts to fortify the state's ability to protect against cybersecurity risks, whether that on the digital aspect of cybersecurity or the physical domain of the state's electrical grid.

The Council is the proper place to gather experts in cybersecurity issues and provide a venue for the coordination of state and private sector experts to identify and mitigate cyber

risks. Creating a subcommittee within the Council will better inform the Legislature and the Governor of cyber threats and will also build a stronger connection to how those threats affect Federal Emergency Management Agency emergency support functions that are coordinating through the state's Council.

The TSBSS within the TSB is an existing subcommittee. This act will codify what is already in existence. The work of the TSBSS adds clarity to the state's policy with regard to cybersecurity policy and will allow the state to analyze these important cybersecurity issues on an ongoing basis and provide clarity of cybersecurity governance across state government. The coordination required under the bill will ensure that a holistic approach is being taken to address cybersecurity issues and create uniform cybersecurity policy.

Commerce is responsible for preparing and implementing contingency plans that address energy emergency and shortages of all types. The act will help Commerce implement its duties better by clarifying the role it has with energy cybersecurity and allows it to take an all-hazards approach to its work.

(Opposed) None.

Persons Testifying: Senator Matt Boehnke, prime sponsor; Jim Baumgart, Washington Military Department; Derek Puckett, Consolidated Technology Services; and Michael Furze, Department of Commerce.

Persons Signed In To Testify But Not Testifying: None.