FINAL BILL REPORT
SHB 1251

C 101 L 20
Synopsis as Enacted

Brief Description: Concerning security breaches of election systems or election data including by foreign entities.

Sponsors: House Committee on State Government & Tribal Relations (originally sponsored by Representatives Tarleton, Hudgins and Wylie).

House Committee on State Government & Tribal Relations
Senate Committee on State Government, Tribal Relations & Elections

Background:

State Information Technology Security.
The Office of the Chief Information Officer (CIO) establishes information technology policy and direction for the state, including security standards to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure.

Elections Security and Testing.
The Secretary of State (SOS) has partnered with the Department of Homeland Security (DHS) to assess vulnerabilities in the state election system, identify mitigation plans, share information, rely on the DHS for local in-person support, and report incidents or threats.

All voting systems or components of voting systems must be inspected, evaluated, and publicly tested by the SOS prior to their use in a primary or election. Any modification, change, or improvement to any voting system or component of a system may be made without reapproval or reexamination if it does not impair its accuracy, efficiency, or capacity, or extend its function. Certain elements must be met prior to the approval of a voting device or vote tallying system.

A manufacturer or distributor of a certified voting system or component of a certified voting system must disclose to the SOS and the Attorney General any security breach of its system under certain circumstances. Prior to sale or lease, a voting system must pass an acceptance test to demonstrate that the equipment is the same as that certified by the SOS and is operating correctly. The SOS may decertify a voting system or component of a voting system and withdraw the authority for its future use or sale in the state if the manufacturer or

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

distributor fails to disclose security breaches as required or if the SOS determines that the system or component does not meet other specified standards.

Washington State Fusion Center.
The Washington State Fusion Center (WSFC) is a state and major urban area fusion center that provides multidisciplinary expertise and situational awareness to inform decision making at all levels of government. The WSFC conducts analysis and facilitates information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. During a significant cyber incident, the WSFC is able to facilitate information sharing using Homeland Security Information Network cyber security alerts.

Summary:

The Secretary of State (SOS) must annually consult with the Washington State Fusion Center (WSFC), the Office of the Chief Information Officer (CIO), and each county auditor to identify security breaches of election systems or election data. A security breach is a breach of the election system or associated data where the system or associated data have been penetrated, accessed, or manipulated by an unauthorized person. The SOS, if possible, must identify whether the source of any security breach is a foreign entity, domestic entity, or both.

By December 31 of each year, the SOS must report to the Governor, the CIO, the WSFC, and the chairs and ranking members of the appropriate legislative committees on:

- information on any identified security breaches;
- options to increase the security of the elections system and election data; and
- options to prevent future security breaches.

The report and any related material, data, or other information provided to the SOS while identifying any security breach, or information used to assemble the report, may only be distributed to recipients of the report.

A voting system or a component of a voting system must pass a vulnerability test conducted by a federal or state public entity which includes participation by local elections officials before being purchased or leased.

Votes on Final Passage:

House	95	0	
House	95	1	
Senate	44	0	(Senate amended)
House	97	0	(House concurred)

Effective: June 11, 2020