SENATE BILL REPORT
SHB 1251

As of March 20, 2019

Title: An act relating to security breaches of election systems or election data including by foreign entities.

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).

Brief History: Passed House: 3/08/19, 95-0.
Committee Activity: State Government, Tribal Relations & Elections: 3/20/19.

Brief Summary of Bill

- Requires the Secretary of State to annually consult with the Washington State Fusion Center, the Office of the Chief Information Officer, and each county auditor to identify security breaches of election systems or election data, including the sources of those breaches, and report the findings.

SENATE COMMITTEE ON STATE GOVERNMENT, TRIBAL RELATIONS & ELECTIONS

Staff: Samuel Brown (786-7470)

Background: Elections Security and Testing. The Secretary of State (Secretary) has partnered with the federal Department of Homeland Security to assess vulnerabilities in the state election system and identify mitigation plans, share information, receive local in-person support, and report incidents or threats. Under Washington law, a manufacturer or distributor of a voting system or component of a voting system certified by the Secretary, must disclose to the Secretary and the Attorney General any security breach of its system under certain circumstances as prescribed by law.

The Secretary 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 distributor fails to disclose security breaches as required;

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.

- the Secretary determines that the system or component fails to meet the standards set forth in applicable federal guidelines;
- the system or component was materially misrepresented in the certification application;
- the applicant has installed unauthorized modifications to the certified software or hardware; or
- any other reason authorized by rule adopted by the Secretary.

State Information Technology Security. The Office of the Chief Information Officer (OCIO), under the direction of the Chief Information Officer, 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.

Washington State Fusion Center. The Washington State Fusion Center (WSFC) is a state and major urban area fusion center providing multidisciplinary expertise and situational awareness to inform governmental decision making. 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, WSFC is able to facilitate information sharing using Homeland Security Information Network cyber security alerts.

Summary of Bill: The Secretary must annually consult with WSFC, OCIO, and each county auditor to identify instances where election systems or associated data have been penetrated, accessed, or manipulated by an unauthorized person and, if possible, identify whether the source of any security breach is a foreign entity, domestic entity, or both.

The Secretary must submit a report to the Governor, the Chief Information Officer, the WSFC, and the chairs and ranking members of the appropriate legislative committees from the Senate and the House of Representatives by December 31st of each year containing:
- information on any instances of election system security breaches;
- options to increase election system and data security; and
- options to prevent future security breaches.

The report and any related material provided to the Secretary while identifying any security breach used to assemble the report may only be distributed to these individuals.

Appropriation: None.

Fiscal Note: Available.

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

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

Staff Summary of Public Testimony: PRO: We do what is in this bill on an ongoing basis, this bill simply adds the reporting requirement. We appreciate that disclosure of the report and its contents is limited; we do not want to leave a roadmap for breaches.

Persons Testifying: PRO: Jay Jennings, Secretary of State's Office.

Persons Signed In To Testify But Not Testifying: No one.