HOUSE BILL REPORT
SHB 1251

As Passed Legislature

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:

Committee Activity:

State Government & Tribal Relations: 2/12/19, 2/19/19 [DPS].

Floor Activity:

Passed House: 3/8/19, 95-0.
Passed House: 1/30/20, 95-1.
Senate Amended.
Passed Senate: 3/4/20, 44-0.
House Concurred.
Passed House: 3/7/20, 97-0.
Passed Legislature.

Brief Summary of Substitute Bill

- Requires the Secretary of State (Secretary) to annually consult with the Washington State Fusion Center (WSFC), State Chief Information Officer (CIO), and each county auditor to identify instances of security breaches of election systems or election data, and identify whether the source of any security breach is a foreign entity, domestic entity, or both.
- Requires the Secretary to annually report to the Governor, the CIO, the WSFC, and the chairs and ranking members of the appropriate legislative committees from the Senate and the House of Representatives on any instances of security breaches, options to increase the security of the elections system and election data, and options to prevent future security breaches.
- Requires a voting system or component of a voting system to pass a vulnerability test before being purchased or leased.

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.

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Gregerson, Chair; Pellicciotti, Vice Chair; Walsh, Ranking Minority Member; Goehner, Assistant Ranking Minority Member; Appleton, Dolan, Hudgins, Mosbrucker and Smith.

Staff: Carrington Skinner (786-7192).

Background:

State Information Technology Security.
The Office 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.

Elections Security and Testing.
The Office of the Secretary of State (OSOS) has partnered with the Department of Homeland Security (DHS) to assess vulnerabilities in the state election system and 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 Secretary of State (Secretary) prior to its 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 as prescribed by law must be met prior to the approval of a voting device or vote tallying system.

A manufacturer or distributor of a voting system or component of a voting system that is certified by the Secretary must disclose to the Secretary and the Attorney General (AG) 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, or if 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.

Washington State Fusion Center.
The Washington State Fusion Center (WSFC) is a state and major urban area fusion center. Similar to other fusion centers, the WSFC provides multidisciplinary expertise and situational awareness to inform decision making at all levels of government. It 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 of Substitute Bill:

The Secretary must annually consult with the WSFC, the CIO, and each county auditor to identify instances of 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 has been penetrated, accessed, or manipulated by an unauthorized person. The Secretary, if possible, must identify whether the source of any security breach is a foreign entity, domestic entity, or both. A foreign entity is an entity that is not organized or formed under the laws of the United States (U.S.), or a person who is not domiciled in the U.S., or a citizen of the U.S.

By December 31 each year, the Secretary must report to the Governor, the CIO, the WSFC, and the chairs and ranking members of the appropriate legislative committees from the Senate and the House of Representatives on:

- information on any instances of 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 Secretary while identifying any security breach, or information used to assemble the report, may only be distributed to these individuals.

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.

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) This is a result of a cooperative effort to protect the cybersecurity of our elections system. Cybersecurity is a top priority for the OSOS and is monitored closely. Bad actors are creative and are seeking new ways to penetrate. There are plenty of attempts, and it requires acute awareness and monitoring to protect the elections system. Elections was declared a critical infrastructure to homeland security and, as a result, the OSOS received federal funds to ensure cybersecurity is being protected. The bill directs the OSOS to do what is already being done. Although the bill requires an annual reporting, if there is a breach of the elections system, the OSOS will report that before the annual report is due. There is a requirement to treat this information as privileged, but additional language to further tighten that might be warranted.

(Opposed) None.

Persons Testifying: Jay Jennings, Office of the Secretary of State.

Persons Signed In To Testify But Not Testifying: None.