Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

State Government & Tribal Relations Committee

HB 1251

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

Sponsors: Representatives Tarleton, Hudgins and Wylie.

Brief Summary of Bill

- Requires the Secretary of State (Secretary) to annually consult with the Attorney General (AG), State Chief Information Office (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, Lieutenant Governor, CIO, AG, 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.

Hearing Date: 2/12/19

Staff: Desiree Omli (786-7105).

Background:

State Information Technology Security.
The Office 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.

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.

Elections Security and Testing.
The Office of the Secretary of State 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.

Summary of Bill:

The Secretary must annually consult with the AG, State Chief Information Office (CIO), and each county auditor to identify instances of security breaches of election systems or election data. A security breach is either an attempt to penetrate, access, or manipulate an election system or associated election data by an unauthorized person, or 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, or a person who is not domiciled in the United States or a citizen of the United States.

By December 31 each year, the Secretary must report to the Governor, Lieutenant Governor, CIO, AG, 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 used to assemble the report may only be distributed to these individuals.

Appropriation: None.

Fiscal Note: Requested on February 10, 2019.

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