SENATE BILL REPORT
SB 5014

As Reported by Senate Committee On:
State Government, Tribal Affairs & Elections, February 7, 2025

Title: An act relating to election security.

Brief Description: Concerning election security.

Sponsors: Senators Boehnke, Bateman, Chapman, Dozier, Hasegawa, Liias, Nobles, Riccelli, Valdez and Wellman; by request of Secretary of State.

Brief History:
Committee Activity: State Government, Tribal Affairs & Elections: 1/21/25, 2/07/25 [DPS].

Brief Summary of First Substitute Bill

- Subjects systems or part of a systems used in the conduct of elections to secretary of state approval prior to use.
- Sets forth security breach disclosure requirements for organizations contracted to provide support to, or manufacturers or distributors of the voter registration database system or official voter list, or both.
- Mandates cybersecurity measures to be implemented by each county auditor, including partitioning, by July 1, 2027.

SENATE COMMITTEE ON STATE GOVERNMENT, TRIBAL AFFAIRS & ELECTIONS

Majority Report: That Substitute Senate Bill No. 5014 be substituted therefor, and the substitute bill do pass.

Signed by Senators Valdez, Chair; Krishnadasan, Vice Chair; Wilson, J., Ranking Member; Fortunato, Hasegawa, Kauffman, McCune, Riccelli and Short.

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.

Staff: Danielle Creech (786-7412)

Background: Approval of Voting Systems. Under current law, any voting systems, devices, or vote tallying systems, prior to use in an election, must be approved by the secretary of state, unless approved by statute before March 22, 1982. Any modification, change, or improvement that does not impair its accuracy, efficiency, or capacity to extend its function, may be made without reexamination or reapproval by the secretary of state.

Detection and Disclosure of Security Breaches. A manufacturer or distributor of a voting system that has been certified by the secretary of state must immediately disclose a security breach to both the secretary of state and attorney general, if:

- the breach has, or is reasonably likely to have, comprised the security, confidentiality, or integrity of an election in any state; or
- personal information of residents of any state was, or is reasonably believed to have been acquired by an unauthorized person.

County Cybersecurity. Each county must install and maintain an intrusion detection system that passively monitors its network for malicious traffic 24 hours a day, seven days a week, 365 days a year by a qualified and trained security team with access to cyberincident response personnel. The system must support the unique security requirements of state, local, tribal, and territorial governments, and possess the ability to receive cyberintelligent threat updates to stay ahead of evolving attack patterns. A county auditor or information technology (IT) director of a county participating in the shared voter registration system operated by the secretary of state, or using a voting system or component of a voting system that is certified by the secretary of state, must immediately disclose to both the secretary of state and attorney general any malicious activity or security breaches of any of its IT systems, if:

- malicious activity was detected by an IT intrusion detection system (IDS), malicious domain blocking and reporting system, or endpoint security software;
- a breach has, or is likely to have compromised the security, confidentiality, or integrity of election systems or IT systems, or compromised the security, confidentiality, or integrity of an election within the state; or
- personal information of residents was, or is reasonably believed to have been acquired by an unauthorized person.

Summary of Bill (First Substitute): Approval of Equipment and Platforms. In addition to voting systems, devices, and vote tallying systems, the secretary of state must approve mechanical, electromechanical, or electronic equipment or platforms including software, firmware, or hardware that is used to provide voter assistance. This includes platforms used in issuing ballots, facilitating voters' response to a required notice, to provide electronic means for submission of a ballot declaration signature, to issue, authenticate, or validate voter identification, and any component of a voting system that the secretary of state determines requires prior approval before use. Upon review, the secretary of state may determine that a modification, change, or improvement required of any voting system or

component of a system does not require a full reexamination or reapproval by the secretary of state.

Disclosure of Security Breaches. An organization contracted to provide support to, or a manufacturer or distributer of, the voter registration database system or the official voter list, must immediately disclose any security breach of the system to the secretary of state and attorney general if:

- the breach has, or is reasonably likely to have compromised the security, confidentiality, or integrity of an election; or
- personal information of residents of any state was, or is reasonably believed to have been, acquired by an unauthorized person due to the breach.

County Cybersecurity. Every county auditor must implement the following cybersecurity measures:

- use of the .gov top-level domain available through the U.S. Department of Homeland Security;
- electronic and physical partitioning of all election and voting infrastructure from other county IT systems;
- isolation of all ballot counting equipment and voting systems components from any other network;
- prohibiting configuration of voting systems to establish a connection to an external network or device external to the voting system;
- purchase of voting systems that include documentation listing security configurations and network security best practices, and adherence to said practices; and
- restricting all data transfers from any voting system to using single-use, previously erased devices that contain no information prior to connection with the system. Devices used for data transfer must be provided by the secretary of state to the county auditor for single use, or the media must be overwritten by the county auditor following rules established by the secretary of state.

EFFECT OF CHANGES MADE BY STATE GOVERNMENT, TRIBAL AFFAIRS & ELECTIONS COMMITTEE (First Substitute):

- Modifies the intent section to specify that partitioning can involve logically separating the entire auditor's office, including its IT systems and assets, and clarifies the goal of partitioning;
- Removes duplicative language regarding secretary approval of equipment and platforms;
- Clarifies that any system or part of a system used in the conduct of elections may be subject to secretary approval prior to use;
- Inserts a date by which county auditors shall implement cybersecurity measures—July 1, 2027; and
- Adds language to clarify the partitioning requirements of county auditors.

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 on Original Bill: *The committee recommended a different version of the bill than what was heard.* PRO: We are seeing more attacks on our network and we want to continue to build trust in our voting system. This provides us surveillance on our voting systems to detect and determine if data breaches have impacted our data. In addition to the security enhancements adopting the .gov domain would provide, it is also a way to reinforce credibility and trust, which is paramount to the integrity of our elections in Washington State. The Secretary of State's Office has provided up to $80,000 per county per fiscal year to support election security enhancements, so that will cover much of the cost of this bill. The network segmentation will reduce the risk of compromise and make it a lot harder for adversaries to access critical data and systems. These are effective and common sense measures to protect the integrity of Washington's elections and instill public trust.

Persons Testifying: PRO: Senator Matt Boehnke, Prime Sponsor; Kylee Zabel, Office of Secretary of State; Kevin McMahan, Office of Secretary of State.

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