S-0896.1

SUBSTITUTE SENATE BILL 5014

State of Washington 69th Legislature 2025 Regular Session

By Senate State Government, Tribal Affairs & Elections (originally sponsored by Senators Boehnke, Bateman, Chapman, Dozier, Hasegawa, Liias, Nobles, Riccelli, Valdez, and Wellman; by request of Secretary of State)

READ FIRST TIME 02/11/25.

AN ACT Relating to election security; amending RCW 29A.12.050 and 29A.12.180; adding a new section to chapter 29A.12 RCW; and creating a new section.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** (1) The legislature finds that the electronic and physical security of election and voting infrastructure are of primary importance, and wishes to require new security requirements. The legislature further finds that:

(a) Requiring the use of the ".gov" top-level domain on all websites and email communication reduces opportunities for confusion and cyber threats. The ".gov" top-level domain is managed by the United States department of homeland security through the cybersecurity and infrastructure security agency, is limited to bona fide government agencies, and features fraud prevention controls. There is no fee charged to adopt a ".gov" top-level domain.

(b) Requiring the partitioning of internal government networks, servers, and other supporting electronic infrastructure separate from other electronic equipment housed in the same location provides a more secure environment. Partitioning can involve physically or logically separating the entire auditor's office, including all its information technology systems and assets, or focusing specifically

on election and voting infrastructure from other county assets. The goal is to reduce the risk of compromises that may occur on other parts of the county network. Partitioning also enables tighter control and monitoring of access to critical systems, whether it applies to the entire auditor's office or just election-related systems and assets.

(c) Because the secretary of state and county election offices are electronically interconnected and speedy communication with the state when a county is under attack or has suffered a security breach is imperative, requiring all vendors supporting county or state cyber assets to communicate to the secretary of state and the attorney general immediately after detecting a breach or successful cyber attack against their assets is necessary to maintain security.

(2) The legislature intends to require adoption of these security measures in all county election offices as soon as practicable, but no later than July 1, 2027.

Sec. 2. RCW 29A.12.050 and 2003 c 111 s 305 are each amended to read as follows:

((~~If voting~~)) (1) Prior to use in conducting any primary or election, the secretary of state must approve systems used in the conduct of elections, including:

(a) Voting systems ((~~or~~)), voting devices, or vote tallying systems ((~~are to be used for conducting a primary or election, only those that have the approval of the secretary of state or had been~~)), unless approved under this chapter or the former chapter 29.34 RCW before March 22, 1982((~~, may be used~~));

(b) Any mechanical, electromechanical, or electronic equipment or platform, including software, firmware, or hardware that is used:

(i) In issuing a ballot;

(ii) To facilitate voters' response to a required notice;

(iii) To provide an electronic means for submission of a ballot declaration signature under RCW 29A.60.165; or

(iv) To issue, authenticate, or validate voter identification; and

(c) Any system or part of a system used in the conduct of elections that the secretary of state determines requires prior approval before use in an election or primary. ((~~Any~~))

(2) The secretary of state may, after review, determine that a modification, change, or improvement to any voting system or

component of a system ((~~that~~)) does not ((~~impair its accuracy, efficiency, or capacity or extend its function, may be made without~~)) require a full reexamination or reapproval by the secretary of state under RCW 29A.12.020.

Sec. 3. RCW 29A.12.180 and 2024 c 28 s 1 are each amended to read as follows:

(1) A manufacturer or distributor of a voting system or component of a voting system that is certified by the secretary of state under RCW 29A.12.020 shall disclose to the secretary of state and attorney general any breach of the security of its system immediately following discovery of the breach if:

(a) The breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election in any state; or

(b) Personal information of residents in any state was, or is reasonably believed to have been, acquired by an unauthorized person as a result of the breach and the personal information was not secured. For purposes of this subsection, "personal information" has the meaning given in RCW 19.255.010.

(2) Every 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, and 365 days a year by a qualified and trained security team with access to cyberincident response personnel who can assist the county in the event of a malicious attack. 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.

(3) A county auditor or county information technology director of any county, participating in the shared voter registration system operated by the secretary of state under RCW 29A.08.105 and 29A.08.125, or operating a voting system or component of a voting system that is certified by the secretary of state under RCW 29A.12.020 shall disclose to the secretary of state and attorney general any malicious activity or breach of the security of any of its information technology (IT) systems immediately following discovery if:

(a) Malicious activity was detected by an information technology intrusion detection system (IDS), malicious domain blocking and

reporting system, or endpoint security software, used by the county, the county auditor, or the county election office;

(b) A breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of election systems, information technology systems used by the county staff to manage and support the administration of elections, or peripheral information technology systems that support the auditor's office in the office's day-to-day activities;

(c) The breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election within the state; or

(d) Personal information of residents in any state was, or is reasonably believed to have been, acquired by an unauthorized person as a result of the breach and the personal information was not secured. For purposes of this subsection, "personal information" has the meaning given in RCW 19.255.005.

(4) A manufacturer of, distributor of, or organization contracted to provide support to, the voter registration database system required by RCW 29A.08.125, the official voter list required by RCW 29A.08.105, or systems or components of the voter registration system used by the secretary of state shall disclose to the secretary of state and attorney general any security breach of any of that organization's systems immediately following discovery of the breach if:

(a) The breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election in any state; or

(b) Personal information of residents in any state was, or is reasonably believed to have been, acquired by an unauthorized person as a result of the breach and the personal information was not secured. For purposes of this subsection, "personal information" has the meaning given in RCW 19.255.010.

(5) For purposes of this section:

(a) "Malicious activity" means an external or internal threat that is designed to damage, disrupt, or compromise an information technology network, as well as the hardware and applications that reside on the network, thereby impacting performance, data integrity, and the confidentiality of data on the network. Threats include viruses, ransomware, trojan horses, worms, malware, data loss, or the disabling or removing of information technology security systems.

(b) "Security breach" means a breach of the election system, information technology systems used to administer and support the election process, or associated data where the system or associated data has been penetrated, accessed, or manipulated by an unauthorized person. The definition of breach includes all unauthorized access to systems by external or internal personnel or organizations, including personnel employed by a county or the state providing access to systems that have the potential to lead to a breach.

((~~(5)~~)) (6) Notification under this section must be made in the most expedient time possible and without unreasonable delay.

NEW SECTION. **Sec. 4.** A new section is added to chapter 29A.12 RCW to read as follows:

Each county auditor shall implement no later than July 1, 2027, cybersecurity measures including but not limited to:

(1) Implementation and adoption of the ".gov" top-level domain available through the United States department of homeland security through the cybersecurity and infrastructure security agency for all election and voting systems and infrastructure. This adoption is required for election and voting systems and websites and may include all county cyber assets and email domains.

(2) Partitioning the entire auditor's office, including all its information technology systems and assets, or specifically partitioning election and voting information technology infrastructure from other county assets.

(3) Isolation of all ballot counting equipment and voting system components as defined in RCW 29A.12.005 from any other network including:

(a) Internal networks within a county election office;

(b) Printer sharing networks external to the ballot counting system;

(c) The internet, world wide web, or other similar networks;

(d) Wifi and radio connectivity;

(e) Wired connectivity; and

(f) Any telephonic or other connectivity.

(4) No configuration of voting systems to:

(a) Establish a connection to an external network; or

(b) Connect to any device external to the voting system.

(5) Purchase of voting systems that include documentation listing security configurations and network security best practices and

operating those systems used for conducting primaries and elections in a manner consistent with that documentation.

(6) 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. This includes pen drives, flash memory drives, memory sticks, and any other removal media used to transfer data. Devices used in data transfer must either be provided by the secretary of state to the county auditor for single use, or the media must be overwritten by the county auditor by following guidelines for media sanitization defined in rules promulgated by the secretary of state.

--- END ---