

---

**SENATE BILL 5014**

---

**State of Washington**

**69th Legislature**

**2025 Regular Session**

**By** Senators Boehnke, Bateman, Chapman, Dozier, Hasegawa, Lias, Nobles, Riccelli, Valdez, and Wellman; by request of Secretary of State

Prefiled 12/05/24. Read first time 01/13/25. Referred to Committee on State Government, Tribal Affairs & Elections.

1 AN ACT Relating to election security; amending RCW 29A.12.050 and  
2 29A.12.180; adding a new section to chapter 29A.12 RCW; and creating  
3 a new section.

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

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

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

16 (b) Requiring the partitioning of internal government networks,  
17 servers, and other supporting electronic infrastructure separate from  
18 other electronic equipment housed in the same location or locations  
19 can also provide a more secure environment. Partitioning means  
20 physically and electronically separating election and voting  
21 infrastructure from other county assets with the goal of reducing

1 vulnerability to attacks that may occur on other parts of a county's  
2 cyber infrastructure. Partitioning also allows access to the  
3 infrastructure to be more tightly controlled and monitored.

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

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

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

16 ~~((If voting))~~ (1) The secretary of state must approve systems  
17 used in the conduct of elections prior to the system being used in  
18 conducting any primary or election, including the following:

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

24 (b) Any mechanical, electromechanical, or electronic equipment or  
25 platform, including software, firmware, or hardware that is used to  
26 provide voter assistance. This includes equipment or platforms used:

27 (i) In issuing a ballot;

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

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

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

32 and

33 (c) Any component part of a voting system that the secretary of  
34 state determines requires prior approval before use in an election or  
35 primary. ~~((Any))~~

36 (2) The secretary of state may, after review, determine that a  
37 modification, change, or improvement to any voting system or  
38 component of a system ~~((that))~~ does not ~~((impair its accuracy,~~  
39 ~~efficiency, or capacity or extend its function, may be made without))~~

1 require a full reexamination or reapproval by the secretary of state  
2 under RCW 29A.12.020.

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

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

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

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

18 (2) Every county must install and maintain an intrusion detection  
19 system that passively monitors its network for malicious traffic 24  
20 hours a day, seven days a week, and 365 days a year by a qualified  
21 and trained security team with access to cyberincident response  
22 personnel who can assist the county in the event of a malicious  
23 attack. The system must support the unique security requirements of  
24 state, local, tribal, and territorial governments and possess the  
25 ability to receive cyberintelligent threat updates to stay ahead of  
26 evolving attack patterns.

27 (3) A county auditor or county information technology director of  
28 any county, participating in the shared voter registration system  
29 operated by the secretary of state under RCW 29A.08.105 and  
30 29A.08.125, or operating a voting system or component of a voting  
31 system that is certified by the secretary of state under RCW  
32 29A.12.020 shall disclose to the secretary of state and attorney  
33 general any malicious activity or breach of the security of any of  
34 its information technology (IT) systems immediately following  
35 discovery if:

36 (a) Malicious activity was detected by an information technology  
37 intrusion detection system (IDS), malicious domain blocking and  
38 reporting system, or endpoint security software, used by the county,  
39 the county auditor, or the county election office;

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

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

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

15 (4) A manufacturer of, distributor of, or organization contracted  
16 to provide support to, the voter registration database system  
17 required by RCW 29A.08.125, the official voter list required by RCW  
18 29A.08.105, or systems or components of the voter registration system  
19 used by the secretary of state shall disclose to the secretary of  
20 state and attorney general any security breach of any of that  
21 organization's systems immediately following discovery of the breach  
22 if:

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

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

31 (5) For purposes of this section:

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

39 (b) "Security breach" means a breach of the election system,  
40 information technology systems used to administer and support the

1 election process, or associated data where the system or associated  
2 data has been penetrated, accessed, or manipulated by an unauthorized  
3 person. The definition of breach includes all unauthorized access to  
4 systems by external or internal personnel or organizations, including  
5 personnel employed by a county or the state providing access to  
6 systems that have the potential to lead to a breach.

7 ~~((5))~~ (6) Notification under this section must be made in the  
8 most expedient time possible and without unreasonable delay.

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

11 Each county auditor shall implement cybersecurity measures  
12 including but not limited to:

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

19 (2) Electronic and physical partitioning of all election and  
20 voting infrastructure from other county information technology  
21 systems.

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

25 (a) Internal networks within a county election office;

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

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

29 (d) Wifi and radio connectivity;

30 (e) Wired connectivity; and

31 (f) Any telephonic or other connectivity.

32 (4) No configuration of voting systems to:

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

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

35 (5) Purchase of voting systems that include documentation listing  
36 security configurations and network security best practices and  
37 operating those systems used for conducting primaries and elections  
38 in a manner consistent with that documentation.

1       (6) Restricting all data transfers from any voting system to  
2 using single use, previously erased devices that contain no  
3 information prior to connection with the system. This includes pen  
4 drives, flash memory drives, memory sticks, and any other removal  
5 media used to transfer data. Devices used in data transfer must  
6 either be provided by the secretary of state to the county auditor  
7 for single use, or the media must be overwritten by the county  
8 auditor by following guidelines for media sanitization defined in  
9 rules promulgated by the secretary of state.

--- END ---