
ENGROSSED 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, Liiias, Nobles, Riccelli, Valdez, and Wellman; by request of Secretary of State)

READ FIRST TIME 02/11/25.

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 provides a
19 more secure environment. Partitioning can involve physically or
20 logically separating the entire auditor's office, including all its
21 information technology systems and assets, or focusing specifically

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

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

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

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

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

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

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

- 29 (i) In issuing a ballot;
30 (ii) To facilitate voters' response to a required notice;
31 (iii) To provide an electronic means for submission of a ballot
32 declaration signature under RCW 29A.60.165; or
33 (iv) To issue, authenticate, or validate voter identification;
34 and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

33 (5) For purposes of this section:

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

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

9 ~~((5))~~ (6) Notification under this section must be made in the
10 most expedient time possible and without unreasonable delay.

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

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

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

21 (2) Partitioning the entire auditor's office, including all of
22 its information technology systems and assets, or specifically
23 partitioning election and voting information technology
24 infrastructure from other county assets. The secretary of state shall
25 consult with county auditors on which systems and assets need to be
26 partitioned or technologically isolated and protected. Eliminating
27 threat actors from moving laterally within a network to target
28 election-related capabilities is paramount. The secretary of state
29 may extend the deadline for a county auditor to comply with this
30 subsection if more time is necessary for implementation.

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

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

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

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

38 (d) Wifi and radio connectivity;

39 (e) Wired connectivity; and

1 (f) Any telephonic or other connectivity.
2 (4) No configuration of voting systems to:
3 (a) Establish a connection to an external network; or
4 (b) Connect to any device external to the voting system.
5 (5) Purchase of voting systems that include documentation listing
6 security configurations and network security best practices and
7 operating those systems used for conducting primaries and elections
8 in a manner consistent with that documentation.
9 (6) Restricting all data transfers from any voting system to
10 using single use, previously erased devices that contain no
11 information prior to connection with the system. This includes pen
12 drives, flash memory drives, memory sticks, and any other removal
13 media used to transfer data. Devices used in data transfer must
14 either be provided by the secretary of state to the county auditor
15 for single use, or the media must be overwritten by the county
16 auditor by following guidelines for media sanitization defined in
17 rules promulgated by the secretary of state.

--- END ---