Chapter 29A.12 RCW
VOTING SYSTEMS

Sections

RCW 29A.12.005 "Voting system." As used in this chapter, "voting system" means:

(1) The total combination of mechanical, electromechanical, or electronic equipment including, but not limited to, the software, firmware, and documentation required to program, control, and support the equipment, that is used:

(a) To define ballots;

(b) To cast and count votes;

(c) To report or display election results from the voting system;

(d) To maintain and produce any audit trail information; and

(e) To perform an audit under RCW 29A.60.185; and

(2) The practices and associated documentation used:

(a) To identify system components and versions of such components;

(b) To test the system during its development and maintenance;

(c) To maintain records of system errors and defects;

(d) To determine specific system changes to be made to a system after the initial qualification of the system; and

(e) To make available any materials to the voter such as notices, instructions, forms, or paper ballots. [2018 c 218 s 5; 2013 c 11 s 21; 2004 c 267 s 601.]

Intent—2018 c 218: See note following RCW 29A.60.185.

Effective dates—2004 c 267: See note following RCW 29A.08.010.

RCW 29A.12.010 Authority for use. At any primary or election in any county, votes may be cast, registered, recorded, or counted by means of voting systems that have been approved under RCW 29A.12.020. [2003 c 111 s 301. Prior: 1990 c 59 s 17; 1967 ex.s. c 109 s 12; 1965 c 9 s 29.33.020; prior: (i) 1913 c 58 s 1, part; RRS s 5300, part. (ii) 1913 c 58 s 18; RRS s 5318. Formerly RCW 29.33.020.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

RCW 29A.12.020 Inspection and test by secretary of state—Report. The secretary of state shall inspect, evaluate, and publicly test all voting systems or components of voting systems that are submitted for review under RCW 29A.12.030. The secretary of state shall determine whether the voting systems conform with all of the requirements of this title, the applicable rules adopted in accordance with this title, and with generally accepted safety requirements. The secretary of state shall transmit a copy of the report of any examination under this section, within thirty days after completing the examination, to the county auditor of each county. [2003 c 111 s 302. Prior: 1990 c 59 s 18; 1982 c 40 s 1. Formerly RCW 29.33.041.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Severability—1982 c 40: "If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected." [1982 c 40 s 11.]

RCW 29A.12.030 Submitting system or component for examination. The manufacturer or distributor of a voting system or component of a voting system may submit that system or component to the secretary of state for examination under RCW 29A.12.020. [2003 c 111 s 303. Prior: 1990 c 59 s 19; 1982 c 40 s 2. Formerly RCW 29.33.051.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Severability—1982 c 40: See note following RCW 29A.12.020.

RCW 29A.12.040 Independent evaluation. (1) The secretary of state may rely on the results of independent design, engineering, and performance evaluations in the examination under RCW 29A.12.020 if the source and scope of these independent evaluations are specified by rule.

(2) The secretary of state may contract with experts in mechanical or electrical engineering or data processing to assist in examining a voting system or component. The manufacturer or distributor who has submitted a voting system for testing under RCW 29A.12.030 shall pay the secretary of state a deposit to reimburse the cost of any contract for consultation under this section and for any other unrecoverable costs associated with the examination of a voting

system or component by the manufacturer or distributor who submitted the voting system or component for examination. [2003 c 111 s 304. Prior: 1990 c 59 s 20; 1982 c 40 s 3. Formerly RCW 29.33.061.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Severability—1982 c 40: See note following RCW 29A.12.020.

RCW 29A.12.050 Approval required—Modification. If voting systems or 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 approved under this chapter or the former chapter 29.34 RCW before March 22, 1982, may be used. Any 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 reexamination or reapproval by the secretary of state under RCW 29A.12.020. [2003 c 111 s 305; 1990 c 59 s 21; 1982 c 40 s 4. Formerly RCW 29.33.081.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Severability—1982 c 40: See note following RCW 29A.12.020.

RCW 29A.12.060 Maintenance and operation. The county auditor of a county in which voting systems are used is responsible for the preparation, maintenance, and operation of those systems and may employ and direct persons to perform some or all of these functions. [2003 c 111 s 306. Prior: 1990 c 59 s 22; 1965 c 9 s 29.33.130; prior: 1955 c 323 s 2; prior: 1935 c 85 s 1, part; 1919 c 163 s 23, part; 1915 c 114 s 5, part; 1913 c 58 s 10, part; RRS s 5309, part. Formerly RCW 29.33.130.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

RCW 29A.12.070 Acceptance and vulnerability tests. An agreement to purchase or lease a voting system or a component of a voting system is subject to that system or component passing:

(1) An acceptance test sufficient to demonstrate that the equipment is the same as that certified by the secretary of state and that the equipment is operating correctly as delivered to the county; and

(2) A vulnerability test conducted by a federal or state public entity which includes participation by local elections officials. [2020 c 101 s 3; 2003 c 111 s 307. Prior: 1998 c 58 s 1; 1990 c 59 s 23. Formerly RCW 29.33.145.]

Findings—Intent—2020 c 101: See note following RCW 29A.12.200.

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

RCW 29A.12.080 Requirements for approval. No voting device shall be approved by the secretary of state unless it:

(1) Secures to the voter secrecy in the act of voting;

(2) Permits the voter to vote for any person for any office and upon any measure that he or she has the right to vote for;

(3) Correctly registers all votes cast for any and all persons and for or against any and all measures;

(4) Provides that a vote for more than one candidate cannot be cast by one single operation of the voting device or vote tally system except when voting for president and vice president of the United States; and

(5) Except for functions or capabilities unique to this state, has been tested and certified by an independent testing authority designated by the United States election assistance commission. [2013 c 11 s 22; 2006 c 207 s 2; 2003 c 111 s 308. Prior: 1990 c 59 s 26; 1982 c 40 s 6; 1977 ex.s. c 361 s 66; 1971 ex.s. c 6 s 1; 1967 ex.s. c 109 s 18. Formerly RCW 29.33.300, 29.34.080.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Severability—1982 c 40: See note following RCW 29A.12.020.

Effective date—Severability—1977 ex.s. c 361: See notes following RCW 29A.16.040.

Severability—1971 ex.s. c 6: "If any provision of this 1971 amendatory act, or its application to any person or circumstance is held invalid, the remainder of the act, or the application of the provision to other persons or circumstances is not affected." [1971 ex.s. c 6 s 3.]

Voting devices, machines—Recording requirements: RCW 29A.12.150.

RCW 29A.12.085 Paper record. Beginning on January 1, 2006, all direct recording electronic voting devices must produce a paper record of each vote that may be accepted or rejected by the voter before finalizing his or her vote. This record may not be removed from the voting center, and must be human readable without an interface and machine readable for counting purposes. If the device is programmed to display the ballot in multiple languages, the paper record produced must be printed in the language used by the voter. Rejected records must either be destroyed or marked in order to clearly identify the record as rejected. Paper records produced by direct recording electronic voting devices are subject to all the requirements of chapter 29A.60 RCW for ballot handling, preservation, reconciliation, transit, and storage. The paper records must be preserved in the same manner and for the same period of time as ballots. [2011 c 10 s 22; 2005 c 242 s 1.]

Notice to registered poll voters—Elections by mail—2011 c 10: See note following RCW 29A.04.008.

Preservation: RCW 29A.60.095.

Unauthorized removal from voting center: RCW 29A.84.545.

RCW 29A.12.101 Requirements of tallying systems for approval. The secretary of state shall not approve a vote tallying system unless it:

(1) Correctly counts votes on ballots on which the proper number of votes have been marked for any office or issue;

(2) Ignores votes marked for any office or issue where more than the allowable number of votes have been marked, but correctly counts the properly voted portions of the ballot;

(3) Accumulates a count of the specific number of ballots tallied for each precinct, total votes by candidate for each office, and total votes for and against each issue of the ballot in that precinct;

(4) Produces precinct and cumulative totals in printed form; and

(5) Except for functions or capabilities unique to this state, has been tested and certified by an independent testing authority designated by the United States election assistance commission. [2006 c 207 s 3; 2004 c 271 s 109.]

RCW 29A.12.110 Record of programming—Devices sealed. In preparing a voting device for a primary or election, a record shall be made of the programming installed in each device. Except where provided by a rule adopted under RCW 29A.04.611, after being prepared for a primary or election, each device shall be sealed with a uniquely numbered seal. The programmed memory pack for each voting device must be sealed into the device during final preparation and logic and accuracy testing. Except in the case of a device breakdown or error in programming, the memory pack must remain sealed in the device until after 8:00 p.m. on the day of the primary, special election, or general election. [2011 c 10 s 23; 2003 c 111 s 311; 1990 c 59 s 25. Formerly RCW 29.33.330.]

Notice to registered poll voters—Elections by mail—2011 c 10: See note following RCW 29A.04.008.

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

RCW 29A.12.120 Counting center personnel—Instruction, requirements. (1) Before each state primary or general election at which voting systems are to be used, the county auditor shall instruct all counting center personnel who will operate a voting system in the proper conduct of their voting system duties.

(2) The county auditor may waive instructional requirements for counting center personnel who have previously received instruction and who have served for a sufficient length of time to be fully qualified to perform their duties. The county auditor shall keep a record of each person who has received instruction and is qualified to serve at the subsequent primary or election.

(3) No person may operate a voting system in a counting center at a primary or election unless that person has received the required instruction and is qualified to perform his or her duties in connection with the handling and tallying of ballots for that primary

or election. [2013 c 11 s 23; 2011 c 10 s 24; 2003 c 111 s 312. Prior: 1990 c 59 s 29; 1977 ex.s. c 361 s 69. Formerly RCW 29.33.340, 29.34.143.]

Notice to registered poll voters—Elections by mail—2011 c 10: See note following RCW 29A.04.008.

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Effective date—Severability—1977 ex.s. c 361: See notes following RCW 29A.16.040.

RCW 29A.12.130 Tallying systems—Programming tests. At least three days before each state primary or general election, the office of the secretary of state shall provide for the conduct of tests of the programming for each vote tallying system to be used at that primary or general election. The test must verify that the system will correctly count the vote cast for all candidates and on all measures appearing on the ballot at that primary or general election. The test shall verify the capability of the vote tallying system to perform all of the functions that can reasonably be expected to occur during conduct of that particular primary or election. If any error is detected, the cause shall be determined and corrected, and an errorless total shall be produced before the primary or election.

Such tests shall be observed by at least one representative from each major political party, if representatives have been appointed by the respective major political parties and are present at the test, and shall be open to candidates, the press, and the public. The county auditor and any political party observers shall certify that the test has been conducted in accordance with this section. Copies of this certification shall be retained by the secretary of state and the county auditor. All programming materials, test results, and test ballots shall be securely sealed until the day of the primary or general election. [2003 c 111 s 313; 1998 c 58 s 2; 1990 c 59 s 32; 1977 ex.s. c 361 s 73. Formerly RCW 29.33.350, 29.34.163.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Effective date—Severability—1977 ex.s. c 361: See notes following RCW 29A.16.040.

RCW 29A.12.140 Operating procedures. The secretary of state may publish recommended procedures for the operation of the various vote tallying systems that have been approved. These procedures allow the office of the secretary of state to restrict or define the use of approved systems in elections. [2003 c 111 s 314. Prior: 1998 c 58 s 3; 1990 c 59 s 34; 1977 ex.s. c 361 s 75; 1967 ex.s. c 109 s 32. Formerly RCW 29.33.360, 29.34.170.]

Intent—Effective date—1990 c 59: See notes following RCW 29A.04.013.

Effective date—Severability—1977 ex.s. c 361: See notes following RCW 29A.16.040.

RCW 29A.12.150 Recording requirements. The secretary of state shall not certify under this title any voting device or machine for use in conducting a primary or general or special election in this state unless the device or machine correctly records on a separate ballot the votes cast by each elector for any person and for or against any measure and such separate ballots are available for audit purposes after such a primary or election. [2013 c 11 s 24; 2003 c 111 s 315; 1998 c 245 s 26; 1991 c 363 s 30; 1990 c 184 s 1. Formerly RCW 29.04.200.]

Purpose—Captions not law—1991 c 363: See notes following RCW 2.32.180.

RCW 29A.12.160 Blind or visually impaired voter accessibility. (1) At each voting center, at least one voting unit certified by the secretary of state shall provide access to individuals who are blind or visually impaired.

(2) For purposes of this section, the following definitions apply:

(a) "Accessible" includes receiving, using, selecting, and manipulating voter data and controls.

(b) "Nonvisual" includes synthesized speech, Braille, and other output methods.

(c) "Blind and visually impaired" excludes persons who are both deaf and blind. [2011 c 10 s 25; 2004 c 267 s 701; 2004 c 266 s 3. Prior: 2003 c 110 s 1. Formerly RCW 29.33.305.]

Notice to registered poll voters—Elections by mail—2011 c 10: See note following RCW 29A.04.008.

Effective dates—2004 c 267: See note following RCW 29A.08.010.

Effective date—2004 c 266: See note following RCW 29A.04.575.

RCW 29A.12.180 Disclosure of security breaches—Use of intrusion detection system. (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) 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) Notification under this section must be made in the most expedient time possible and without unreasonable delay. [2024 c 28 s 1; 2018 c 218 s 6.]

Intent—2018 c 218: See note following RCW 29A.60.185.

RCW 29A.12.190 Decertification. (1) The secretary of state may decertify a voting system or any component of a voting system and withdraw authority for its future use or sale in the state if, at any time after certification, the secretary of state determines that:

(a) The system or component fails to meet the standards set forth in applicable federal guidelines;

(b) The system or component was materially misrepresented in the certification application;

(c) The applicant has installed unauthorized modifications to the certified software or hardware; or

(d) Any other reason authorized by rule adopted by the secretary of state.

(2) The secretary of state may decertify a voting system or any component of a voting system and withdraw authority for its future use or sale in the state if the manufacturer or distributor of the voting system or component thereof fails to comply with the notification requirements of RCW 29A.12.180. [2018 c 218 s 7.]

Intent—2018 c 218: See note following RCW 29A.60.185.

RCW 29A.12.200 Security breach identification and reporting. (1) The secretary of state must annually consult with the Washington state fusion center, state chief information officer, and each county auditor to identify instances of security breaches of election systems or election data.

(2) To the extent possible, the secretary of state must identify whether the source of a security breach, if any, is a foreign entity, domestic entity, or both.

(3) By December 31st of each year, the secretary of state must submit a report to the governor, state chief information officer, Washington state fusion center, and the chairs and ranking members of the appropriate legislative committees from the senate and house of representatives that includes information on any instances of security breaches identified under subsection (1) of this section and options to increase the security of the election systems and election data, and to prevent future security breaches. The report, and any related material, data, or information provided pursuant to subsection (1) of this section or used to assemble the report, may only be distributed to, or otherwise shared with, the individuals specifically mentioned in this subsection (3).

(4) For the purposes of this section:

(a) "Domestic entity" means an entity organized or formed under the laws of the United States, a person domiciled in the United States, or a citizen of the United States, and includes elected officials and staff of the state or a county.

(b) "Foreign entity" means 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.

(c) "Security breach" means 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. [2024 c 28 s 2; 2020 c 101 s 2.]

Findings—Intent—2020 c 101: "The legislature finds that public confidence in state elections systems and election data are of

paramount consideration to the integrity of the voting process. The legislature also finds that recent events have revealed an intentional and persistent effort by foreign entities to influence election systems and other cybernetworks. Therefore, the legislature intends to review the state's electoral systems and processes and take appropriate measures to identify whether foreign entities were responsible for the intrusions." [2020 c 101 s 1.]