Z-0477.4

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SENATE BILL 5843**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State of Washington 68th Legislature 2024 Regular Session**

**By** Senators Nguyen, Boehnke, Hasegawa, Hunt, Kuderer, Mullet, Nobles, Randall, and Valdez; by request of Secretary of State

AN ACT Relating to security breaches of election systems and election-related systems; amending RCW 29A.12.180, 29A.12.200, 29A.40.100, 29A.40.160, 29A.60.200, 29A.84.550, 29A.84.560, 29A.84.720, and 29A.84.050; adding a new section to chapter 29A.84 RCW; and prescribing penalties.

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

**Sec.**  RCW 29A.12.180 and 2018 c 218 s 6 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) 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 ((~~subsection (1) of~~)) this section must be made in the most expedient time possible and without unreasonable delay.

**Sec.**  RCW 29A.12.200 and 2020 c 101 s 2 are each amended to read as follows:

(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.

((~~(b)~~)) (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.

**Sec.**  RCW 29A.40.100 and 2011 c 10 s 40 are each amended to read as follows:

County auditors must request that observers be appointed by the major political parties to be present during the processing of ballots at the counting center. County auditors have discretion to also request that observers be appointed by any campaigns or organizations. The absence of the observers will not prevent the processing of ballots if the county auditor has requested their presence. Observers may not touch any ballots, ballot materials, or election systems. Unauthorized physical contact, or access to ballots or election systems is a crime subject to punishment under chapter 29A.84 RCW.

**Sec.**  RCW 29A.40.160 and 2022 c 69 s 1 are each amended to read as follows:

(1) Each county auditor shall open a voting center each primary, special election if the county is conducting an election, and general election. The voting center shall be open during business hours during the voting period, which begins eighteen days before, and ends at 8:00 p.m. on the day of, the primary, special election if the county is conducting an election, or general election.

(2) Each county auditor shall open a voting center at each of the following locations in the county:

(a) At the county auditor's office or at the division of elections that is in a separate location from the county auditor's office; and

(b) For each presidential general election, in each city in the county with a population of one hundred thousand or greater which does not have a voting center as required in (a) of this subsection. A voting center opened pursuant to this subsection (2) is not required to be open on the Sunday before the presidential election.

(3) Voting centers shall be located in public buildings or buildings that are leased by a public entity including, but not limited to, libraries.

(4) Each voting center, and at least one of the other locations designated by the county auditor to allow voters to register in person pursuant to RCW 29A.08.140(1)(b), must provide voter registration materials, ballots, provisional ballots, disability access voting units, sample ballots, instructions on how to properly vote the ballot, a ballot drop box, and voters' pamphlets, if a voters' pamphlet has been published.

(5) Each voting center must be accessible to persons with disabilities. Each state agency and entity of local government shall permit the use of any of its accessible facilities as voting centers when requested by a county auditor.

(6) Each voting center must provide at least one voting unit certified by the secretary of state that provides access to individuals who are blind or visually impaired, enabling them to vote with privacy and independence.

(7) No person may interfere with a voter attempting to vote in a voting center. Interfering with a voter attempting to vote is a violation of RCW 29A.84.510. The county auditor shall designate by administrative rule a specific point or points as the entrance to each voting center, taking into account the unique attributes of the voting center, to assure that voters have the ability to arrive and depart unimpeded.

(8) No person may interfere with the operation of a voting center. Interfering with the operation of a voting center is a violation of RCW 29A.84.510. This prohibition includes unauthorized access or handling of ballots, and unauthorized access to any voting equipment or election systems. Unauthorized access includes elected officials and county staff accessing systems in any manner not required by their job function.

(9) Before opening the voting center, the voting equipment shall be inspected to determine if it has been properly prepared for voting. If the voting equipment is capable of direct tabulation of each voter's choices, the county auditor shall verify that no votes have been registered for any issue or office, and that the device has been sealed with a unique numbered seal at the time of final preparation and logic and accuracy testing. A log must be made of all device numbers and seal numbers.

((~~(9)~~)) (10) The county auditor shall require any person desiring to vote at a voting center to either sign a ballot declaration or provide identification.

(a) The signature on the declaration must be compared to the signature on the voter registration record before the ballot may be counted. If the voter registered using a mark, or can no longer sign ((~~his or her~~)) the voter's name, the election officers shall require the voter to be identified by another registered voter.

(b) The identification must be valid photo identification, such as a driver's license, state identification card, student identification card, tribal identification card, or employer identification card. A tribal identification card is not required to include a residential address or an expiration date to be considered valid under this section. Any individual who desires to vote in person but cannot provide identification shall be issued a provisional ballot, which shall be accepted if the signature on the declaration matches the signature on the voter's registration record.

((~~(10)~~)) (11) Provisional ballots must be accompanied by a declaration and security envelope, as required by RCW 29A.40.091, and space for the voter's name, date of birth, current and former registered address, reason for the provisional ballot, and disposition of the provisional ballot. The voter shall vote and return the provisional ballot at the voting center. The voter must be provided information on how to ascertain whether the provisional ballot was counted and, if applicable, the reason why the vote was not counted.

((~~(11)~~)) (12) Any voter may take printed or written material into the voting device to assist in casting ((~~his or her~~)) votes. The voter shall not use this material to electioneer and shall remove it when ((~~he or she leaves~~)) leaving the voting center.

((~~(12)~~)) (13) If any voter states that ((~~he or she~~)) the voter is unable to cast ((~~his or her votes~~)) a vote due to a disability, the voter may designate a person of ((~~his or her~~)) the voter's choice, or two election officers, to enter the voting booth and record the votes as ((~~he or she~~)) the voter directs.

((~~(13)~~)) (14) No voter is entitled to vote more than once at a primary, special election, or general election. If a voter incorrectly marks a ballot, ((~~he or she~~)) the voter may be issued a replacement ballot.

((~~(14)~~)) (15) A voter who has already returned a ballot but requests to vote at a voting center shall be issued a provisional ballot. The canvassing board shall not count the provisional ballot if it finds that the voter has also voted a regular ballot in that primary, special election, or general election.

((~~(15)~~)) (16) Any voter who is inside or in line at the voting center at 8:00 p.m. on the day of the primary, special election, or general election must be allowed to vote.

((~~(16)~~)) (17) For each primary, special election, and general election, the county auditor may provide election services at locations in addition to the voting center. The county auditor has discretion to establish which services will be provided at the additional locations, and which days and hours the locations will be open.

**Sec.**  RCW 29A.60.200 and 2011 c 10 s 60 are each amended to read as follows:

(1) Before canvassing the returns of a primary or election, the chair of the county legislative authority or the chair's designee shall administer an oath to the county auditor or the auditor's designee attesting to the authenticity of the information presented to the canvassing board. This oath must be signed by the county auditor or designee and filed with the returns of the primary or election.

(2) The county canvassing board shall proceed to verify the results from the ballots received. The board shall execute a certificate of the results of the primary or election signed by all members of the board or their designees. Failure to certify the returns, if they can be ascertained with reasonable certainty, is a crime under RCW 29A.84.720.

(3) If the county canvassing board refuses to certify the results of the election without cause, the secretary of state may examine the records, ballots, and results of the election and certify the results of the election. This must be completed within two business days after the certification deadline in RCW 29A.60.190 after the refusal of the county canvassing board to certify the results of the election.

**Sec.**  RCW 29A.84.550 and 2011 c 10 s 74 are each amended to read as follows:

Any person who willfully defaces, removes, or destroys any of the supplies or materials that the person knows are intended both for use in a voting center ((~~and~~)), election office, ballot counting area, ballot storage area, or election system including materials and systems meant for enabling a voter to prepare ((~~his or her~~)) the voter's ballot is guilty of a class C felony punishable under RCW 9A.20.021.

NEW SECTION. **Sec.**  A new section is added to chapter 29A.84 RCW to read as follows:

Any person who willfully and without authority accesses or assists another person or entity with unauthorized access to a voting center, election office, ballot counting area, ballot storage area, or any election system, or provides unauthorized access to another person or entity to a voting center, election office, ballot counting area, ballot storage area, or any election system, whether electronic or physical access, is guilty of a class C felony punishable under RCW 9A.20.021.

**Sec.**  RCW 29A.84.560 and 2003 c 111 s 2126 are each amended to read as follows:

Any person who tampers with or damages or attempts to damage any voting machine or device to be used or being used in a primary or special or general election, or who prevents or attempts to prevent the correct operation of such machine or device, or any unauthorized person who ((~~makes or has in his or her possession a key to a~~)) accesses or assists another person or entity with unauthorized access to a voting center, election office, ballot counting area, ballot storage area, or election system, voting machine, or device to be used or being used in a primary or special or general election, is guilty of a class C felony punishable under RCW 9A.20.021.

**Sec.**  RCW 29A.84.720 and 2003 c 111 s 2138 are each amended to read as follows:

Every person charged with the performance of any duty under the provisions of any law of this state relating to elections, including primaries, or the provisions of any charter or ordinance of any city or town of this state relating to elections who willfully neglects or refuses to perform such duty, or provides unauthorized access to a person or entity to physical locations or electronic or physical access to election software or hardware used in any element of conduct of an election, or who, in the performance of such duty, or in ((~~his or her~~)) the person's official capacity, knowingly or fraudulently violates any of the provisions of law relating to such duty, is guilty of a class C felony punishable under RCW 9A.20.021 and shall forfeit ((~~his or her~~)) the person's office.

**Sec.**  RCW 29A.84.050 and 2011 c 10 s 68 are each amended to read as follows:

(1) A person who knowingly destroys, alters, defaces, conceals, or discards a completed voter registration form ((~~or~~)), signed ballot declaration, or voted ballot is guilty of a gross misdemeanor. This section does not apply to (a) the voter who completed the form or declaration, or (b) a county auditor who acts as authorized by law.

(2) Any person who intentionally fails to return another person's completed voter registration form ((~~or~~)), signed ballot declaration, or voted ballot to the proper state or county elections office by the applicable deadline is guilty of a gross misdemeanor.

**--- END ---**