H-0805.1

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

**HOUSE BILL 1708**

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

**State of Washington 68th Legislature 2023 Regular Session**

**By** Representatives Volz, Abbarno, Walsh, Schmidt, Schmick, Corry, Couture, Hutchins, Harris, Dent, Low, Klicker, Cheney, McClintock, Chambers, Robertson, Barnard, Sandlin, Jacobsen, and Eslick

AN ACT Relating to requiring each ballot to have a unique serial number that permits a voter to view their voted ballot through an online portal; amending RCW 29A.40.091, 29A.40.130, and 42.56.420; and adding a new section to chapter 29A.40 RCW.

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

**Sec.**  RCW 29A.40.091 and 2021 c 10 s 3 are each amended to read as follows:

(1) The county auditor shall send each voter a ballot, a security envelope in which to conceal the ballot after voting, a larger envelope in which to return the security envelope, a declaration that the voter must sign, and instructions on how to obtain information about the election, how to mark the ballot, and how to return the ballot to the county auditor. The calendar date of the election must be prominently displayed in bold type, twenty-point font or larger, on the envelope sent to the voter containing the ballot and other materials listed in this subsection((~~:~~

~~(a) For all general elections in 2020 and after;~~

~~(b) For all primary elections in 2021 and after; and~~

~~(c) For all elections in 2022 and after~~)).

(2) The ballot must be imprinted with a 16-digit serial number that is unique to each voter in each election, and it must be accompanied by a detachable copy of the number for the voter to keep. The county auditor may not retain any documentation that connects the serial number to a particular voter's identity.

(3) The voter must swear under penalty of perjury that he or she meets the qualifications to vote, and has not voted in any other jurisdiction at this election. The declaration must clearly inform the voter that it is illegal to vote if he or she is not a United States citizen; it is illegal to vote if he or she is serving a sentence of total confinement under the jurisdiction of the department of corrections for a felony conviction or is currently incarcerated for a federal or out-of-state felony conviction; and it is illegal to cast a ballot or sign a ballot declaration on behalf of another voter. The ballot materials must provide space for the voter to sign the declaration, indicate the date on which the ballot was voted, and include a telephone number.

((~~(3)~~)) (4) For overseas and service voters, the signed declaration constitutes the equivalent of a voter registration. Return envelopes for overseas and service voters must enable the ballot to be returned postage free if mailed through the United States postal service, United States armed forces postal service, or the postal service of a United States foreign embassy under 39 U.S.C. 3406.

((~~(4)~~)) (5) The voter must be instructed to either return the ballot to the county auditor no later than 8:00 p.m. the day of the election or primary, or mail the ballot to the county auditor with a postmark no later than the day of the election or primary. Return envelopes for all election ballots must include prepaid postage. Service and overseas voters must be provided with instructions and a privacy sheet for returning the ballot and signed declaration by fax or email. A voted ballot and signed declaration returned by fax or email must be received by 8:00 p.m. on the day of the election or primary.

((~~(5)~~)) (6) The county auditor's name may not appear on the security envelope, the return envelope, or on any voting instructions or materials included with the ballot if he or she is a candidate for office during the same year.

((~~(6)~~)) (7) For purposes of this section, "prepaid postage" means any method of return postage paid by the county or state.

NEW SECTION. **Sec.**  A new section is added to chapter 29A.40 RCW to read as follows:

The secretary of state must create an online portal in which voters can input the serial number associated with their ballot in order to view an electronic record of all the votes cast on their ballot.

**Sec.**  RCW 29A.40.130 and 2011 c 10 s 42 are each amended to read as follows:

(1) Each county auditor shall maintain in his or her office, open for public inspection, a record of all voters issued a ballot and all voters who returned a ballot. For each primary, special election, or general election, any political party, committee, or person may request a list of all registered voters who have or have not voted. Such requests shall be handled as public records requests pursuant to chapter 42.56 RCW.

(2) Within 30 days after a primary, special election, or general election, each county auditor must scan and upload a copy of each voted ballot into the online portal created by the secretary of state under section 2 of this act.

**Sec.**  RCW 42.56.420 and 2022 c 140 s 1 are each amended to read as follows:

The following information relating to security is exempt from disclosure under this chapter:

(1) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:

(a) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and

(b) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism;

(2) Those portions of records containing specific and unique vulnerability assessments or specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility, or secure facility for persons civilly confined under chapter 71.09 RCW, the public disclosure of which would have a substantial likelihood of threatening the security of a city, county, or state adult or juvenile correctional facility, secure facility for persons civilly confined under chapter 71.09 RCW, or any individual's safety;

(3) Information compiled by school districts or schools in the development of their comprehensive safe school plans under RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school;

(4) Information regarding the public and private infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of security, information technology infrastructure, or assets;

(5) The system security and emergency preparedness plan required under RCW 35.21.228, 35A.21.300, 36.01.210, 36.57.120, 36.57A.170, and 81.112.180;

(6) Personally identifiable information of employees, and other security information, of a private cloud service provider that has entered into a criminal justice information services agreement as contemplated by the United States department of justice criminal justice information services security policy, as authorized by 28 C.F.R. Part 20; and

(7)(a) In addition to the information in subsection (4) of this section, the following related to election security:

(i) The continuity of operations plan for election operations and any security audits, security risk assessments, or security test results, relating to physical security or cybersecurity of election operations or infrastructure. These records are exempt from disclosure in their entirety;

(ii) Those portions of records containing information about election infrastructure, election security, or potential threats to election security, the public disclosure of which may increase risk to the integrity of election operations or infrastructure; ((~~and~~))

(iii) Voter signatures on ballot return envelopes, ballot declarations, and signature correction forms, including the original documents, copies, and electronic images; and a voter's phone number and email address contained on ballot return envelopes, ballot declarations, or signature correction forms. The secretary of state, by rule, may authorize in-person inspection of unredacted ballot return envelopes, ballot declarations, and signature correction forms in accordance with RCW 29A.04.260;

(iv) Any information or documents related to the development, maintenance, and administration of the portal established in section 2 of this act; and

(v) Any data that has been uploaded to the portal established in section 2 of this act.

(b) The exemptions specified in (a) of this subsection do not include information or records pertaining to security breaches, except as prohibited from disclosure pursuant to RCW 29A.12.200.

(c) The exemptions specified in (a) of this subsection do not prohibit an audit authorized or required under Title 29A RCW from being conducted.

**--- END ---**