Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

State Government, Elections & Information Technology Committee

HB 2406

Brief Description: Concerning election security practices around auditing and equipment.

Sponsors: Representatives Hudgins, Stanford and Ormsby.

Brief Summary of Bill

- Requires the county auditor to audit the election results, prior to certification of the election, using at least one of four methods provided and authorizes sealed ballot containers to be opened for such audits.
- Requires a manufacturer or distributor of a certified voting system or component thereof to disclose of certain breaches of its security system.
- Provides for a decertification process of voting systems or components thereof that is permissive if the Secretary of State determines that it no longer conforms to generally accepted safety requirements, and mandatory for failure of a manufacturer or distributor to disclose of certain breaches of its security system.

Hearing Date: 1/12/18

Staff: Desiree Omli (786-7105).

Background:

Election audits.
Prior to certification of the election, the county auditor must audit the results of votes cast on the direct recording electronic voting devices (DRE). A DRE is a machine that directly records a voter's choice. All DREs must produce a paper record of each vote that may be accepted or rejected by the voter before finalizing their vote. To audit the DRE, the county auditor must randomly select up to four percent of the DRE devices or one DRE, whichever is greater, and compare the results recorded electronically on each DRE selected with the results shown on the paper record produced by the same machine.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

In addition to an audit of votes cast on the DRE, a random check of the ballot counting equipment used to tabulate ballots may be conducted at the discretion of the county auditor, or upon mutual agreement of the political party observers. Under the random check process, a manual count of ballots is compared to the machine count. The size of the random check may involve up to either three precincts or six batches.

Ballot containers.
After a ballot is tabulated, all ballots must be sealed in containers that identify the specific primary or election. The containers may only be opened by the canvassing board as part of the canvass, to conduct recounts, to conduct a random check of the original ballot counting equipment, or by order of the superior court in a contest or election dispute.

Voting systems.
A "voting system" is the total combination of mechanical, electromechanical, or electronic equipment including the software, firmware, and documentation required to program, control, and support the equipment that is used to define ballots, cast and count votes, report or display election results, and maintain and produce any audit trail information.

The Secretary of State (Secretary) must inspect and certify all voting systems, or component of a system, prior to its use in the state. Under administrative rule, the Secretary may decertify a voting system or component thereof and withdraw authority for its future use or sale in the state if: (1) the system or component fails to meet the standards set in federal guidelines or state statute or rules; (2) the system or component was materially misrepresented in the certification or application process; or (3) the manufacturer or distributor installed unauthorized modifications to the certified software or hardware.

Summary of Bill:

Election Audit.
Prior to certification of the election, the county auditor must conduct an audit using at least one of the following methods:

1. Audit of the DRE or other in-person ballot marking system.
   An audit of DREs is not required unless the county auditor chooses this audit method. If so, all other in-person ballot marking systems (systems) are subject to the same audit requirements as DREs. This audit method may be used if there are races or issues with greater than 10 votes cast on all DREs or other system in the county, or the number of votes cast on the DREs or systems is statistically significant in relation to the election result.

2. Random check of the ballot counting equipment.
   A random check may also be done by comparing the electronic count to the machine count from the original ballot counting equipment. The procedures adopted by the county canvassing board must comply with the rules adopted by the Secretary for the implementation and administration of audits. In addition, the procedures must include a process for expanding the audit in cases where a discrepancy is found.

3. Risk-limiting audit.
   A risk-limiting audit is an audit protocol that makes use of statistical principles and methods and is designed to limit the risk of certifying an incorrect election outcome. There are two types of risk-limiting audits. The first type is a "comparison risk-limiting audit", in which the county auditor compares the voter markings on the ballot to the ballot-level cast vote record produced by the ballot counting equipment. The second type is a "ballot polling risk-limiting audit", which is used in counties where the ballot counting equipment does not produce a ballot-level cast vote record. In a ballot polling risk-limiting audit, the county auditor reports the markings on randomly selected ballots until the prespecified risk limit is met.

   The Secretary must:
   - set the risk limit, which is the largest statistical probability that an incorrect reported tabulation outcome is not detected in a risk-limiting audit;
   - select at least one statewide contest, and at least one other ballot contest for each county, to audit; and
   - establish procedures for implementation of risk-limiting audits.

4. Independent electronic audit of the original ballot counting equipment.
   In an independent electronic audit of the original ballot counting equipment used in the county, the county auditor may choose to audit all ballots cast, or limit the audit to three precincts or six batches. The method of auditing must comply with procedures adopted by the county canvassing board.

   The audit tool used must be an independent electronic audit system that is at least:
   - approved by the Secretary,
   - completely independent from all voting systems,
   - distributed or manufactured by a vendor different from the distributor or manufacturer of the original ballot counting equipment, and
   - capable of demonstrating that it can verify and confirm the accuracy of the original ballot counting equipment.

For each audit method, the Secretary must adopt procedures for expanding the audit to include additional ballots when the initial audit results in a discrepancy. Separate from such process, at the discretion of the county auditor or upon request of a candidate, officer of a political party, or any group of five or more registered voters, an additional number of ballots may be audited to supplement the audits conducted. The Secretary must determine the number of additional ballots that may be audited. A person who requests a supplemental audit is subject to the same cost structure as for recounts. If a discrepancy is found during an audit of supplemental ballots, the procedures for auditing in cases of a discrepancy must be followed.

The Secretary must establish rules to implement and administer the auditing methods above.

Ballot Containers.
The sealed containers may be opened to conduct an audit of the DRE or other in-person ballot marking system, a risk-limiting audit, and an independent electronic audit of the original ballot counting equipment.

Voting Systems.
A voting system also includes mechanical, electromechanical, or electronic equipment that is used to perform an audit. A manufacturer or distributor of a certified voting system or component thereof must disclose to the Secretary and Attorney General any breach of the security of its system immediately, and without unreasonable delay, following discovery of the breach if:

- the breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election in any state; or
- 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. "Personal information" includes a person's first name, or their first initial and last name, in combination with at least one of the following data elements: (1) social security number; (2) driver's license number or state identification card; or (3) the number of an account, credit or debit card, in combination with a code that would permit access to the person's financial account.

The Secretary must decertify a voting system or component thereof and withdraw authority for its future use or sale in the state if the manufacturer or distributor of the system or component fails to comply with notification requirements in cases where notification of a breach is required. The Secretary may otherwise decertify a voting system or component thereof and withdraw authority for its future use or sale in the state if the Secretary determines that it no longer conforms with the statutory requirements, adopted rules, or generally accepted safety requirements.

Appropriation: None.

Fiscal Note: Not requested.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.