SENATE BILL REPORT
ESHB 2406

As of February 22, 2018

Title: An act relating to ensuring the integrity of elections through strengthening election security practices around auditing and equipment.

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

Sponsors: House Committee on State Govt, Elections & IT (originally sponsored by Representatives Hudgins, Stanford and Ormsby).

Brief History: Passed House: 2/12/18, 97-1.
Committee Activity: State Government, Tribal Relations & Elections: 2/21/18.

Brief Summary of Bill

- Requires the county auditor to audit duplicated ballots and electronic ballot return systems under certain circumstances, and conduct a random check of ballot counting equipment.
- Authorizes the use of certain audit methods to conduct audits in addition to the random check.
- Requires the Secretary of State (Secretary) to survey and report on county canvassing board procedures for random checks of ballot counting equipment.
- Requires a manufacturer or distributor of a certified voting system or component thereof to disclose certain breaches of the security of its system.
- Authorizes the Secretary to decertify a voting system or component for certain reasons.

SENATE COMMITTEE ON STATE GOVERNMENT, TRIBAL RELATIONS & ELECTIONS

Staff: Samuel Brown (786-7470)

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.

Background: Election Audits. Prior to certifying an election, the county auditor must audit the results of votes cast on the direct recording electronic voting devices (DREs), which directly record a voter's choice. The county auditor must randomly select up to 4 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.

At the discretion of the county auditor, or upon mutual agreement of political party observers, a random check of ballot counting equipment may be conducted. Under the random check process, a manual count of ballots, involving either up to three precincts or six batches, is compared to the machine count.

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 contested election or election dispute.

Voting Systems. A voting system is the mechanical, electromechanical, or electronic equipment required to program, control, and support equipment used to define ballots, cast and count votes, report or display election results, and maintain and produce any audit trail information. The Secretary may decertify a voting system or component and withdraw authority for its future use or sale in the state if:

- the system or component fails to meet the standards set in federal guidelines or state statute or rules;
- the system or component was materially misrepresented in the certification or application process; or
- the manufacturer or distributor installed unauthorized modifications to the certified software or hardware.

Summary of Bill: The bill as referred to committee not considered.

Summary of Bill (Proposed Striking Amendment): Election Audits. Prior to election certification, the county auditor must conduct:

- a random check of at least 100 ballots each day ballots are certified, or all ballots certified if fewer than 100; and
- a comparison of duplicated ballots to original ballots, for which the county canvassing board must establish procedures.

The county auditor may also conduct an additional audit using any of the following methods:

- DRE or in-person ballot marking system audit;
- risk-limiting audit; or
- independent electronic audit.

For each audit method, the Secretary must adopt procedures for expanding the audit when the initial audit results in a discrepancy. 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, additional ballots may be audited. The Secretary determines 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.

The Secretary must establish rules to implement and administer the auditing methods. Sealed ballot containers may be opened to conduct an audit of duplicated ballots. The county auditor must also develop methods to regularly audit electronic ballot return systems when at least 100 ballots have been returned electronically by voters non-overseas or service voters.

Random Check. A random check compares the electronic count to the machine count from the original ballot counting equipment. The procedures adopted by the county canvassing board for random checks must comply with the rules adopted by the Secretary for the implementation and administration of audits and include a process for expanding the audit where a discrepancy is found. The requirement to complete the random check within 48 hours after election day is removed.

The Secretary of State must survey all random check procedures adopted by each county canvassing board and evaluate the procedures to identify best practices and discrepancies by November 1, 2018, and submit a report to the Legislature with recommendations for adopting best practices and uniform procedures for random checks by December 1, 2018.

DRE or In-Person Ballot Marking System Audit. If the county auditor chooses to audit DRE results, all other in-person ballot marking systems are subject to the same audit requirements. This audit method may be used if there are races or issues with more than ten votes cast on all DREs or in-person ballot marking systems in the county, or the number of votes cast on the DREs or in-person ballot marking systems is statistically significant.

Risk-Limiting Audit. A risk-limiting audit is an audit protocol that makes use of statistical principles and methods, designed to limit the risk of certifying an incorrect election outcome. There are two types of risk-limiting audits:

- the comparison risk-limiting audit, where the county auditor compares the voter markings on the ballot to the ballot-level cast vote record produced by the ballot counting equipment; and
- the 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 pre-specified risk limit is met.

The Secretary must establish procedures for implementation of risk-limiting audits, including setting the risk limit and selecting races for each county to audit.

Independent Electronic Audit. The county auditor may use an independent electronic audit system that is:

- 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.

The county auditor may choose to independently audit all ballots cast or limit the audit to three precincts or six batches.

Political Party Observers. The county auditor must request that political party observers be present at other locations where incoming ballots are handled and processed. Political party observers must have access to view various stages of processing incoming ballots, such as post-election audits, removal of ballots from drop boxes, and adjudication.

Voting Systems. Mechanical, electromechanical, or electronic audit equipment is added to the definition of voting system. A manufacturer or distributor of a certified voting system or component must immediately disclose to the Secretary and attorney general any security system breach if:

- the breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election in any state; or
- unsecured 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.

Voting System Decertification. The Secretary may decertify a voting system or component if:

- the system or component fails to meet federal standards;
- the system or component was materially misrepresented in the certification application;
- the applicant has installed unauthorized modifications to the certified software or hardware;
- the manufacturer or distributor of the system or component fails to comply with breach notification requirements; or
- pursuant to any reason authorized by rule adopted by the Secretary.

Appropriation: None.

Fiscal Note: Available. New fiscal note requested on February 16, 2018.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony: OTHER: We support mandatory random check audits and the choice of other audit types, and support working with the Secretary to develop best practices. We have concerns about the daily random check requirement, which is impractical and in some cases impossible, as it would reveal race results before election day. Every random check audit takes two hours and that frequency wouldn't provide any security enhancements. We also have concerns about the role of observers—they already have all this visibility. Risk-limiting audit methods recently used in Colorado will provide confidence that the count is accurate while using minimal resources.

Persons Testifying: OTHER: Julie Anderson, Washington Association of County Auditors; Stuart Holmes, Office of the Secretary of State.

Persons Signed In To Testify But Not Testifying: No one.