

# HOUSE BILL REPORT

## ESHB 2406

---

**As Passed House:**  
February 12, 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:**

**Committee Activity:**

State Government, Elections & Information Technology: 1/12/18, 1/23/18 [DPS].

**Floor Activity:**

Passed House: 2/12/18, 97-1.

### Brief Summary of Engrossed Substitute 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 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 of State (Secretary) to decertify a voting system or component thereof for certain reasons.

---

### HOUSE COMMITTEE ON STATE GOVERNMENT, ELECTIONS & INFORMATION TECHNOLOGY

**Majority Report:** The substitute bill be substituted therefor and the substitute bill do pass. Signed by 8 members: Representatives Hudgins, Chair; Dolan, Vice Chair; McDonald, Ranking Minority Member; Kraft, Assistant Ranking Minority Member; Appleton, Gregerson, Irwin and Pellicciotti.

---

*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.*

**Minority Report:** Without recommendation. Signed by 1 member: Representative Johnson.

**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 (DREs). 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 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.

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.

Political Party Observers.

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. However, the absence of observers will not prevent the processing of ballots if the county auditor requested their presence.

Duplication of Ballots.

The county auditor may refer a physically damaged, unreadable, or uncountable ballot to the county canvassing board, or duplicate the ballot if authorized by the county canvassing board. The procedure for duplication of ballots is set in statute. The original and duplicate ballots must be sealed in secured storage, except during duplication, inspection by the canvassing board, or tabulation.

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.

Reconciliation Report.

The county auditor must prepare, at the time of certification, an election reconciliation report that discloses certain information to reconcile the number of ballots counted with the number of voters credited with voting.

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 components 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 Engrossed Substitute Bill:**

#### Election Audit.

Prior to certification of the election, the county auditor must conduct:

1. a random check of the ballot counting equipment which involves a random check of at least 100 ballots per day, for each ballot counting equipment, until the results are certified; and
2. an audit of duplicated ballots that involves a comparison of the ballots duplicated to the original ballot, for which the county canvassing board must establish procedures.

The procedures around random checks are modified to authorize a random check by comparing the electronic count to the machine count from the original ballot counting equipment. In addition, the procedures adopted by the county canvassing board must comply with the rules adopted by the Secretary for the implementation and administration of audits, and must include a process for expanding the audit in cases where a discrepancy is found. The requirement to complete the random check no later than 48 hours after election day is removed.

The county auditor must also develop methods to regularly audit electronic ballot return systems when 100 or more ballots in any election have been returned electronically by voters who are not overseas voters or service voters.

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

1. Audit of the Direct Recording Electronic Voting Devices or Other In-Person Ballot Marking System.

The requirement to audit DREs is changed to be permissive. If an audit is conducted using this method, all other in-person ballot marking systems (systems) that retain or produce a voting record of each vote cast using the system are subject to the same audit requirements as the DREs. This audit method may be used if there are races or issues with greater than 10 votes cast on all DREs or other systems in the county.

2. 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 pre-specified 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, for audit. If there is no statewide contest, then the county auditor must select a ballot contest for audit; and
- establish procedures for implementation of risk-limiting audits.

3. 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: (1) approved by the Secretary; (2) completely independent from all voting systems; (3) distributed or manufactured by a vendor different from the distributor or manufacturer of the original ballot counting equipment; and (4) 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. The Secretary must adopt procedures to investigate the cause of any discrepancy found during an audit.

The Secretary must establish rules by January 1, 2019 to implement and administer the auditing practices above.

Political Party Observers.

The county auditor must request that political party observers also be present at other locations where election officials handle or process incoming ballots. 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.

Ballot Containers.

The sealed ballot containers may be opened to conduct an audit of the DRE or other in-person ballot marking system, a risk-limiting audit, an independent electronic audit of the original ballot counting equipment, and a random check of the ballot counting equipment. The sealed storage containing duplicated ballots and the originals may be opened to conduct an audit of the duplicated ballots.

### Reconciliation Report.

The reconciliation report must also include the number of replacement ballots requested, issued, received, counted, and rejected, as well as other information the Secretary deems necessary to maintain an audit trail.

### 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 may decertify a voting system or component thereof and withdraw authority for its future use or sale if the Secretary determines that:

- the system or component fails to meet the standards set forth in applicable federal guidelines;
- 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 notification requirements in cases where notification of a breach is required; or
- any other reason authorized by rule adopted by the Secretary.

**Appropriation:** None.

**Fiscal Note:** Available. New fiscal note requested on January 23, 2018.

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

### **Staff Summary of Public Testimony:**

(In support) Colorado is the first state to implement risk-limiting audits. Under the bill, risk-limiting audits are not required but is permissive if counties choose to audit using this method. This gives auditors more flexibility and the goal is to increase confidence in the process and strengthen processes that are already in place. The ultimate test of accuracy in close races is a recount, but making some sort of audit mandatory will do a good job to

augment what counties already do to test accuracy. Some in-person marking mechanisms do not retain information, so those machines will not be able to be audited. Auditing will increase voter confidence and trust in the system. Statistically based, post-election audits are an integral component of ensuring elections are secure and accurate. Such audits are the most economic component of a voting system that requires a small cost for a large benefit. Rhode Island recently passed robust election audit legislation.

Supplemental audits take time. It requires administrators to stop processing ballots and the public notification period is significant. If there is no reason triggering the expanded sample, there is no benefit to it. The bill is a step in the right direction, but should be more robust. There are checks and balances that can be put in place.

(Opposed) None.

(Other) All voting systems must be tested and certified by an independent testing authority designated by the federal Elections Assistance Commission prior to being inspected and tested by the Secretary. No voting system is or would be certified by the Secretary if it stores or requires voter personal information in order to cast a ballot. Recent data breaches in other states, such as Georgia and Illinois, were related to electronic poll books which are not used in Washington. Currently, the Secretary may decertify voting systems by rule. Elevating this to a statutory level is supported. Using methods related to risk-limiting audits will provide additional statistical evidence that the count was accurate, while keeping resources that auditors must use as low as possible. Four out of seven of the voting systems used in the state are capable of a comparison audit.

**Persons Testifying:** (In support) Representative Hudgins, prime sponsor; Julie Anderson, Washington Association of County Auditors; Greg Kinsey, Clark County Auditor; Kirstin Mueller, League of Women Voters; and Cindy Black, Fix Democracy First.

(Other) Stuart Holmes, Office of the Secretary of State; and Denice Carnahan.

**Persons Signed In To Testify But Not Testifying:** None.