LWV LEAGUE OF WOMEN VOTERS®
OF COLORADO

Election Security Position

The election process is the foundation of our representative form of government. Election integrity, accuracy, transparency, security, and trustworthiness require vigilance for public confidence.

Security requirements include but are not limited to:

1. **Voter registration databases** must be secure, accurate, regularly updated, transparent, and able to be independently audited. Individuals must be able to verify their own records and voting history;
2. **Chain of custody security** with strict protocols to show direct accountability and control of key systems and passwords - designate select personnel with appropriate expertise to enforce limited access to original ballots - strictly document ballot access times and places;
3. **Election officials, workers, and volunteers** must be qualified and trained, with no history of fraud or election offense, and no relationship to candidates;
4. **Ensuring sensitive task security** by team oversight, with no two team members from the same political party;
5. **Voting systems**, both hardware and software, must be supported, tested, accessible, and secure;
6. **Verifying voter eligibility** to cast a ballot via best practices that promote the ease and security of voting;
7. **Auditability**, requiring “software independence.” Election outcome changes or errors caused by software must be detectable without relying on software. We must ensure that accurate vote counts are possible, for example, by using voter-verifiable paper ballots which can be recounted;

8. **Voter-verifiability**, encouraging voters to confirm their votes, such as reviewing their easily verifiable paper ballots before casting them, and/or verifying that recording and tabulation occurred as the voters intended;
9. **Providing equitable voting access.** When a voter would otherwise be disenfranchised, we should work diligently to provide a voting method which is as secure as possible under the circumstances. If allowing less secure voting methods, such as online ballot return, limit use to the rare situation in which a voter cannot physically use and return a voter-verifiable paper ballot. Voters should be warned that all online methods will be less private as well as less secure;
10. **Voting systems** which allow recounts;
11. **Evidence-based election auditing** for all contests, including some risk-limiting audits
12. **Protecting individual voter's privacy** so ballots are not traceable to individual voters; and
13. **Developed and rehearsed contingency plans** for disasters and cybersecurity recovery.

More on Election Security:

Elections should be structured to provide transparent, verifiable, convincing evidence that the reported outcomes actually reflect how people voted (evidence-based elections).

Conducting elections securely and with ballot anonymity is much harder than doing banking securely because financial transaction details can be traced back to the originator, but ballots cannot. Additionally, although online banking security regularly fails, the customer's identity is known, and corrections and restitution can be made, even well after the fact. However, similar techniques cannot be used in online elections because ballots must not be traceable to individual voters.

All eligible voters should be able to vote privately and independently, with strong ballot protections and overall election security, including, where needed, electronic blank ballot delivery to voters, mailing paper ballots to uniformed and absentee overseas voters (UOCAVA) 45 days in advance, and providing accessible ballot marking equipment.

For those rare voters who may be allowed to return ballots online, use of a software-independent approach such as an end-to-end verifiable Internet voting system (E2E-VIV) is preferable - though it remains significantly less private and less secure than paper ballots.

Different vendors' election system components should communicate with each other in standardized ways (interoperability), so election officials can mix and match, encouraging innovation and competitive pricing.

Election officials should securely retain all paper and electronic records, including ballot images and cast vote records.

The public should have access to copies of election equipment source code, samples of election equipment, copies of ballots (with personally identifying information removed), and copies of procedures. Passwords and other authentication secrets must be secured. Election officials must remain in control of ballots and the actual equipment and software used.

Processes should be designed so that the public can observe the election, auditing, and testing processes closely enough to verify their integrity, but without interfering in an ongoing process. The public should have a mechanism to address election process flaws, if possible while an election is still underway, without interfering in ongoing elections.