LWV LEAGUE OF WOMEN VOTERS® OF COLORADO

# Election Security Study Material

OFFICIAL BALLOT DROP-OFF LOCATION - OPEN 24/7
This ballot drop-off location is open now and will remain open 24 hours a day until 7:00 pm Election Day
OFFICIAL BALLOT DROP-OFF LOCATION - OPEN 24/7
Official Ballot Drop Box
El Paso County Clerk & Recorder 719-575-VOTE (8683)
WARNING
BALLOT BOX UNDER 24 HOUR VIDEO SURVEILLANCE
COLORADO SPRINGS OLYMPIC CITY USA

**League of Women Voters of Colorado**
**December 2021**
**Election Security Team**
**Karen Sheek,** LWVCO President
**Toni Larson,** LWVCO Director for Action and Advocacy
**Gaythia Weis,** LWVCO Legislative Action Committee Member, Voting Rights
**Maud Naroll,** LWVCO Legislative Action Committee Member
**Neal McBurnett,** Election Integrity Consultant and LWV Boulder Member

# Election Security Study Material

The League of Women Voters recognizes that the right to vote is a fundamental principle of our democracy, and LWV is committed to expanding voter access.  It is also committed to defending democracy. Therefore, the League should promote election security, to minimize the risk that election outcomes are undermined. The League of Women Voters of Colorado needs a robust position on election security to help us advocate for further improvements and avoid compromising Colorado's achievements. Nationally, LWV's *Impact on Issues* also needs to give local leagues updated positions for advocacy. League positions should address the need for risk-limiting audits, cyber-damage recovery plans, a secure chain of custody; and the risk of returning ballots over the Internet.

Material below was used by the League of Women Voters of Colorado (LWVCO)'s election security group in evaluating LWV Oregon's request for concurrence with their election security and cybersecurity study, and in preparing a proposed LWVCO Election Security Position and consensus questions. A few notes and comments are included from the election security team.

The links in the table of contents below jump to sections in the text. In Google Doc, click in the popup. In Word, Ctrl+Click. In a pdf, click.

Additional Resources

**League of Women Voters of the United States**

> "Founded by the activists who secured voting rights for women, the League has always worked to promote the values and processes of representative government. Protecting and enhancing voting rights for all Americans; assuring opportunities for citizen participation; and working for open, accountable, representative, and responsive government at every level—all reflect the deeply held convictions of the League of Women Voters. "
> Impact on Issues 2020-2022 page 18

The League of Women Voters of the  United States, (LWVUS) already has a strong historical record with regard to  election security, emphasizing the need for voter-verifiable paper ballots providing an auditable paper record.

> "At the 2004 Convention, the League determined that to ensure integrity and voter confidence in elections, LWVUS supports the implementation of voting systems and procedures that are secure, accurate, recountable, and accessible. State and local Leagues may support a particular voting system appropriate to their area, but should evaluate them based on the "secure, accurate, recountable, and accessible" criteria. While LWVUS has not commented on specific voting systems, Leagues should continue to consult with LWVUS before taking a stand on a specific type of voting system to ensure that the League speaks consistently. Leagues should also consult standards developed by the Election Assistance Commission (EAC) pertaining to voting systems when studying or improving their own voting systems.
>
> "At Convention 2006, delegates further clarified this position with a resolution stating that the Citizens' Right to Vote be interpreted to affirm that LWVUS supports only voting systems that are designed so that:
>
> - They employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's Intent.
> - The voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent.
> - Such verification takes place while the voter is still in the process of voting.
> - The paper ballot/record is used for audits and recounts.
> - The vote totals can be verified by an independent hand count of the paper ballot/record.
> - Routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.
>
> "At Convention 2010, delegates added the principle of transparency, so that the League would support voting systems that are secure, accurate, recountable, accessible, and transparent.
> Impact on Issues 2020-2022 pages 27-28

But note, while LWVUS's *Impact on Issues* says paper ballots are needed so there *can* be audits, it says nothing about the importance of *performing* regular audits. Nor does it specify that audits should be robust, responsible, transparent, or risk-limiting. Nor does it address other election security issues such as chain of custody, returning ballots over the Internet, cyber-damage contingency plans, and voter registration databases.

**Why the League of Women Voters of Colorado Needs an Election Security Position**

Election security, an important topic for years, became a pressing issue after the 2020 election, and existing League positions are inadequate to advocate effectively.

League of Women Voters of the US (LWVUS) conventions addressed election security, but did not adopt a formal position. The 2021 Colorado legislative session included a bill, SB21-188, that would have allowed any disabled Colorado voter to return their ballot over the Internet. Supporters argued that those who physically could not vote a paper ballot on their own lost the privacy of their vote when having to ask others for help voting. The LWVCO Legislative Action Committee (LAC) agreed that voters with visual disabilities, and others who could not mark their ballots independently, should be allowed to return ballots electronically. But the LAC argued that returning a ballot over the Internet not only risked losing the privacy of one's vote, but could be vulnerable to hackers. The larger the group returning ballots over the Internet, the larger the target for hackers, and the more likely a hack could affect election outcomes. The LAC worked to convince legislators of the election security issue, who then narrowed the bill's scope before passage. However, neither the state nor national League have positions on the intersection between voters' ease of access and the security of the election as a whole. The LAC had a slim League position to stand on. Based on conversations with legislators, it seems likely the broader bill will come back as early as the 2022 session. It would be wise to have a sturdy position before the next round of discussions.

Legislation is not the only place where the League could wish for a position to advocate for secure elections. One of Colorado's own county clerks allowed an outsider to photograph election system passwords, and the photos were posted on social media. Again, neither LWVCO nor LWVUS have positions on controlling access to the actual election machines used in counts, and to their passwords.

To keep Colorado's election system secure, LWV Colorado needs a robust election security position from which to advocate.

**The Importance of Evidence-Based Elections**

Key work by Philip Stark and D.A. Wagner asserts that elections should be structured to provide convincing evidence that the reported outcomes actually reflect how people voted.

https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf

While no system is completely tamper proof or fail-proof, reducing and mitigating vulnerabilities, and focusing on the ability to recover no matter what goes wrong, lends confidence in the voting public that every voter was able to cast a ballot effectively, and the election outcome was reliable.
https://verifiedvoting.org/electionsecurity/

**Software Independence through Voter-Verifiable Paper Ballots**

> "Election security experts agree that the most resilient voting systems use paper ballots (marked by hand or with an assistive device for those who need to use them) that are verified by the voter before casting" https://verifiedvoting.org/votingequipment/
>
> "Without a paper audit trail, it can be difficult to detect errors or breaches in the voting machine's software or hardware, possibly allowing an incursion into American voting systems to go unnoticed. Even if an error is found, performing an audit of a paperless system can be difficult or impossible given a lack of redundant records to verify vote totals."
> https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/

The underlying principle is that of "software independence." That means that if an undetected change or error in the software causes a change or error in the election outcome, that change or error can be detected without relying on the existing software, ensuring that accurate votes are possible. At the present time that means using paper ballots and risk-limiting audits.

http://people.csail.mit.edu/rivest/pubs/RW06.pdf
https://people.csail.mit.edu/rivest/pubs/RV16.pdf

**Risk-Limiting Audits**

Risk-limiting audits are smart recounts of the voter-verifiable paper ballots. Rather than sampling a fixed share of ballots, election verification expert Jennifer Morrell says risk-limiting audits

> "take a statistically significant sample and ensure that if there were errors, there weren't enough that they would change the outcome."
> https://www.ncsl.org/research/elections-and-campaigns/the-what-why-and-how-of-election-audits-magazine2021.aspx

National Conference of State Legislatures also noted

> "If the margin of victory was narrow or if discrepancies are found, the audit escalates, and more paper ballots are reviewed until either the required level of confidence has been met or a full hand recount has been performed."
> https://www.ncsl.org/research/elections-and-campaigns/the-what-why-and-how-of-election-audits-magazine2021.aspx

A more precise definition is in the peer-reviewed literature.

https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
https://georgetownlawtechreview.org/wp-content/uploads/2020/07/4.2-p523-541-Appel-Stark.pdf

Colorado's risk-limiting audit process is described in these references:

https://www.eac.gov/colorados-implementation-of-risk-limiting-audits
http://bcn.boulder.co.us/~neal/elections/corla/

Audits must not compromise the chain of custody of the ballots or equipment, or harass voters

https://bipartisanpolicy.org/report/bipartisan-principles-for-election-audits/
https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2021/PR20210909Canvassing.html

Good background on resilience to disinformation, and cybersecurity for elections:

Zero Trust: How to Secure American Elections When the Losers Won't Accept They Lost
https://fsi.stanford.edu/publication/zero-trust

## Up-to-Date Hardware Tested and Secure

Aging equipment is an issue in many parts of the nation

https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today

Accreditation of voting system testing laboratories (VSTLs)

https://nvlpubs.nist.gov/nistpubs/hb/2021/NIST.HB.150-22-2021.pdf

The difficulty of integrating one brand of scanner with another brand's election management system can lock election officials into a single vendor and increase costs.

https://penntoday.upenn.edu/news/business-voting

If there were interoperability standards for how different components talk to each other, and different vendors' systems could talk to each other seamlessly, officials could mix and match, picking the best pieces from different vendors, encouraging competition, and innovation.

https://www.nist.gov/itl/voting/interoperability

### Ransomware

"Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. "

> "In some instances, ransomware may also steal an organization's information and demand an additional payment in return for not disclosing the information to others" "organizations can follow recommended steps to prepare for and reduce the potential for successful ransomware attacks. This includes identifying and protecting critical data, systems, and devices; detecting ransomware events as early as possible."
> Sept 2021 draft: https://csrc.nist.gov/publications/detail/nistir/8374/draft

Preventative steps that organizations can take to reduce the likelihood of a ransomware threat are outlined in NIST 8374 (link above) as well as in documents from the FBI and Department of Homeland Security

> https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
> https://www.cisa.gov/stopransomware

### Voter Registration Databases

Voter registration databases should be accurate, audited, have highly effective eligibility verification, and have transparency so that individuals can verify their own records. Purging of voter registration data needs to take place in a manner that is nondiscriminatory and does not disenfranchise eligible voters.

On the importance of voter registration databases that are accurate, audited, have effective eligibility verification and have transparency so individuals can verify their own records

> "Their dynamic functionality and capacity to hold data from entire jurisdictions give electronic poll books some advantages over traditional paper poll books."
> "Electronic poll books are not without their drawbacks: unlike paper poll books, they are vulnerable to cyberattacks and programming errors. Jurisdictions must take safeguards against hacking, the installation of malware, and unauthorized access. Many electronic poll books require some kind of network or internet connection to function and are therefore vulnerable not only to power outages, but also to network failure and remote hacking."
> "Election officials must have election security practices embedded, including a robust backup plan to speedily check in voters if the technology fails."
> https://verifiedvoting.org/wp-content/uploads/2020/08/Verified-Voting-Electronic-Poll-Book-Use-in-the-United-States-20200831.pdf

On the privacy threats of electronic poll books

> https://www.nist.gov/publications/privacy-threats-electronic-poll-books

### Cyber-Damage Contingency Plans

> "While there are many options to improve overall election security through the use of paper-based voting equipment, risk-limiting audits, and other crucial steps, they might not happen

> before November [2018]. Efforts to prevent attacks in the first place are, of course, critical. But in the months remaining before the election, it is at least equally important to ensure adequate preparations are in place to quickly and effectively recover if prevention efforts are unsuccessful."
> https://www.brennancenter.org/our-work/policy-solutions/better-safe-sorry-how-election-officials-can-plan-ahead-protect-vote-face

The Brennen Institute has devised a checklist detailing five critical areas election officials must address in preparation for possible equipment failure or foreign interference on Election Day.

1. Prevent and Recover from Electronic Pollbook Failures and Outages
2. Be Prepared for Voting Equipment Failures
3. Prevent and Recover from Voter Registration System Failures/Outages
4. Prevent and Recover from Election Night Reporting System Failures/Outages
5. Develop a Communication Strategy

For more detail see checklist

> https://www.brennancenter.org/sites/default/files/publications/2018_08_13_ChecklistV4.pdf

**Voting Online Creates More Difficulties than Financial Transactions Do**

An MIT paper notes that:

> "Online voting systems are vulnerable to serious failures: attacks that are larger scale, harder to detect, and easier to execute than analogous attacks against paper-ballot-based voting systems. Furthermore, online voting systems will suffer from such vulnerabilities for the foreseeable future given the state of computer security and the high stakes in political elections."
> Journal of Cybersecurity by authors from the Digital Currency Initiative of the Massachusetts Institute of Technology (MIT) Media Lab, MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), and MIT Internet Policy Research Institute (IPRI).
> https://people.csail.mit.edu/rivest/pubs/PSNR21.pdf

This article also gives a clear explanation of how voting differs from other transactions now carried out on the internet, such as online shopping, banking and cyber-currency transactions.

> "Security considerations for online shopping and online banking are different than those for election systems, in two key ways. First, online shopping and banking systems have higher tolerance for failure—and they do fail. Credit card fraud happens, identity theft happens [27], and sensitive personal data are massively breached (e.g., the 2017 Equifax breach [28]). Online shopping and banking are designed to tolerate failure: merchants, banks, and insurers absorb the risk because doing so is in their economic interest. Governments may also provide legal recourse for victims (as for the Equifax settlement [29]). But for elections, there can be no insurance or recourse against a failure of democracy: there is no means to "make voters whole again" after a compromised election."
> Journal of Cybersecurity, 2021, 1–15 doi: 10.1093/cybsec/tyaa025 Research Paper

https://people.csail.mit.edu/rivest/pubs/PSNR21.pdf

Furthermore, confidence in our democratic system is at stake

> “Elections are high value targets for sophisticated (nation-state) attackers, whose objective is not fraudulent financial transactions but changing or undermining confidence in election outcomes.” “While the voter of course knows the details of his votes, election officials must not. Officials know the names of those who voted, and the contents of the cast ballots, but they are never supposed to know exactly who cast which ballot. This is a requirement for information suppression, a partial blindness on the part of one side in the transaction that has no analog in the e-commerce world.” “The flip side of privacy is openness or transparency. Once again, the requirements are completely different for e-commerce and for online voting. In the e-commerce world a person buying something online is entitled to know everything about his particular transaction, but nothing about other people’s transactions. A buyer is not entitled to know how many other transactions there are, what the merchant’s revenues or profits are, who else the merchant sells to, or what price others pay for the same goods or services, and he has no right to audit the books of the merchant he is dealing with. In the voting world, however, most of this is reversed. Complete election information is (or should be) open to all. Election officials report not just the names of the winners, but also exactly how many votes were cast and how many each candidate received down to the precinct level.” https://verifiedvoting.org/publication/if-i-can-shop-and-bank-online-why-cant-i-vote-online/

**Balancing Election Security with the Right to Vote**

Most voters can be conveniently accommodated via a variety of methods that result in auditable voter-verified paper ballots, including in-person voting and ballots mailed to voters with the option of returning them in person, via drop boxes, or via the mail. The MOVE act requires that Uniformed and Overseas Citizens Absentee Voters (UOCAVA) be mailed absentee ballots no later than 45 days before a federal election.

https://ballotpedia.org/Military_and_Overseas_Voter_Empowerment_(MOVE)_Act

Federal guidelines for UOCAVA also include electronic transmission of *blank* ballots *to* such voters:

https://www.justice.gov/crt/uniformed-and-overseas-citizens-absentee-voting-act

But a small subset of voters are still not able to vote privately and independently via these options. Options to *return* their ballots electronically (“Internet voting”) are often introduced.

https://www.eac.gov/sites/default/files/document_library/files/Electronic-Ballot-Return-for-UOCAVA-Voters-FINAL.pdf

These usually involve having the voter sign a form acknowledging that they understand that by submitting their ballot electronically, their right to a secret ballot is waived.

But as recently as May of 2020,

> "Several U.S. government agencies [CISA, EAC, FBI, and NIST] told states ... that casting ballots over the internet poses high levels of cybersecurity risk and is vulnerable to disruption, a warning that came as some states consider expanding online voting options to cope with challenges created by the coronavirus pandemic."

Their advice is that, if an Internet return option is mandated

> "its use should be limited to voters who have no other means to return their ballot and have it counted."

I.e. Internet return should only be used when voters would otherwise be disenfranchised.

> https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf
> https://www.wsj.com/articles/agencies-warn-states-that-internet-voting-poses-widespread-security-risks-11588975848
> https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf

In addition, the Center for Scientific Evidence in Public Issues of the American Association for the Advancement of Science wrote a letter to all Governors and Secretaries of State in April of 2020 stating that:

> "At this time, internet voting is not a secure solution for voting in the United States, nor will it be in the foreseeable future. "

This letter was signed by more than 80 leading organizations, scientists, and security experts.

> https://www.aaas.org/programs/epi-center/internet-voting-letter

For Colorado in particular, the American Association for the Advancement of Science's (AAAS) Center for Scientific Evidence in Public Issues and the U.S. Technology Policy Committee of the Association for Computing Machinery (USTPC) wrote regarding Colorado's consideration of an expansion of insecure internet voting. They addressed issues in the introduced version of SB21-188 from the 2021 legislative session at the request of LWVCO Legislative Action Committee member, Gaythia Weis. This restates the information in the more general signed letter cited above.

> https://www.aaas.org/sites/default/files/2021-04/Colorado_State_Legislator_4_19_2021_.pdf

"Any implementation of electronic ballot return should adopt the best security practices possible and limit access only to those who absolutely require the option...."

The four points that the AAAS/ACM letter makes leading up to that conclusion are:

- “All commercially available internet voting systems and technologies are currently inherently insecure.
- “No technical evidence exists that any internet voting technology is safe or can be made so in the foreseeable future; rather, all research performed to date demonstrates the opposite.
- “No blockchain technology can mitigate the profound dangers inherent in internet voting.
- “No mobile voting app is sufficiently secure to permit its use.”
  https://www.aaas.org/sites/default/files/2021-04/Colorado_State_Legislator_4_19_2021_.pdf

Other sources agree:

> “When a voter cannot otherwise access the polls, election authorities may provide a remote voting solution, e.g., mail-in ballots for over-seas military and other absentee voters. However, the risks discussed in this section strongly favor in such cases (i) limiting remote voting to the settings where there is no feasible alternative and (ii) using mail-in ballots rather than online voting.”
> Journal of Cybersecurity, 2021, 1–15 doi: 10.1093/cybsec/tyaa025 Research Paper
> https://people.csail.mit.edu/rivest/pubs/PSNR21.pdf
>
> “The most secure option for remote voting is to mail pre-printed paper ballots to voters as is traditionally done for mail-in ballots. This allows most ballots to be hand-marked and to be mailed back or dropped off in a condition suitable for immediate scanning, eliminating the need to re-make the ballot. Jurisdictions should make every effort to ramp up their capability to bulk mail paper ballots to all voters, or to as many as allowed by law.”
> Center for Scientific Evidence in Public Issues Leveraging Electronic Balloting Options Safely and Securely During the COVID-19 Pandemic
> https://freespeechforpeople.org/wp-content/uploads/2020/06/rabm.white_.paper_.6.23.20.pdf

Some states use electronic ballot return systems from Voatz and Democracy Live which, besides being unauditable, uncertified proprietary *black boxes*, were shown to be dangerously insecure in reports from both independent researchers and the company’s own external reviews.

> http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213
> https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/
> https://www.usenix.org/conference/usenixsecurity21/presentation/specter-security

Several decades of research has made some progress on achieving software independence without relying on voter-verifiable paper ballots. The first step is worth deploying in conjunction with voter-verifiable paper ballots for in-person voting. While applications to Internet voting exist, they retain serious problems and are not ready for use by more than a small fraction of voters.
“End-to-end verifiable” (E2E-V) systems use cryptographic techniques to achieve software independence. They actually give voters the evidence they need to audit their own vote themselves: to verify that their own vote was counted as cast, and amazingly enough, to do so without being able to prove how they voted to anyone else. ThisVersion 2.0 of the Voluntary Voting System Guidelines allow

for a path to certification of *in-person* voting systems with these properties, providing the potential for a major advance in security. E2E-V systems have security advantages, but cannot be used by voters to return their ballots over the Internet

> https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

There is also ongoing work on how to let *remote* voting systems take advantage of this end-to-end verifiability for voters, resulting in end-to-end verifiable Internet voting (E2E-VIV). But even if E2E-VIV systems were highly accessible and commercially available, they are not suitable for use by large numbers of voters. Internet voting faces enormous challenges of how to securely and privately determine voter eligibility, and protect against denial-of-service, malware attacks on the voter's devices, and address privacy risks, which is why even E2E forms of internet voting should restrict use to only those who would otherwise be disenfranchised, unable to vote privately, or to vote at all. For the few voters unable to vote using voter-verifiable paper ballots, who instead return their ballot over the Internet, we need carefully and independently tested E2E-VIV voting systems which are considerably more secure and auditable than current methods.

> https://www.usvotefoundation.org/E2E-VIV

Voter access to ballots is a fundamental value. There are serious cybersecurity issues with online voting. Voters need to know that this method is neither as private nor as secure as other methods, including mail in ballots. Online voters could be malware targets, and special efforts are needed to guard against this. The general public needs to be aware that hacking is more likely when more people vote online, possibly to the extent of changing election results.

**Comparison to Mail in Ballots**

Again from the MIT paper

> "When a voter cannot otherwise access the polls, election authorities may provide a remote voting solution, e.g., mail-in ballots for over-seas military and other absentee voters. However, the risks discussed in this section strongly favor in such cases (i) limiting remote voting to the settings where there is no feasible alternative and (ii) using mail-in ballots rather than online voting. While mail-in ballots enable vote selling and coercion, they are still far less susceptible to large-scale covert attacks than online voting. Destroying a mail-in ballot generally requires physical access, and large-scale efforts must target ballots across post offices that are geographically and operationally diverse—a very different task from exploiting a single vulnerability that could stealthily affect millions of devices with practically the same effort as one device. As a result, attacks against mail-in ballots are less likely to be scalable or to go undetected than attacks against purely electronic systems."
> Journal of Cybersecurity, 2021, 1–15 doi: 10.1093/cybsec/tyaa025 Research Paper
> https://people.csail.mit.edu/rivest/pubs/PSNR21.pdf

## Difficulties in Detecting Security Breaches

This statement may be true but does not offer much reassurance:

> "Caleb Thornton, a legal, policy and rulemaking manager in the Department of State's Elections Division, added 'we have seen no evidence that any ballot has ever been manipulated, intercepted or cast fraudulently via this method of voting.' "
> https://www.coloradopolitics.com/elections/lawmakers-advance-online-voting-for-the-blind-over-objections-from-election-security-experts-homeland-security/article_39f56a44-a90e-11eb-8b36-ab16ad229f7d.html

This is not something that they can know for sure. Reports come in regularly of cybersecurity breaches that are only discovered months or years after they happened, and many more could be lying in wait for an appropriate exploit moment.

It is very hard to verify when one has been the victim of a cyber attack. Secretaries of State and county election officials generally have no reliable mechanism for evaluating what happens to the contents of an electronically submitted ballot between the time it leaves the voter and arrives at the election office. Additionally, hacks can take time to discover, even when carried out against very technologically expert targets such as Microsoft, cyber security firm FireEye and the US Departments of Homeland Security and Treasury.
https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

## Election Transparency

The public should be welcome to observe all aspects of the election process and to access copies of election equipment source code, samples of election equipment, copies and/or images of ballots (with personally identifying information removed), and copies of procedures. However, passwords and other authentication secrets must be kept secure, and secure custody of ballots, the actual equipment used, and the software on it must remain in control of election officials.  The public should not be allowed to interfere in the election process.

## Chain of Custody

The Election Assistance Commission homepage features a link to a detailed page on Chain of Custody Best Practices

> "The chain of custody of ballots, voting equipment, and associated data is essential to ensure the election system remains trustworthy. Documentation of the chain of custody also provides evidence that all voting procedures were followed. It is a best practice for chain of custody

procedures to be clearly defined in advance of every election, well documented and followed consistently throughout the entire election lifecycle or process."
https://www.eac.gov/election-officials/chain-custody-best-practices

There is growing interest in using scanned ballot images, made and digitally-signed, timestamped and committed to as early as as possible in the processing of the paper ballots, to help secure their chain-of-custody. Since the images are computer-generated, they are not voter-verified and are subject to cyberattacks. In "UnclearBallot, Automated Ballot Image Manipulation," Bernhard et al. demonstrated that ballot images can be changed, moving voters' marks so they appear to be for a different candidate. Thus it is still necessary to use the original voter-verified paper ballot for a risk-limiting audit.

https://mbernhard.com/papers/unclearballot.pdf

But if the ballot images are examined at the same time as the paper ballots in a risk-limiting audit, they would provide added assurance that the chain-of-custody of the paper ballots was not compromised between when ballot images were secured and the audit conducted. Early work in this direction was done in the Humboldt County Elections Transparency Project in 2008.

https://electionstransparencyproject.com/
https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/rescorla-ballot.pdf

## Conclusion

The League of Women Voters was founded on the premise that the right to vote is a fundamental principle of our democracy, and LWV is committed to expanding voter access.   This must be done with election security in mind, to minimize risk that the overall election outcome is undermined. LWV Colorado needs a robust position on election security.  The LWVUS *Impact on Issues* also needs sufficient detail to give local leagues solid positions for advocacy.

Both national and state League positions need to address the risk of returning ballots over the internet and the need for software independence of voting systems,risk -limiting audits, cyber-damage recovery plans, and a secure chain of custody.

## Additional Resources

### Some Authors Cited

Fernandez  https://www.aaas.org/person/michael-d-fernandez
Greenhalgh  https://freespeechforpeople.org/about/
Masterson https://electionsgroup.com/leadership-team.html
https://fsi.stanford.edu/people/matt-masterson

Morell https://electionsgroup.com/leadership-team.html.
Newell https://www.aaas.org/person/steve-newell
Norden https://www.brennancenter.org/experts/lawrence-norden
Rivest http://people.csail.mit.edu/rivest/
Stark https://www.stat.berkeley.edu/~stark/
Simons, Jefferson, McBurnett https://verifiedvoting.org/team/

### Additional Information

https://www.fvap.gov/uploads/FVAP/CRA-Report_B.2.1.LitReview_20130228.pdf 2013

https://csrc.nist.gov/CSRC/media/Presentations/election-equipment-security-requirements-brief/images-media/1-6Howell%20-%20Election%20Equipment%20Security%20Requirements%20Breif.pdf 2019 (presentation)

https://www.nist.gov/speech-testimony/election-security-voting-technology-vulnerabilities June 2019 (Testimony)

https://www.nased.org/

Security considerations for remote UOCAVA voting
https://www.nist.gov/system/files/documents/itl/vote/NISTIR-7700-feb2011.pdf

UOCAVA threat analysis https://www.nist.gov/system/files/documents/itl/vote/uocava-threatanalysis-final.pdf
https://verifiedvoting.org/publication/if-i-can-shop-and-bank-online-why-cant-i-vote-online/

NIST & Verified Voting: Principles for Remote Ballot Marking Systems https://civicdesign.org/wp-content/uploads/2015/09/Principles-for-remote-ballot-marking-systems-16-0210.pdf

Voter verified paper ballots, Harvard
https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf