SB 727 - FAV - MML.pdf
Uploaded by: Angelica Bailey Thupari
Position: FAV

TESTIMONY

COMMITTEE:	Senate Education, Energy, and the Environment	**DATE:**	February 24, 2026
POSITION:	Favorable	**BILL:**	SB 727

The Maryland Municipal League supports SB 727, which authorizes municipalities to use qualified electronic transmission systems for municipal elections subject to strict security and integrity standards. Municipal elections often operate independently from State and federal cycles and with limited resources. This legislation provides a carefully structured option for municipalities to modernize election administration in a way that can enhance voter access while maintaining public trust.

The bill establishes a high bar for security. Any electronic transmission system must incorporate end-to-end encryption, auditability, multifactor authentication, air-gapping of critical systems, biometric or equivalent identity verification, and a process for printing decrypted ballots to create a paper record. These safeguards ensure that electronic transmission is not synonymous with reduced oversight; instead, the bill requires layered protections and preserves a tangible paper trail for accountability and auditing. SB 727 also includes important privacy protections by prohibiting the use of voter information for purposes beyond election administration and voter participation statistics. This clear limitation reinforces public confidence in how sensitive data will be handled.

Importantly, the legislation is permissive, not mandatory. Municipalities retain the discretion to determine whether adopting such a system is appropriate for their community's needs and resources. By enhancing access, preserving strong security standards, protecting voter privacy, and respecting local control, SB 727 provides municipalities with a responsible and modern tool for conducting local elections.

For these reasons, the League respectfully requests a favorable report on Senate Bill 727.

For more information relating to this piece of testimony, please contact:
Angelica Bailey Thupari: Director, Advocacy and Public Policy, angelicab@mdmunicipal.org

Reverend Brenda Girton-Mitchell Testimony SB727_HB

Uploaded by: Brenda Girton-Mitchell

Position: FAV

Reverend Brenda Girton-Mitchell

Good afternoon, Chair and members of the Committee.

My name is Rev. Brenda Girton-Mitchell. I am a pastor at Metropolitan Baptist Church in Largo, MD. I believe that any tool that can increase voter participation is essential.

Municipal election turnout often lags as much as 30 points behind national elections.

Mobile voting addresses very real barriers: long lines, unreliable transportation, inaccessible polling places, demanding work schedules, and challenges faced by elders and people with disabilities.

Providing municipalities the option to offer secure mobile voting is a step toward removing unnecessary obstacles and strengthening participation at the local level which is necessary for the health of our democracy.

Thank you.

Forrest_Senti_Testimony_SB727.docx.pdf
Uploaded by: Forrest Senti
Position: FAV

Forrest Senti — Testimony in Support of SB727
Senate Education, Energy, and the Environment Committee
February 25, 1:00 p.m.

Chair and members of the Committee,

My name is Forrest Senti. I've spent my career building secure systems for the United States and working in cybersecurity in both the public and private sector. At the National Cybersecurity Center, I led the first independent security audits of mobile voting technology and have worked in several states on their first uses of this technology. I'm here as a cybersecurity consultant to address the security of what this bill contemplates.

You will likely hear that internet voting is insecure. For email. fax, and unsecured web portal ballot return, that is correct—I would oppose their use. But this bill requires something fundamentally different: end-to-end verifiable cryptography, the same mathematics protecting banking, military communications, and classified systems.

Here is the critical distinction. Traditional electronic systems ask you to *trust* that nothing went wrong. This system asks you to *verify*. Every ballot is encrypted on the voter's device and mathematically provable from submission to final count. If anything is tampered with—by malware, an insider, anyone—the math breaks and the discrepancy is detected. It fails loudly, not silently.

You may hear three specific objections. First, that malware could compromise a voter's phone—but verification happens on a *separate* device, requiring an attacker to compromise both independently. Second, that most voters won't check their ballots—but even a small percentage checking creates a statistical tripwire that makes large-scale undetected fraud mathematically improbable. Third, that there's no dispute resolution—but this bill requires paper records. Decrypted ballots are printed and enter the same audit and recount processes as every other paper ballot.

A lot has changed since 2020 when the federal Cybersecurity and Infrastructure Security Agency and the FBI warned that electronic ballot return is high-risk. That assessment evaluated email, fax, and basic web portals. The next generation mobile voting model is significantly more secure —encrypted, independently verifiable, and auditable. We are excited for an updated federal evaluation.

Mobile voting technology now exists to meet the standards of The National Academy of Sciences for robust security and verifiability. Today, malware and discrepancies are detectable through independent "Ballot Check" protocols and a public verification board.

This new technology meets the highest standard and I welcome skepticism, that's how good security works. I'm happy to answer your questions.

Support for SB0727; Municipal Elections - Qualifie

Uploaded by: George Sewell

Position: FAV

Gayon M. Sampson
Chief of Staff

Allen W. Etzler, III
Deputy Chief of Staff

FREDERICK
OFFICE OF THE MAYOR

Michael C. O'Connor
Mayor

The Honorable Brian Feldman
Maryland State Senate
2 West Miller Senate Office Building
11 Bladen Street
Annapolis, MD 2140

Re: **SB0727: Municipal Elections - Qualified Electronic Transmission Systems - Authorization for Use**

Chair Feldman, Vice Chair Kagan, and members of the Committee,

The City of Frederick supports SB727 and its efforts to allow municipal elections to be conducted through the use of a qualified electronic transmission system.

This bill allows municipalities, such as Frederick, to modernize and expand their voting system by legally allowing them to adopt a secure electronic ballot transmission system for municipal races, if they can procure or build systems that meet these standards. HB1066 enables voters facing mobility challenges, disabilities, transportation barriers, or irregular work schedules to participate remotely using a secure platform.

SB727 ensures that security and data privacy are at the forefront with the integration of these systems, mandating security auditability, end-to-end encryption, biometric or equivalent digital identity verification technologies, and production of a paper voting record. These requirements are aimed at ensuring that remote marking and transmission of ballots maintains ballot secrecy, integrity, and verifiability.

Included in SB727 is a narrow data usage clause, only allowing for participant data to be used for election administration such as ballot processing and for voter participation statistics. It prohibits repurposing that data for campaigning, commercial use, or other non-election functions, which is a significant privacy concern given the sensitivity of biometric and identity data.

Overall, SB727 equips Maryland municipalities with the tools to modernize elections for upcoming cycles, supporting local democracy in a digital age.

Sincerely,

Michael O'Connor

Samuel SB0727 Qualified Electronic Transmission Sy

Uploaded by: Janice Samuel

Position: FAV

From: Janice Samuel
12700 Woodbridge Court, Bowie MD, 20721
jlwsamuel@gmail.com

To: Senate Government, Labor, and Election Committee

SB0727 is a good bill. It permits the use of an electronic transmission system to cast a ballot only in a municipal election. Municipal elections are important because they have the most impact in day-to-day life for the voters.

I am legally blind and would not be able to see the print on a paper ballot. For me, being able to utilize an electronic transmission system enables me to vote privately, independently, and with secrecy. The seven examples listed in the bill for security and verification give a voter who uses it assurance while casting their ballot.

Please vote yes for SB0727 because it will allow for greater voter participation in the democratic process.

Letter of Support

Uploaded by: Julius Whaley
Position: FAV

Julius Whaley, Letter of Support for SB 727
Senate Education, Energy and the Environment Committee Hearing on SB727-
February 25th, 2026 at 1:00 p.m.

Chair and Members of the Committee, thank you for the opportunity to testify.

My name is Julius Whaley, and I live in Hyattsville, Maryland. I've lived here my whole life. Growing up, I always went with my mom to vote at my elementary school. I remember seeing many elderly and disabled neighbors coming in to vote—sometimes without caregivers to assist them. It may seem small, but for people with limited mobility, getting to a polling place can be a significant physical and logistical burden.

Mail-in voting expanded access during COVID, but it also raised concerns. We've seen ballots misplaced, drop boxes vandalized, and even set on fire. Those incidents, while not widespread, affect public confidence and should be taken seriously when we talk about voter access and security.

We live in a digital world. Technology expands access in education, healthcare, and work. I believe we can apply that same innovation to voting—especially to help elderly residents, people with disabilities, and those who cannot easily get to a polling location.

Through my involvement with Civics Unplugged, serving as Student Body President at my high school, and participating in youth-led civic initiatives across Maryland, I've seen firsthand how important participation is. Democracy works best when everyone—not just those who find it easiest to vote—can have a voice.

Senate Bill 727 would allow cities to explore mobile voting as an additional option. It does not replace existing methods, but it gives communities flexibility to expand access responsibly.

I respectfully urge you to support SB 727.

Thank you for your time.

MIchelle Feldman Testimony MD SB727.pdf
Uploaded by: Michelle Feldman
Position: FAV

MIchelle Feldman Testimony in Support of SB 727
Senate Education, Energy, and the Environment Committee
February 25, 1:00 p.m.

Chair and members of the committee,

My name is Michelle Feldman, and I am the Campaigns Director at the Mobile Voting Project, a nonprofit dedicated to expanding voting access through secure smartphone voting.

Today, we face new and evolving barriers to voting, but through great leaps innovation, we can responsibly address these roadblocks.

Mobile voting is not theoretical. Nationally, 32 states allow for specific groups of voters to return their ballots electronically. Mobile voting has been piloted in 11 states—red and blue—including Colorado, West Virginia, Virginia, Oregon, Washington, Utah, South Carolina, Montana, Alabama, and North Carolina. Most recently, Anchorage and Juneau, Alaska used mobile voting for its municipal elections.

The results are significant: turnout doubled among military and overseas voters in Denver, tripled in a special district in Seattle, and in South Carolina ballot returns increased from 9.8% to 55%. In addition, the streamlined process saved dozens of hours of manual work for election staff.

Mobile voting also strengthens transparency and verification. Here is how it works:

First, a voter downloads the secure application through their board of elections website.

Second, they verify their identity through multi-factor authentication.

Third, they mark their ballot on their device. When they submit, three things happen at once: the ballot is encrypted, anonymized, and the voter receives a tracking code.

Next, the digital ballot goes to election officials who immediately take the ballot offline, decrypt it, print it onto paper, and mix it with all other paper ballots for tabulation.

Finally, Using their tracking code, the voter can verify that their ballot was cast, recorded, and counted correctly.

This bill ensures that, if used, mobile voting meets the highest standards of security, transparency, and efficiency while expanding access for Maryland voters.

Thank you for your consideration.

Moms First Support MD SB727 .docx.pdf
Uploaded by: Michelle Feldman
Position: FAV

Moms First - Support SB272
Senate Education, Energy and the Environment Committee

Dear Chair and Members of the Committee,

On behalf of Moms First, a national nonprofit organization dedicated to building a country that truly values mothers through policies like paid leave and affordable, accessible childcare, we write to express our support for efforts to explore mobile voting as an additional, secure method of voting in Maryland city elections.

Every day, moms across Maryland balance work, caregiving, transportation, and household responsibilities. These realities often create significant time and logistical barriers to participating in elections. Arranging childcare, taking time away from work, or coordinating transportation to a polling place can make civic engagement far more complicated than it should be.

While vote-by-mail has expanded access, it does not eliminate all barriers. In areas with delayed or limited mail service, or for parents navigating unpredictable schedules, returning a ballot can still present challenges.

We believe cities should have the option to responsibly pilot secure, well-safeguarded mobile voting systems that meet rigorous security standards and maintain public trust. Expanding access – without replacing existing methods – can help ensure that eligible voters, including busy parents, are better able to participate in local democracy.

When caregivers can fully participate in civic life, communities benefit. Policies are stronger and more responsive when they reflect the lived experiences of families raising the next generation.

We respectfully urge you to consider policies that thoughtfully modernize local elections in ways that maintain security, transparency, and accessibility for today's families.

Thank you for your leadership and your commitment to an inclusive and secure democracy.

Sincerely,

Reshma
Moms First

SB 727 _ HB 1066 RCVMD Testimony - Mobile Voting.p
Uploaded by: Michelle Whittaker
Position: FAV

February 23, 2026

Education, Energy, and the Environment Committee
Maryland Senate
2 West Miller Senate Office Building
Annapolis, Maryland 21401

Re: Senate Bill 727 (House Bill 1066)
Municipal Elections - Qualified Electronic Transmission Systems - Authorization for Use

Position: FAVORABLE

Dear Education, Energy, and the Environment Committee Members:

Ranked Choice Voting Maryland (RCV Maryland) is dedicated to promoting transparent, secure, and accurate elections at all levels. Senate Bill 727, Municipal Elections - Qualified Electronic Transmission Systems - Authorization for Use (cross-filed as House Bill 1066), addresses a common challenge for municipalities: low voter participation and access.

This legislation would provide Maryland municipalities with a secure and innovative tool to enhance voter participation. Furthermore, it would provide the entire state with valuable information and best practices.

Many municipalities experience diminished voter turnout in municipal elections, even though the same constituents participate in county and state elections. Multiple factors contribute to low turnout, including accessibility, awareness, competitiveness, and timing. HB 1066 could potentially mitigate low participation by authorizing secure mobile voting in municipal elections.

The American Bar Association (ABA) notes that mobile voting has been successfully piloted across the United States, citing a tripling of turnout in King County, Washington, as one example[1]. The ABA recommends piloting mobile voting systems with smaller groups of voters while rigorously maintaining strong security and voter integrity protocols.

In conjunction with ranked choice voting, which the ABA found to increase turnout and decrease negative campaigning[2], Maryland municipalities have an opportunity to lead the way in strengthening democracy by making it more accessible and representative for a broader electorate.

We strongly urge a favorable report for SB 727 and encourage municipalities to explore innovative tools to enhance participation and representation.

Sincerely,

Michelle C. Whittaker
Executive Director

Ranked Choice Voting Maryland
8484 Georgia Avenue, Ste 240
Silver Spring, MD 20910

[1] Addressing Negative Partisanship with Mobile Voting
https://www.americanbar.org/groups/public_interest/election_law/american-democracy/our-work/addressing-negative-partisanship-mobile-voting/
[2] What We Know About Ranked Choice Voting, Updated for 2025
https://www.americanbar.org/groups/public_interest/election_law/american-democracy/our-work/what-we-know-about-ranked-choice-voting-2025

Testimony in support of SB0727 - Municipal Electio

Uploaded by: Richard KAP Kaplowitz

Position: FAV

SB0727_RichardKaplowitz_FAV
02/25/2026
Richard Keith Kaplowitz
Frederick, MD 21703

TESTIMONY ON SB#0727- POSITION: FAVORABLE

Municipal Elections - Qualified Electronic Transmission Systems - Authorization for Use

TO: Chair Feldman, Vice Chair Kagan, and members of the Education, Energy and the Environment Committee
FROM: Richard Keith Kaplowitz

My name is Richard Keith Kaplowitz. I am a resident of District 3, Frederick County. I am submitting this testimony in support of SB#0727, **Municipal Elections - Qualified Electronic Transmission Systems - Authorization for Use**

This bill will have two purposes. First, it will define and permit a "qualified electronic transmission system", an electronic transmission system through which a qualified voter may receive, mark, and return a ballot and that maintains reasonable data security and voter integrity protections. Second, a municipality may not use information received from a voter using a qualified electronic transmission system in a municipal election for any purpose other than election administration and voter participation statistics.

This bill will authorize a municipality to conduct a municipal election through the use of a qualified electronic transmission system; and prohibiting a municipality from using information received from a voter using a qualified electronic transmission system for certain purposes.

This bill will expand the availability of safe election processes. As a partially disabled person living in a senior community this could expand ways that my community can vote without the need to leave home to do so. Other groups with access problems to voting sites will also benefit if this methodology is made available.

I respectfully urge this committee to return a favorable report on SB#0727.

Favorable SB0727 Mobile voting.pdf
Uploaded by: Ronza Othman
Position: FAV

NATIONAL FEDERATION OF THE BLIND
MARYLAND

Live the life you want.

From: Ronza Othman, President
National Federation of the Blind of Maryland
15 Charles Plaza, #3002
Baltimore, MD 21201 president@nfbmd.org

To: Senate Energy, Education, and the Environment Committee

The members of the National Federation of the Blind of Maryland urge the Senate Energy, Education, and the Environment Committee to give a favorable report to SB0727 –Municipal Elections – Qualified Electronic Transmission Systems – Authorization for Use.

The National Federation of the Blind of Maryland is the State's oldest and largest civil rights organization of and for blind, low vision, and deaf-blind Marylanders. We represent voters across the State who are committed to full participation in every aspect of civic life — including the fundamental right to vote.

This bill authorizes municipalities to conduct municipal elections using a "qualified electronic transmission system." The bill defines such a system as one that allows an eligible voter to receive, mark, and return a ballot electronically while incorporating robust security protections, including:

- Security auditability
- End-to-end encryption
- End-to-end verifiability
- Multifactor authentication
- Air-gapping
- A process for printing decrypted ballots to create a paper record
- Biometric or equivalent digital identity verification.

The bill further prohibits municipalities from using information received through the system for any purpose other than election administration and voter participation statistics.

In short, This bill permits municipalities — but does not require them — to adopt a secure electronic transmission option with clear statutory guardrails.

Voting is a fundamental right. Equal access to voting methods is essential to maintaining a fair and inclusive democracy. Yet many blind and print-disabled voters continue to face structural barriers to fully private and independent participation.

According to the U.S. Election Assistance Commission, 20% of voters with disabilities report difficulty voting due to accessibility barriers, compared to just 6% of voters without disabilities. In Maryland, more than 235,000 voters — approximately 3.8% of the population — have a disability that may affect their ability to complete or return a paper ballot independently.

While in-person voting often includes accessible ballot marking devices, municipal elections frequently operate differently from State-run elections. Some municipalities rely heavily on paper-based processes or absentee-style voting systems that may not offer the same accessibility infrastructure as statewide elections.

For blind voters, electronic ballot delivery alone is not enough. If a voter can receive and mark a ballot electronically but must then print, sign, and return it physically, independence is lost. Many blind voters do not have printers. Many cannot independently verify a signature line. Many must rely on family members, neighbors, or friends — sacrificing ballot secrecy and privacy in the process.

No other demographic group is asked to surrender privacy and independence in order to vote. Voters with disabilities should not be treated differently.

This bill creates a lawful pathway for municipalities to implement secure systems that allow voters to receive, mark, and return ballots electronically — while maintaining paper records and strong auditability safeguards.

The National Federation of the Blind of Maryland takes election security seriously. Accessibility and security are not opposing values; they must coexist. This bill explicitly requires:

- End-to-end encryption
- End-to-end verifiability

- Multifactor authentication
- Air-gapped systems
- A paper record created by printing decrypted ballots. These protections reflect modern best practices in secure electronic systems and address common concerns about integrity and auditability. Moreover, by requiring a printed paper record, the bill ensures that ballots can be audited and recounted just like traditional paper ballots. The prohibition on secondary use of voter information further protects voter privacy.

This bill is not a mandate for universal internet voting. It is an authorization for municipalities to adopt a qualified, secure, statutorily defined system if they choose — with explicit security parameters written into law.

The Mobile Voting Project and other accessibility-focused initiatives across the country have demonstrated that secure electronic ballot return systems can be designed with layered protections, identity verification safeguards, and audit mechanisms. Several states already permit electronic ballot return for certain voter populations, including military and overseas voters. A growing number have extended such systems to voters with disabilities. Municipal elections, which are often smaller in scale, can serve as responsible pilot environments for carefully designed, secure systems. This bill provides the statutory framework necessary to allow municipalities to innovate responsibly while maintaining voter protections.

For blind and print-disabled voters, the question is not one of convenience — it is one of equality. If a municipality adopts a voting method that is technologically capable of being made accessible but fails to do so, voters with disabilities are effectively excluded or forced to rely on assistance.

We would not tolerate a polling place without a ramp. We should not tolerate voting systems that deny private and independent access when secure technological solutions exist. This Bill gives municipalities the legal authority to remove those barriers.

This legislation reflects a balanced approach — one that embraces innovation without sacrificing security.

For these reasons, on behalf of the National Federation of the Blind of Maryland, I respectfully ask for a favorable report on SB0727. For questions, please contact me at President@nfbmd.org or at 443-426-4110.

National Federation of the Blind of Maryland
Ronza Othman, *President NFBMD* | 15 Charles Plaza, #3002, Baltimore, MD 21201 **|** 443-426-4110**|** www.nfbmd.org

Sam Kinch Testimony SB727.pdf
Uploaded by: Sam Kinch
Position: FAV

Sam Kinch Draft Testimony in Support of SB 727
Senate Education, Energy, and the Environment Committee
February 25, 1:00 p.m.

Chair and Members of the Committee,

My name is Sam Kinch. I am a resident of Crownsville, Maryland. I'm testifying as a 30-year veteran of United States military and as a cyber security expert who spent years leading the integration of all National Guard cybersecurity forces into U.S. Cyber Command.

As a military veteran, I know personally how difficult it can be to exercise the basic right to vote when you're stationed overseas. Far too many service members deployed abroad do not vote—not because they lack commitment, but because the process can be slow, complicated, and unreliable. When stationed overseas I never knew whether my ballot was actually counted.

I was skeptical whether mobile voting could provide a solution. I spent my career defending critical cyber systems and identifying vulnerabilities. As a veteran and cyber security professional, I could not support mobile voting unless it had strong systems integrity.

However, after years of thorough review, I believe mobile voting can be secure and transparent. Technology and Security systems have evolved rapidly. We can now expand access without sacrificing integrity. The new technology is transparent and assumes bad actors are everywhere. If there's a problem, the system is designed to fail loudly and ensure that problems can be corrected, which is not the case with other forms of voting.

SB 727 provides Maryland municipalities the opportunity to use a responsible tool that has demonstrated a 300% increase in voter participation, encourages our deployed military members to vote, creates additional resilience in our electoral processes, and strengthens voter trust."

I respectfully urge a favorable report.

Thank you for your time and consideration.

Sarah Pan, Testimony in Support of SB 727.pdf
Uploaded by: Sarah Pan
Position: FAV

Sarah Pan, Testimony in Support of SB 727

Senate Education, Energy, and Environment Committee

February 25, 2026

Chair and Members of the Senate Education, Energy, and Environment Committee,

My name is Sarah Pan. I live in Ellicott City, Maryland, and I attend Marriotts Ridge High School. I am writing in support of Senate Bill 727, which will be heard on February 25 at 1:00 p.m.

I am a member of New Voters, an organization dedicated to expanding voter registration and civic participation among young people. Through that work, I have seen firsthand how important it is to remove barriers to voting and make participation possible for everyone—not just those who find it easiest to access the ballot.

SB 727 would allow cities to opt in to offering mobile voting as an additional method in municipal elections. It does not replace in-person or mail voting, but it gives communities flexibility to expand access responsibly.

I strongly resonate with the fact that this technology is not experimental. Secure mobile voting systems have already been piloted in multiple states, and studies have examined their security and auditability. The software incorporates encryption, identity verification, and transparent processes that allow ballots to be securely transmitted and counted.

Importantly, mobile voting can meaningfully expand disability voting rights. For voters with mobility challenges or print disabilities, traveling to a polling place or navigating paper ballots can be difficult. Secure mobile options can help ensure that more people are able to cast their ballots independently and privately.

As a young Marylander, I believe our democracy should reflect the world we live in—secure, accessible, and inclusive. I respectfully urge you to support SB 727.

Thank you for your time and consideration.

Sincerely,
Sarah Pan

SFI Statement in support of SB 727.pdf
Uploaded by: Sarah Streyder
Position: FAV

SECURE FAMILIES INITIATIVE

February 23, 2026

On behalf of the Secure Families Initiative, thank you for the opportunity to submit written testimony in support of SB 727. Secure Families Initiative (SFI) is a nonpartisan organization representing thousands of proud, diverse, active-duty military family members living across the country and stationed abroad. SFI's mission is to mobilize diverse military partners, parents, children, and veterans to vote and advocate for their communities.

This legislation is needed. Maryland's current system of voting leaves the ballot box inaccessible for many in our community. When military service members and their families get stationed far away from home, it can be an isolating and frustrating experience. Getting to vote in elections back home can help families stay connected and ease that transition – it's a reminder of where we belong, and an affirmation that our input matters.

Unfortunately, absentee military voters face high logistical barriers to casting their ballots through existing methods, which in Maryland is voting by mail. Military families stationed overseas or in rural domestic locations often face long wait times for mail delivery and return, which are out of our control. For example, if you are stationed in Japan, some families report a 6-8 week return time.

Electronic ballot return is already securely in use in a majority of states, including Delaware, Maine, Massachusetts, New Jersey, Rhode Island, and West Virginia. A total of 32 states plus the District of Columbia permit at least military service members and their families to return a ballot electronically, often by email or fax. Of those, 13 states expanded eligibility to voters with disabilities in order to make absentee voting fully accessible for all voters.

We urge you to support SB 727.

1725 I Street Northwest Suite 300, Washington, DC 20006

SB0727 Written Testimony.pdf
Uploaded by: Senator Karen Lewis Young
Position: FAV

KAREN LEWIS YOUNG
Legislative District 3
Frederick County

Budget and Taxation Committee
Chair
Pensions Subcommittee

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Annapolis Office
Miller Senate Office Building
11 Bladen Street, Suite 3 West
Annapolis, Maryland 21401
410-841-3575
800-492-7122 *Ext.* 3575
Karen.LewisYoung@senate.maryland.gov

District Office
253 East Church Street
Frederick, MD 21701
301-662-8520

The Honorable Brian Feldman, Chair
The Honorable Cheryl Kagan, Vice Chair
Education, Energy, and the Environment Committee
Miller Senate Office Building
Annapolis, MD 21401

February 25th, 2026

SB0727 Municipal Elections – Qualified Electronic Transmission Systems – Authorization for Use

Chair Feldman, Vice Chair Kagan, and esteemed colleagues,

Under current Maryland law, there are limited options for blind and print disabled voters to cast a *private* ballot in municipal elections. Additionally, for members of the military and their families deployed overseas, there are obstacles to voting in their hometown elections. Senate Bill 727 is a bill that enables, but does not require, municipalities to utilize a "qualified electronic transmission system" if, and only if, they determine it makes sense for their community.

A "qualified electronic transmission system" often takes the form of an application for a mobile device like a cellular telephone or tablet, by which residents can receive, mark, and return a ballot. Importantly, this legislation is built around modern security standards. SB727 requires that any system used meets strict qualifications. These include:

- End-to-end encryption,
- Multifactor authentication,
- Auditability for security purposes,
- A process for decrypting ballots by which to create a paper record; and,
- Biometric or equivalent digital identity verification.

The process begins with residents entering identifying information to look up their voter registration. Tools like two-factor authentication and biometric identities are used to confirm their identity. Next, voters mark their ballot and sign their absentee affidavit, similar to voting by mail. The ballot and affidavit are encrypted, and then the voter submits their vote directly to election officials.

Once submitted, the digital ballot box is disconnected from the internet for added security, and ballots are decrypted and printed to create an auditable paper trail. Further, many applications include a

means through which the voter can track their ballot for added oversight. Standard cybersecurity infrastructure, like that used in sensitive institutions like banks and healthcare systems, mitigates the threat of attacks.[1]

The concept of using a mobile device to receive a ballot is not new to Maryland. In 2016, the U.S. 4th Circuit Court of Appeals affirmed a district court ruling in *National Federation of the Blind v. Lamone*[2] requiring the State to implement electronic ballot delivery for all voters. The court found that an "online ballot marking tool" would enable disabled voters to mark their ballots electronically and privately in Maryland and "was a reasonable modification that did not fundamentally alter Maryland's absentee voting program." Indeed, the State Board of Elections offers a process whereby a voter can request an e-mail through which they can access the State's secure online ballot delivery system. From there, the voter is able to mark their ballot in private before printing it out and returning it to the State.

Unfortunately, under current law, the process for a voter to electronically receive and mark a ballot in private is only available for elections conducted by the State. Further, without State-level resources, municipalities face practical challenges. By enabling municipalities, they are free to implement mobile voting using tools within their means and on a timeline that accommodates their needs. Just as this legislation does not require municipalities to use mobile voting, neither does it require the use of any specific vendor or qualified electronic transmission system.

Beyond Maryland, 32 states allow electronic ballot returns for certain voters. In 2019, Denver, Colorado implemented mobile voting city-wide for military and overseas voters. Just last year, Anchorage, Alaska followed suit by offering all eligible voters the option of mobile voting in city elections.

Senate Bill 727 burdens neither municipalities nor the State. It offers a path towards enfranchisement for all voters, especially disabled voters and military families deployed overseas, while respecting local control. SB727 requires multifactor authentication of the voter's identity and end-to-end encryption to protect the integrity of their ballot. At the same time, by requiring the system to be auditable, it ensures the process is ultimately accountable to the public. I request a favorable report.

Sincerely,

Senator Karen Lewis Young

---

[1] "How Mobile Voting Works." *The Mobile Voting Project.*
[2] *National Federation of the Blind v. Lamone*, 813 F.3d 494 (4th Cir. 2016).

DRM Written Testimony FAV SB 727 Qualified Electro

Uploaded by: Braden Stinar

Position: FWA

Empowering People to Lead Systemic Change
The Protection and Advocacy System for the State of Maryland
1500 Union Ave., Suite 2000, Baltimore, MD 21211
Phone: 410-727-6352 | Fax: 410-727-6389
DisabilityRightsMD.org

SENATE EDUCATION, ENERGY, AND THE ENVIRONMENT COMMITTEE
Senate Bill 727: Municipal Elections – Qualified Electronic Transmission Systems – Authorization for Use
February 25, 2026
Position: Support (with Amendments)

Disability Rights Maryland (DRM) is the State's Protection and Advocacy agency, dedicated to advancing and protecting the civil rights of people with disabilities. As part of that mandate, DRM works to ensure that Marylanders with disabilities can fully and equally participate in the electoral process. DRM submits this testimony in support of Senate Bill 727, with amendments.

For many Marylanders with disabilities, voting still remains far more difficult than it should be. Senate Bill 727 would allow Maryland municipalities to opt in to secure mobile voting for local elections. Federal law, including the Americans with Disabilities Act (ADA) and the Help America Vote Act (HAVA), requires that voting systems and polling places provide meaningful access to individuals with disabilities. Yet practical barriers remain, preventing full participation in our democracy.

In particular, many voters with print disabilities—including individuals who are blind, have low vision, or certain cognitive or dexterity impairments—are unable to mark a paper ballot independently and privately. Too often, these voters must rely on assistance from poll workers, family members, or aides, which can undermine the fundamental right to cast a private ballot.

Secure mobile voting has the potential to address these barriers meaningfully. When implemented with strong safeguards, it can allow voters with disabilities to cast their ballots independently, privately, and securely, using assistive technologies they already rely on in their daily lives. This legislation is not intended to replace existing voting options but to expand access, ensuring that no voter is excluded because the current system fails to meet their needs.

We respectfully request that the bill be amended to explicitly require accessibility for voters with disabilities. Specifically, we propose adding a new element in the definition of "Qualified Electronic Transmission System," (Section 4–107.1(A) pg.2 line 8), as follows:

(8) Accessibility to voters with disabilities, including compatibility with commonly used assistive technologies and compliance with applicable digital accessibility standards for federal, state, and local governments.

This amendment provides clarity for municipalities and election officials, ensuring that accessibility obligations are implemented, and that municipal elections are equitable for all voters. Explicit statutory language ensures that all voters with disabilities, including voters who are blind, low-vision, Deaf or hard of hearing, have print disabilities, or cognitive disabilities, can vote privately and independently. Anchoring accessibility to recognized digital standards ensures protections remain consistent and durable, even if federal or state technical standards evolve. Requiring compatibility with assistive technologies ensures practical usability for all voters.

Although Senate Bill 727 represents an important step toward expanding voting access in Maryland, it is essential to emphasize that this effort must not be viewed as a substitute for the ongoing obligation to ensure that all physical polling places remain fully accessible and that all voters can cast their ballots privately and independently in person on election day. Voting is a personal experience, and some voters prefer in-person voting for a variety of reasons. Further, not all voters have access to reliable technology, or internet.

Maryland must continue to explore and implement accessibility improvements across all voting methods to accommodate the needs of individuals with diverse disabilities. Ensuring that every Marylander can vote securely, privately, and independently should remain a central priority in election policy. Access to the ballot is a bipartisan principle that strengthens our democracy and affirms the fundamental right to participate in civic life. **For these reasons, DRM requests a favorable report on Senate Bill 727 with amendments.**

Contact: Braden Stinar, BradenS@DisabilityRightsMD.org or 410-929-6859.

2026 Senate Bill 727 Oppose-merged.pdf
Uploaded by: C.Jay Coles
Position: UNF

Verified Voting

February 23, 2026

The Honorable Brian Feldman
Chair
Education, Energy, and the Environment Committee
Senate of Maryland
2 West Miller Senate Office Building
Annapolis, Maryland 21401
Via email

Dear Chair Feldman and Committee Members,

On behalf of Verified Voting, I am writing in opposition to Senate Bill 727 which would allow ballot return via the internet for certain voters. Verified Voting is a nonpartisan nonprofit organization with a mission to strengthen democracy for all voters by promoting the responsible use of technology in elections. Since our founding in 2004 by computer scientists, we have acted on the belief that the integrity and strength of our democracy rely on citizens' trust that each vote is counted as cast.

Ballot return via the internet (including mobile, email, fax, or website portal) fails to confer that trust. The security risks associated with electronic ballot return are severe, well-documented, and broadly acknowledged by the federal government's top security agencies and the nation's leading cybersecurity experts. At present, no known technology can secure ballots returned over the internet.

A joint analysis from the Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) classifies electronic ballot return as high risk, capable of enabling attacks that could alter or disrupt election results at scale. As stated in the analysis, "Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and can occur at scale."[1]

Other agencies have been equally clear. The Department of Defense has stated that it does not advocate transmitting cast ballots electronically under any method.[2] The Department of Homeland Security has likewise advised that online voting is not recommended at any level of government at this time.[3]

Congress shares these concerns. The U.S. Senate Select Committee on Intelligence concluded that no system of online voting has yet established itself as secure, and urged states to resist

[1] CISA, EAC, FBI, and NIST, Risk Management for Electronic Ballot Delivery, Marking, and Return, 2020/2024.

[2] DOD statement quoted in Greg Gordon, McClatchy, April 16, 2015.

[3] DHS statement quoted in Sarah Horwitz, Washington Post, May 17, 2016.

adopting internet voting.[4]

Independent cybersecurity experts mirror these findings. A working group convened by the University of California, Berkeley—including pioneers in cryptography and election security—determined that the technology required to secure online ballot return does not exist today, and that a single attacker could potentially alter thousands or even millions of votes.[5] The group further emphasized that online voting lacks the basic safeguards present in other online transactions, because the secret ballot prevents voters from verifying that their vote was received and counted as cast. Currently, no certification standards exist for electronic ballot return systems.

Electronic ballot return also carries multiple unique vulnerabilities, including malware, denial-of-service attacks, spoofing, identity fraud, and breaches that could expose voters' private information.[6] Any one of these could compromise an election; several could do so without detection.

Recently, a group of computer scientists and security researchers reaffirmed that while electronic ballot return methodologies continue to be researched, it is still not yet suitable for use in public elections. According to this group, "it has been the scientific consensus for decades that internet voting is not securable by any known technology. Research on future technologies is certainly worth doing. However, the decades of work on [electronic ballot return] systems has yet to produce any solution, or even any hope of a solution, to the fundamental problems."[7]

For these reasons, we respectfully urge you to reject Senate Bill 727 which would allow electronic ballot return for certain voters. Implementing electronic ballot return would run counter to the unified assessment of national security experts, cybersecurity professionals, federal intelligence agencies, and leading academic researchers. The risks—to ballot confidentiality, integrity, and public confidence—simply outweigh any potential benefits at this time.

We appreciate your leadership and your commitment to ensuring both accessibility and security in our elections.

Sincerely,

C.Jay Coles
Deputy Director of Legislative Affairs

[4] SSCI, Russian Active Measures, Vol. 1.

[5] UC Berkeley CSP, Working Group Statement on Internet Ballot Return, 2022.

[6] Ibid.

[7] Appel, Andrew, "Internet Voting Is Insecure and Should Not Be Used in Public Elections - CITP Blog, 2026."

BRENNAN CENTER FOR JUSTICE

February 23, 2026

The Honorable Brian Feldman
Chair
Education, Energy, and the Environment Committee
Senate of Maryland
2 West Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chair Feldman and Committee Members:

I am writing to you on behalf of the Brennan Center for Justice at NYU School of Law to oppose Senate Bill 727, which would enact law to allow the electronic return of marked ballots via the Internet for municipal elections. The Brennan Center is a national nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Brennan Center has a long history of partnering with election administrators, legislators, and other elected officials at the local, state, and federal level to reform and improve our elections and election administration.

Every independent review has found that we currently lack the technology to make electronic ballot return secure from attack. In 2020 and again in 2024, four federal executive branch agencies --the Cybersecurity and Infrastructure Security Agency (part of the Department of Homeland Security or DHS), the Election Assistance Commission, the Federal Bureau of Investigation, and the National Institute of Standards and Technology (NIST)-- jointly released a report concluding that internet-based return of votes presents a "high risk" to United States elections and cannot be secured.[1] It noted that, with internet-based ballot return, hackers from anywhere in the world could engage in large-scale, high-volume tampering with ballots that could impact results and possibly the outcome of an election. Two of these agencies have opined repeatedly on the issue over the years. In 2022, NIST issued the report *Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities* and notably did not include internet-based ballot return among its recommendations because, as it concluded, "there remain significant security, privacy, and ballot secrecy challenges."[2] In 2016, through its Office of Cybersecurity and Communications, DHS stated that "online voting, especially online voting in large scale, introduces great risk into the

[1] CISA et al., *Risk Management for Electronic Ballot Delivery, Marking, and Return*, at 1 (May 8, 2020).

[2] Kerrianne Buchanan et al., *NIST Spec. Pub. No. 1273, Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities*, at 48, 51 (Mar. 23, 2022).

election system by threatening voters' expectations of confidentiality, accountability and security of their votes and provides an avenue for malicious actors to manipulate the voting results."[3]

These agencies are not the only independent experts to opine on the issue. The Department of Defense has stated it "does not advocate for the electronic transmission of any voted ballot, whether it be by fax, email or via the Internet."[4] The United States Select Senate Committee on Intelligence concluded in a 2020 report that "States should resist pushes for online voting," because "no system of online voting has yet established itself as secure."[5] And a Working Group from the Center for Security in Politics at the University of California, Berkeley formed to determine "the feasibility of technical and implementation standards that would enable safe and secure digital remote ballot marking and return of these ballots" instead concluded "the current cybersecurity environment and state of technology makes it infeasible for the Working Group to draft responsible standards to support the use of internet ballot return in U.S. public elections at this time."[6]

Importantly, the consensus on the security challenges should be viewed within the current risk landscape. For at least a decade, our foreign adversaries—including Russia, China, and Iran—have launched cyberattacks targeting the United States' digital election infrastructure. They have done so in the 2016, 2018, 2020, 2022, and 2024 federal elections, with the goal of undermining confidence in our elections. At the same time, federal agencies have cut back on cyber and other election security support for local election offices.[7] Additionally, there is an active movement within the United States to undermine confidence in our elections, and we should not give it more oxygen through use of an untested and unproven technology for which there are currently no federal security standards.[8] Within this context, it is unwise for Maryland to adopt the use of electronic ballot return.

Of course, there are voters who face unique challenges casting their ballots and it is important to address those challenges -- but not with solutions that may put the security of their votes at risk or open them to challenge. There are many existing alternatives for casting ballots to electronic ballot return, which is unproven and untested.[9] We are happy to explore those alternatives with you.

---

[3] Sarah Horwitz, *More than 30 states offer online voting, but experts warn it isn't secure*, WASH. POST (May 17, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/.

[4] Greg Gordon, *As states warm to online voting, experts warn of trouble ahead*, MCCLATCHY WASHINGTON BUREAU (Apr. 16, 2015).

[5] See S. Rep. No. 116-290, at 61-62 (2020).

[6] R. Michael Alvarez et al., *Working Group Statement on Developing Standards for Internet Ballot Return*, CTR. FOR SEC. IN POL.,UNIV. OF CAL.,BERKELEY, at 2 (Dec. 2022).

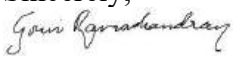
[7] Lawrence Norden, How the Federal Government Is Undermining Election Security, BRENNAN CENTER FOR JUSTICE (April 14, 2025).

[8] The Briefing, *Brennan Center Live:The Campaign to Undermine the Mid-terms* (YouTube, September 18, 2025).

[9] Verified Voting, *Casting Votes Safely: Examining Internet Voting's Dangers and Highlighting Safer Alternatives (October 2023).*

For these reasons, we respectfully urge you to reject Senate Bill 727, which would allow electronic ballot return in municipal elections. We appreciate your leadership and commitment to ensuring both accessibility and security in our elections.

Sincerely,



Gowri Ramachandran
Director of Elections and Security, Elections & Government
Brennan Center for Justice at NYU School of Law

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

INTRODUCTION

Some voters face challenges voting in-person and by mail. State and local election officials in many states use email, fax, web portals, and/or web-based applications to facilitate voting remotely for groups like military and overseas voters and voters with specific needs.

The Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) assess that the risks vary for electronic ballot delivery, marking, and return. While there are effective risk management controls to enable electronic ballot delivery and marking, we recommend paper ballot return as electronic ballot return technologies are high-risk even with controls in place. Recognizing that some election officials are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Notably, we assess that electronic delivery of ballots to voters for return by mail is less vulnerable to systemic disruption.

In this document, we identify risks and considerations for election administrators seeking to use electronic ballot delivery, electronic ballot marking, and/or electronic return of marked ballots. The cybersecurity characteristics of these remote voting solutions are further explored in NISTIR 7551: A Threat Analysis on UOCAVA Voting Systems.

RISK OVERVIEW

	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Technology Overview	Digital copy of blank ballot provided to voter	Making voter selections on digital ballot through the electronic interface	Electronic transmission of voted ballot
Risk Assessment	Low	Moderate	High
Identified Risks	Electronic ballot delivery faces security risks to the integrity and availability of a single voter's unmarked ballot	Electronic ballot marking faces security risks to the integrity and availability of a single voter's ballot	Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and, can occur at scale

CONNECT WITH US
www.cisa.gov

For more information,
www.cisa.gov/protect2020

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

All states use **electronic ballot delivery** to transmit a digital copy of an unmarked ballot to the intended voter to mark, in compliance with the Military and Overseas Voters Empowerment Act (MOVE). These ballot delivery systems are exposed to typical information security risks of internet-connected systems. The most severe risks to electronic ballot delivery systems are those that would impact the integrity and/or availability of the ballots, such as altering or removing ballot choices. These risks can be reduced and managed through use of appropriate security controls. Additionally, some electronic ballot delivery systems perform functions to verify a voter's identity before presenting them their assigned ballot. The identification process can use personal identifying information, such as name and driver's license number, or biometrics. When this verification is improperly configured, remote electronic ballot delivery systems can present additional privacy risks—like the loss or theft of the voter's personal and/or biometric identity information. These risks may be managed through configuration management and appropriate security controls.

Electronic ballot marking allows voters to mark their ballots outside of a voting center or polling place. Typically, this describes the electronic marking of a digital copy of the blank ballot using the electronic interface. The marked ballot is then returned to the appropriate official. Risks to electronic ballot marking are best managed through the production of an auditable record, meaning the voted ballot is printed and verified by the voter before being routed to the appropriate official. This auditable record is an important compensating control for detecting a compromise of security in remote voting.

Electronic ballot return, the digital return of a voted ballot by the voter, creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system. We view electronic ballot return as high risk.

Securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time. As the National Academies of Science, Engineering, and Medicine write in Securing the Vote: Protecting American Democracy (2018), "We do not, at present, have the technology to offer a secure method to support internet voting. It is certainly possible that individuals will be able to vote via the internet in the future, but technical concerns preclude the possibility of doing so securely at present." If election officials choose or are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Further, election officials should have a mechanism for voters to check the status of their ballot, as required for provisional ballots and military and overseas voters by the Help America Vote Act and the MOVE Act, respectively.

RISK COMPARISON – ELECTRONIC AND MAILED BALLOT RETURN

Some risks of electronic ballot return have a physical analogue to the return mailing of ballots. However, electronic systems present far greater risk to impact a significant number of ballots in seconds.

- **Scale –** While mailing of ballots could be vulnerable to localized exploitation, electronic return of ballots could be manipulated at scale. For mailed ballots, an adversary could theoretically gain physical access to a mailed ballot, change the contents, and reinsert it into the mail. This physical man-in-the-middle (MITM) attack is limited to low-volume attacks and mitigated by proper chain of custody procedures by election officials. In comparison, an electronic MITM attack could be conducted from anywhere in world, at high volumes, and could compromise ballot confidentiality, ballot integrity, and/or stop ballot availability.
- **Bring Your Own Device –** Unlike traditional voting systems, electronic ballot delivery and return systems require a voter to use their own personal devices such as a cell phone, computer, or tablet to access the ballot. A voter's personal device may not have the necessary safeguards in place. As a result, votes cast through "bring your own device" voting systems may appear intact upon submission despite tampering as a result of an attack on the personal device rather than on the ballot submission application itself. Voters using personal devices increase the potential for an electronic ballot delivery and return system to be exposed to security threats.
- **Voter Privacy –** Electronic ballot return brings significant risk to voter privacy. Unlike traditional vote by mail where there is separation between the voter's information and their ballot, many remote voting systems link the two processes together digitally. This makes it difficult to implement strong controls that preserve the privacy of the voter while keeping the system accessible.

TECHNICAL CONSIDERATIONS FOR ELECTRONIC BALLOT RETURN

Some voters, due to specific needs or remote locations, may not be able to print, sign, and mail in a ballot without significant difficulty. While we assess electronic ballot return to be high risk, some jurisdictions already use electronic ballot return systems, and others may decide to assume the risk.

While risk management activities should lower risk, election officials, network defenders, and the public may all have different perspectives on what level of risk is acceptable for the systems used to administer an election. For those jurisdictions that have accepted the high risk of electronic ballot return, the following guidance identifies cybersecurity best practices for internet- and network-connected election infrastructure. The information provided should be considered a starting point and is not a comprehensive list of defensive cybersecurity actions. Even with these technical security considerations, electronic ballot return remains a high-risk activity. Refer to applicable standards, best practices, and guidance on secure system development, acquisition, and usage.

GENERAL

- All election systems and technology should be completely separated from systems that are not required for the implementation or use of that specific system.
- Any ballots received electronically should be printed or remade as a paper record.
- Election officials should implement processes to separate the ballot from the voter's information in a manner that maintains the secrecy of the ballot.

CONNECT WITH US
www.cisa.gov

For more information,
www.cisa.gov/protect2020

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

- If the system attempts to verify the voter's identity through digital signature, biometric capture, or other method, assess whether an attacker could use this to violate ballot secrecy.
- The auditability of the results should not rely solely on the data stored digitally within the system.
- Best practices for securing voter registration data should be used to protect the personal identifying information that is stored in the voter registration database and used to authenticate voters.
- Removable storage media (e.g., USB drives, compact flash cards) used to handle sensitive election data should be obtained from a trusted source and erased before being used. To the extent practical, removable storage media should be new.
- Follow the domain security best practices issued by the Federal Government available at https://home.dotgov.gov/management/security-best-practices/

FAX

Facsimile (fax) machines are often used by local election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers should be aware of the risks and challenges associated with fax. Fax has no security protections unless sent over a secured phone line and is generally not considered suitable for sensitive communications. Faxes may be viewed or intercepted by malicious actors with access to phone lines. Furthermore, multipurpose fax machines with networked communications capability can be leveraged by cyber actors to compromise other machines on the network. We recommend election officials using fax machines implement the following best practices.

- Use a no-frills fax machine; multipurpose fax machines typically have modems for external network communications. If you only have a multipurpose fax machine, turn off the Wi-Fi capability and do not plug it into the network—only connect it to the phone line.
- Check the configuration to make sure that the fax cannot print more pages than anticipated from a single fax or ballot package.
- Use a dedicated fax machine and fax line for the distribution and receipt of ballots. Do not make the phone number publicly available, and only provide it in the electronic ballot package for voters who have been authorized to vote using electronic return.
- Election officials should set up transmission reports when faxing a ballot package to the voter to verify that the ballot package was received by the fax machine it was sent to.
- Use a trusted fax machine that has been under your control. Ensure you have enough fax machines and phone lines to handle the anticipated volume.
- When a public switch telephone line (PSTN) fax machine is not available and internet Protocols are used to fax, treat these systems as internet-connected systems, not as a fax machine using telephone protocols.

EMAIL

Email is a nearly ubiquitous communications medium and is widely used by election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers and election officials should be aware of the risks and challenges associated with email. Email provides limited security protections and is generally not considered suitable for sensitive communications. Email may be viewed or tampered with at multiple places in the transmission

process, and emails can also be forged to appear as if they were sent from a different address. Furthermore, email is often used in cyberattacks on organizations, such as attackers sending messages with malicious links or attachments to infect computers with malware. This malware could spread to other machines on the network if strong network segmentation techniques are not used.

- Use a dedicated computer that is separated from the remainder of the election infrastructure to receive and process these ballots. For very small offices that may not have the resources to use a dedicated computer, a virtual machine should be installed to separate these devices.
- Patch and configure the computer—as well as document viewer software—against known vulnerabilities (e.g., disable active content, including JavaScript and macros.).
- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify U.S.-based government organizations on the internet.
- Use encryption where possible (e.g., implement STARTTLS on your email servers to create a secure connection, encrypt attached files, etc.)
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to help identify phishing emails.
- Implement DMARC, DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) on emails to help authenticate emails sent to voters.
- Utilize anti-malware detection and encourage voters to as well. Make sure to update the anti-malware regularly.
- Implement multi-factor authentication (MFA) on any email system used by election officials.
- Follow best practices for generating and protecting passwords and other authentication credentials.
- Use a dedicated, shared email address for receiving ballots, such as Ballots@County.Gov. Implement naming conventions in subject lines that will help identify emails as legitimate (e.g., 2020 Presidential General). While a dedicated, shared email account is typically not a best practice, in this instance, it segregates potentially malicious attachments from the network.

WEB-BASED PORTALS, FILE SERVERS, AND APPLICATIONS

Websites may provide accessible and user-friendly methods for transmitting ballots and other election data. While web applications support stronger security mechanisms than email, they are still vulnerable to cyberattacks. Software vulnerabilities in web applications could allow attackers to modify, read, or delete sensitive information, or to gain access to other systems in the elections infrastructure. Sites that receive public input, such as web forms or uploaded files, may be particularly vulnerable to such attacks and should be used only after careful consideration of the risks, mitigations, and security/software engineering practices that went into that software.

- Avoid using knowledge-based authentication (e.g., address, driver's license number, social security number). To the extent practical, implement MFA for employees and voters and mandate MFA for all system administrators and other technical staff (including contractors).
- Patch and configure computers as well as document viewer software against known vulnerabilities (i.e., disable active content, including JavaScript and macros.).

CONNECT WITH US
www.cisa.gov

For more information,
www.cisa.gov/protect2020

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify US-based government organizations on the internet.
- Use secure coding practices (e.g., sanitized inputs, parameter checking) for web applications.
- Encrypt traffic using Hypertext Transfer Protocol Secure (HTTPS) supporting Transport Layer Security (TLS) version 1.2. If you use a file server, ensure it uses a secure file transfer protocol, such as SFTP or FTPS.
- Ensure you have the bandwidth/capacity to handle the anticipated volume of traffic.
- Obtain outside cybersecurity assessments, such as CISA vulnerability scanning and remote penetration testing.
- Develop a vulnerability management program (VMP). This allows well-meaning cybersecurity researchers to find and disclose vulnerabilities privately to an election official, giving the election official time to implement upgrades and patches before disclosing the information publicly.
- Place the application on a network that is continuously monitored, such as the network with a web application firewall, an Albert sensor, or an intrusion detection and prevention system.
- Carefully vet any third-party companies or contractors obtaining system access to perform security assessments or regular maintenance.
- Inform voters to only download the application from the trusted mobile application store.
- Encourage voters to use a trusted network and not an open Wi-Fi network.

RESOURCES

- CISA services can be located in the CISA Election Infrastructure Security Resource Guide. All services can be requested at cisaservicedesk@cisa.dhs.gov.
- Become an EI-ISAC Member by going to https://www.cisecurity.org/ei-isac/.
- CISA's Binding Operational Directive (BOD)18-01 addresses enhancing email and web security.
- NIST Activities on UOCAVA Voting
- NIST special publication (SP) 800-177 provides recommendations and guidelines for enhancing trust in email.
- NIST SP 800-52r2 provides guidelines for selection, configuration, and use of TLS.
- FBI's Protected Voices initiative provides information and guidance on cybersecurity and foreign influence topics.
- The EAC's Election Security Preparedness webpage collects multiple resources that can assist election administrators.
- For more information about how election jurisdictions in the United States vote remotely, please see Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes.

CONNECT WITH US
www.cisa.gov

For more information,
www.cisa.gov/protect2020

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

APPENDIX: DETAILED RISK MAPPING

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
RISK: Exploitation of software flaws in election infrastructure			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	High
Web	High	High	High
RISK: Unauthorized modification(s) to blank ballots			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	N/A
Web	Low	Moderate	N/A
RISK: Loss of voted ballot integrity			
Fax	N/A	N/A	High
Email	N/A	N/A	High
Web	N/A	N/A	High
Risk: Loss of ballot secrecy			
Fax	N/A	N/A	Moderate
Email	N/A	N/A	High
Web	N/A	N/A	High
RISK: Unauthorized individual participates in voting channel			
Fax	Moderate	N/A	High
Email	Low	Low	High
Web	Low	Moderate	High

CONNECT WITH US
www.cisa.gov

For more information,
www.cisa.gov/protect2020

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Risk: Broken Chain of Custody			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Low	Moderate	Moderate
RISK: Unable to access system or obtain ballot			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Moderate	High	High

CONNECT WITH US
www.cisa.gov

For more information,
www.cisa.gov/protect2020

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

Internet voting is insecure and should not be used in public elections

January 16, 2026

https://blog.citp.princeton.edu/2026/01/16/internet-voting-is-insecure-and-should-not-be-used-in-public-elections/

Signed by a group of 21 computer scientists expert in election security

Executive summary

Scientists have understood for many years that internet voting is insecure and that there is no known or foreseeable technology that can make it secure. Still, vendors of internet voting keep claiming that, somehow, their new system is different, or the insecurity doesn't matter. Bradley Tusk and his Mobile Voting Foundation keep touting internet voting to journalists and election administrators; this whole effort is misleading and dangerous.

Part I. All internet voting systems are insecure. The insecurity is worse than a well-run conventional paper ballot system, because a very small number of people may have the power to change any (or all) votes that go through the system, without detection. This insecurity has been known for years; every internet voting system yet proposed suffers from it, for basic reasons that cannot be fixed with existing technology.

Part II. Internet voting systems known as "End-to-End Verifiable Internet Voting" are also insecure, in their own special ways.

Part III. Recently, Tusk announced an E2E-VIV system called "VoteSecure." It suffers from all the same insecurities. Even its developers admit that in their development documents. Furthermore, VoteSecure isn't a complete, usable product, it's just a "cryptographic core" that someone might someday incorporate into a usable product.

Conclusion. Recent announcements by Bradley Tusks's Mobile Voting Foundation suggest that the development of VoteSecure somehow makes internet voting safe and appropriate for use in public elections. This is untrue and dangerous. All deployed Internet voting systems are unsafe, VoteSecure is unsafe and isn't even a deployed voting system, and there is no known (or foreseeable) technology that can make Internet voting safe.

Part I. All internet voting systems are insecure

Internet voting systems (including vote-by-smartphone) have three very serious weaknesses:

1. Malware on the voter's phone (or computer) can transmit different votes than the voter selected and reviewed. Voters use a variety of devices (Android, iPhone, Windows, Mac) which are constantly being attacked by malware.
2. Malware (or insiders) at the server can change votes. Internet servers are constantly being hacked from all over the world, often with serious results.
3. Malware at the county election office can change votes (in those systems where the internet ballots are printed in the county office for scanning). County election computers are not more secure than other government or commercial servers, which are regularly hacked with disastrous results.

Although conventional ballots (marked on paper with a pen) are not perfectly secure either, the problem with internet ballots is the ability for a single attacker (from anywhere in the world) to alter a very large number of ballots with a single scaled-up attack. That's much harder to do with hand-marked paper ballots; occasionally people try large-scale absentee ballot fraud, typically resulting in their being caught, prosecuted, and convicted.

Part II. E2E-VIV internet voting systems are also insecure

Years ago, the concept of "End-to-End Verifiable Internet Voting" (E2E-VIV) was proposed, which was supposed to remedy some of these weaknesses by allowing voters to check that their vote was recorded and counted correctly. Unfortunately, all E2E-VIV systems suffer from one or more of the following weaknesses:

1. Voters must rely on a computer app to do the checking, and the checking app (if infected by malware) could lie to them.
2. Voters should not be able to prove to anyone else how they voted – the technical term is "receipt-free" – otherwise an attacker could build an automated system of mass vote-buying via the internet. But receipt-free E2E-VIV systems are complicated and counterintuitive for people to use.
3. It's difficult to make an E2E-VIV checking app that's both trustworthy and receipt-free. The best solutions known allow checking only of votes that will be discarded, and casting of votes that haven't been checked; this is highly counterintuitive for most voters!
4. The checking app must be separate from the voting app, otherwise it doesn't add any malware-resistance at all. But human nature being what it is, only a tiny fraction of voters will do the extra steps to run the checking protocol. If hardly anyone uses the checker, then the checker is largely ineffective.

5. Even if some voters do run the checking app, if those voters detect that the system is cheating (which is the purpose of the checking app), there's no way the voters can prove that to election officials. That is, there is no "dispute resolution" protocol that could effectively work.

Thus, the problem with all known E2E-VIV systems proposed to date is that the "verification" part doesn't add any useful security: if a few percent of voters use the checking protocol and see that the system is sometimes cheating, the system can still steal the votes of all the voters that don't use the checking protocol. And you might think, "well, if some voters catch the system cheating, then election administrators can take appropriate action", but no appropriate action is possible: the election administrator can't cancel the election just because a few voters claim (without proof) that the system is cheating! That's what it means to have no dispute resolution protocol.

All of this is well understood in the scientific consensus. The insecurity of non-E2E-VIV systems has been documented for decades. For a survey of those results, see "Is Internet Voting Trustworthy? The Science and the Policy Battles". The lack of dispute resolution in E2E-VIV systems has been known for many years as well.

Part III. VoteSecure is insecure

Bradley Tusk's Mobile Voting Foundation contracted with the R&D company Free and Fair to develop internet voting software. Their press release of November 14, 2025 announced the release of an open-source "Software Development Kit" and claimed "This technology milestone means that secure and verifiable mobile voting is within reach."

After some computer scientists examined the open-source VoteSecure and described serious flaws in its security, Dr. Joe Kiniry and Dr. Daniel Zimmerman of Free and Fair responded. They say, in effect, that all the critiques are accurate, but they don't know a way to do any better: "We share many of [the critique's] core goals, including voter confidence, election integrity, and resistance to coercion. Where we differ is not so much in values as in assumptions about what is achievable—and meaningful—in unsupervised voting environments."

In particular,

- "We make no claim of receipt-freeness."
- "Of course, it may be possible for the voter to extract the randomizers from the voting client," meaning that voters would be able to prove how they voted, for example to someone on the internet who wanted to purchase votes at scale.
- "We agree that dispute resolution is essential to any *complete* voting system. We also agree that VoteSecure does not fully specify such a protocol." But really, the problem is much worse than this admission suggests. No one knows of a protocol

that could possibly work. So it's not a matter of dotting some i's and crossing some t's in their specification; it's a gaping hole (an unsolved, research-level problem).
- "Critique: Malware on the voter's device can compromise both voting and checking, rendering verification meaningless. Response: This critique is correct—and universal. There is no known technical solution that can fully protect an unsupervised endpoint from a sufficiently capable adversary."
- "VoteSecure does not claim to: Advance the state of the art in cryptographic voting protocols beyond existing E2E-VIV research; Eliminate coercion or vote selling in unsupervised elections; [or] Fully specify election administration, dispute resolution, or deployment processes. What VoteSecure aims to do is: Clearly define its threat model . . ."

In addition to the previously described flaws in the VoteSecure protocol, we note that its vote checking system is susceptible to mass automated vote-buying attacks[1]; and we have discovered a new flaw in the VoteSecure protocol that allows votes to be stolen[2]. *[click for details]*[1] This conclusion is based on a technical analysis. In the VoteSecure protocol, checking app can be run on a vote that is then cast; the checking app must be runnable on an alternate device than the voting app; that alternate device is likely a PC on which the user has control of installed software; user-installed software can extract decrypted randomizers; this allows the voter to participate in a mass vote-buying scheme. [2] "Clash attacks on the VoteSecure voting and verification process", by Vanessa Teague and Olivier Pereira, January 13, 2026.

Based on our own expertise test, and especially in light of the response from Free and Fair, we stand by the original analysis: Mobile Voting Project's vote-by-smartphone has critical security gaps.

Conclusion

It has been the scientific consensus for decades that internet voting is not securable by any known technology. Research on future technologies is certainly worth doing. However, the decades of work on E2E-VIV systems has yet to produce any solution, or even any hope of a solution, to the fundamental problems.

Therefore, when it comes to internet voting systems, election officials and journalists should be especially wary of "science by press release." Perhaps some day an internet voting solution will be proposed that can stand up to scientific investigation. The most reliable venue for assessing that is in peer-reviewed scientific articles. Reputable cybersecurity conferences and journals have published a lot of good science in this area. Press releases are not a reliable way to assess the trustworthiness of election systems.

Signed

(affiliations for for identification only and do not indicate institutional endorsement)

Andrew W. Appel, *Eugene Higgins Professor Emeritus of Computer Science, Princeton University*

Steven M. Bellovin, *Percy K. and Vida L.W. Hudson Professor Emeritus of Computer Science, Columbia University*

Duncan Buell, *Chair Emeritus — NCR Chair in Computer Science and Engineering, University of South Carolina*

Braden L. Crimmins, *PhD Student, Univ. of Michigan School of Engineering & Knight-Hennessy Scholar, Stanford Law*

Richard DeMillo, *Charlotte B and Roger C Warren Chair in Computing, Georgia Tech*

David L. Dill, *Donald E. Knuth Professor, Emeritus, in the School of Engineering, Stanford University*

Jeremy Epstein, *National Science Foundation (retired) and Georgia Institute of Technology*

Juan E. Gilbert, *Andrew Banks Family Preeminence Endowed Professor, Computer & Information Science, University of Florida*

J. Alex Halderman, *Bredt Family Professor of Computer Science & Engineering, University of Michigan*

David Jefferson, *Lawrence Livermore National Laboratory (retired)*

Douglas W. Jones, *Emeritus Associate Professor of Computer Science, University of Iowa*

Daniel Lopresti, *Professor of Computer Science and Engineering, Lehigh University*

Ronald L. Rivest, *Institute Professor, MIT*

Bruce Schneier, *Fellow and Lecturer at the Harvard Kennedy School, and at the Munk School at the University of Toronto*

Kevin Skoglund, *President and Chief Technologist, Citizens for Better Elections*

Barbara Simons, *IBM Research (retired)*

Michael A. Specter, *Assistant Professor, Georgia Tech*

Philip B. Stark, *Distinguished Professor, Department of Statistics, University of California*

Gary Tan, *Professor of Computer Science & Engineering, The Pennsylvania State University*

Vanessa Teague, *Thinking Cybersecurity Pty Ltd and the Australian National University*

Poorvi L. Vora, *Professor of Computer Science, George Washington University*

MD.SB 727 .testimony.written.pdf
Uploaded by: Susan Greenhalgh
Position: UNF

Testimony of Susan Greenhalgh
Senior Advisor on Election Security
Free Speech For People
Submitted to the
Maryland Senate
Education, Energy and the Environment Committee
Contact: susan@freespeechforpeople.org

Re: SB 727-UNFAVORABLE

February 23, 2026

Thank you Chair Feldman, Vice Chair Kagan, and members of the Committee for the opportunity to offer testimony on SB 727.

I serve as the senior advisor on election security for Free Speech For People, a national, non-profit non-partisan legal advocacy organization dedicated to defending our democracy and our Constitution. I have studied electronic ballot return for twenty years and have authored several reports on it, with partners including the American Association for the Advancement of Science[1] and the Association of Computing Machinists.[2] Free Speech For People is committed to preserving and enhancing access to the ballot for all voters, and to protecting the security and integrity of all ballots cast to ensure our elections represent the will of the voters.

We recognize and agree with the intent of SB 727 and support efforts to increase voter participation. *But we vigorously oppose the electronic return of voted ballots because ballots transmitted electronically, by email, fax and online ballot portal, are all at high risk for privacy risks, manipulation, and fraud.* At a time when election confidence is under attack, employing dangerously insecure electronic ballot return will degrade not just the security of Maryland's elections, but also confidence in elections and trust in government.

It is well-researched, settled science that returning ballots electronically over the internet is dangerously and unacceptably insecure. This has been established by the

[1] Greenhalgh, S., Newell, S., "Leveraging Electronic Ballot Return Safely and Securely During the COVID-19 Pandemic," *American Association for the Advancement of Science,* (Jun 2020). https://www.aaas.org/sites/default/files/2020-06/Leveraging%20Electronic%20Balloting%20Options%20Safely%20and%20Securely%20During%20the%20COVID-19%20Pandemic.pdf

[2] Greenhalgh, S., et al, "Email and Internet Voting: The Overlooked Threat to Election Security," *ACM U.S. Technology Policy Committee*, (Oct. 18, 2018). https://www.acm.org/binaries/content/assets/public-policy/jtreportemailinternetvoting.pd

Department of Homeland Security, the National Institute of Standards and Technology, the FBI, and U.S. Election Assistance Commission, as well as the National Academies of Science, Engineering and Medicine, and countless public and private studies. *Furthermore, the Maryland Department of Legislative Services has already conducted extensive and exhaustive research into this matter and presented its findings to the Committee, concluding that electronic return was unacceptably insecure. The Department of Legislative Services also concluded that Maryland was unlikely to face successful litigation to force online ballot return under the Americans with Disabilities Act.*

Existing security controls do not mitigate the security risks inherent with mobile voting.

The security controls included in SB 727, such as printing paper ballots after transmission, "air-gapping" the tabulation device, and end-to-end encryption, do not eliminate the high risk of mobile voting. These are provisions that vendors and proponents of online voting promote to obfuscate the insoluble security risks inherent with electronic ballot return.

Cyber-attacks cannot be effectively mitigated if an electronic ballot is printed on paper after it is received at the election office and the tabulation is conducted offline. Any cyber-attack, or manipulation of electronically transmitted ballots, can occur *after* the voter reviews the ballot, and *before* the ballot reaches the election office for printing. This means the printed ballot would reflect the corrupted votes chosen by the attacker, not the voter. Printing a ballot transmitted over the internet on an air-gapped does not protect it from online threats.

Moreover, even with so-called "end-to-end" encryption, ballots voted on a mobile application are vulnerable to undetectable and invisible manipulation by malware before the ballot is encrypted on the voter's device, and/or after it's decrypted at the election office. Encryption's security benefits are limited and cannot protect ballots created on a mobile application from malware on the mobile device.

Quite plainly, ballots returned online cannot be made secure. In 2020 and again in 2024, the Department of Homeland Security, the Federal Bureau of Investigation, the National Institute of Standards and Technology and the U.S. Election Assistance Commission published a risk-assessment[3] which "*recommends paper*

[3] Available at: https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001

ballot return, as electronic ballot return technologies are high risk even with controls in place."[4] [Emphasis added.] In other words, from 2020 to 2024, the Department of Homeland Security recommended states should continue to use paper ballots because there are serious and significant security risks introduced with the electronic transmission of marked ballots that cannot be adequately mitigated with the security tools and controls available, and ballots returned online are at high risk of tampering or manipulation.

DHS's blunt warning against the use of online voting echoed bipartisan recommendations from the U.S. Senate Select Committee on Intelligence, published in response to findings that foreign governments were actively trying to attack U.S. election systems. The Committee explicitly wrote: "States should resist pushes for online voting."[5]

In 2018, the National Academies of Sciences, Engineering and Medicine (NASEM) released a report stating that the technology to return marked ballots securely and anonymously over the internet does not exist.[6] These findings were all further affirmed by a study that was released from the University of California at Berkeley in December 2022.[7] This study is notable as it was commissioned by Bradley Tusk, a prominent proponent for online voting.

Despite promises from vendors and online voting supporters, many studies have reviewed specific[8] internet[9] voting systems[10] and consistently, all have found that despite their claims of innovation and security, these systems have fundamental vulnerabilities that are not remediable.

---

[4] *Ibid*.

[5] Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 2019, *Available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf*

[6] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. *Available at: https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy*

[7] R. Michael Alvarez et al., University of California, Berkeley Center for Security in Politics, Working Group Statement on Developing Standards for Internet Ballot Return 10 (2022), https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement-on-Internet-Ballot-Return.pdf.

[8] Massachusetts Institute of Technology, 2020. "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections." https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

[9] "Our full report on the Voatz Internet voting system," Trail of Bits, March 13, 2020. *Available at: https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/*

[10] See *supra* note 3.

At a time when election security and public confidence in our elections are under attack, increased electronic return of voted ballots, whether from a phone, tablet, or computer, is simply not safe or secure in any form.

Online voting is not comparable to online banking.

The public may ask, 'I can bank online, why can't I vote online?' But voting involves critical differences that make it a much more difficult enterprise to secure than online banking or commerce.[11] Online transactions are not secret or anonymous; a customer can check her statement to detect and address fraudulent charges. But we vote by secret ballot; there is no mechanism for the voter or election official to check to ensure ballots were not manipulated or hacked in transit and that the votes are legitimate. This makes online elections especially vulnerable to undetectable hacking.

The assumption that online banking can be done securely is faulty. It is estimated that banks lose millions or even billions of dollars every year to online attacks.[12] High profile hacks like that on Citibank, JP Morgan Chase, and Bank of America prove that even system with high cyber security budgets (much higher than Maryland's), cannot resist determined attackers.

Use of online voting is not evidence that it is secure.

During the early 2000's, Congress tasked the Department of Defense, through the National Defense Authorization Act, to develop a secure online voting system for military voters. Consequently, many states passed laws to permit electronic ballot return, planning to opt into the system provided by the Department of Defense. A system was developed in 2004 but was never deployed because a security evaluation determined that illegitimate ballots could be cast undetectably. Subsequently, after years of federal research that concluded electronic ballot return could not be made secure,[13] the Department of Defense and federal government abandoned the effort. Yet many states, adopted laws in the 2000's based on the

---

[11] "If I Can Shop and Bank Online, Why Can't I Vote Online?" *by David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory, member, Verified Voting Foundation Board, Board of Directors, California Voter Foundation https://www.verifiedvoting.org/resources/internet-voting/vote-online/*

[12] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[13] https://www.nist.gov/itl/voting/uocava-voting

reasonable assumption that the Department of Defense would soon offer a “secure” online balloting option, which never materialized.

It’s also important to also understand that most of these states enacted policies to allow online return of voted ballots when cybercrime was much less commonplace and mature. Cybercrime has advanced significantly in the last decade, and by expert accounts, the expertise and sophistication of today’s cyber criminals has far out-paced our defenses. We know much more today than we did then, and today’s policy decisions should be based on the research conducted and the current threat model.

Thank you for the opportunity to provide this testimony.

Respectfully submitted,

Susan Greenhalgh

Senior Advisor on Election Security

Free Speech For People.

CCMD - Oppose SB 727.pdf
Uploaded by: Susannah Goodman
Position: UNF

Common Cause
Maryland
Holding Power Accountable

121 Cathedral Street
Annapolis, MD 21401
443.906.0442
www.commoncause.org/md

February 23, 2026

The Honorable Brian J Feldman
Chair
The Honorable Vice Chair Kagan
Education, Energy, and the Environment Committee
Maryland Senate
2 West Miller Senate Office Building
Annapolis, Maryland 21401

Re: Senate Bill 727 – Oppose

Dear Chair Feldman, Vice Chair Kagan and Committee Members,

On behalf of Common Cause Maryland, I am writing in opposition to Senate Bill 727 which would allow ballot return via the internet for certain voters. Common Cause's mission is to uphold the core values of American democracy by creating an open, honest, and accountable government that serves the public interest, promotes equal rights, opportunity, and representation for all, and empowers people to make their voices heard in the political process. We are a nonprofit, nonpartisan membership organization with approximately 18,920 members in the state of Maryland.

Thank you for your work to expand and enhance voting access for Maryland voters and especially voters with disabilities. We share your commitment to ensuring that all voters, including those with disabilities can exercise their right to vote. However, legislation to allow electronic ballot return, via the passage of Senate Bill 727, would put voters' ballots at risk and undermine confidence in election results.

The security risks associated with electronic ballot return are severe, well-documented, and broadly acknowledged by the federal government's top security agencies and the nation's leading cybersecurity experts. At present, no known technology can secure ballots returned over the internet.

A joint analysis from the Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) classifies electronic ballot return as high risk, capable of enabling attacks that could alter or disrupt election results at scale. As stated in the analysis, "Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and can occur at scale."[1]

Other agencies have been equally clear. The Department of Defense has stated that it does not advocate transmitting cast ballots electronically under any method.[2] The Department of Homeland Security has likewise advised that online voting is not recommended at any level of government at this time.[3]

[1] CISA, EAC, FBI, and NIST, Risk Management for Electronic Ballot Delivery, Marking, and Return, 2020/2024.
[2] DOD statement quoted in Greg Gordon, McClatchy, April 16, 2015.
[3] DHS statement quoted in Sarah Horwitz, Washington Post, May 17, 2016.

Congress shares these concerns. The U.S. Senate Select Committee on Intelligence concluded that no system of online voting has yet established itself as secure, and urged states to resist adopting internet voting.[4]

Independent cybersecurity experts mirror these findings. A working group convened by the University of California, Berkeley—including pioneers in cryptography and election security—determined that the technology required to secure online ballot return does not exist today, and that a single attacker could potentially alter thousands or even millions of votes.[5] The group further emphasized that online voting lacks the basic safeguards present in other online transactions, because the secret ballot prevents voters from verifying that their vote was received and counted as cast. Currently, no certification standards exist for electronic ballot return systems.

Electronic ballot return also carries multiple unique vulnerabilities, including malware, denial-of-service attacks, spoofing, identity fraud, and breaches that could expose voters' private information.[6] Any one of these could compromise an election; several could do so without detection.

Recently, a group of computer scientists and security researchers reaffirmed that while electronic ballot return methodologies continue to be researched, it is still not yet suitable for use in public elections. According to this group, "it has been the scientific consensus for decades that internet voting is not securable by any known technology. Research on future technologies is certainly worth doing. However, the decades of work on [electronic ballot return] systems has yet to produce any solution, or even any hope of a solution, to the fundamental problems."[7]

For these reasons, we respectfully urge you to reject Senate Bill 727 which would allow electronic ballot return for certain voters. Implementing electronic ballot return would run counter to the unified assessment of national security experts, cybersecurity professionals, federal intelligence agencies, and leading academic researchers. The risks—to ballot confidentiality, integrity, and public confidence—simply outweigh any potential benefits at this time.

We appreciate your leadership and your commitment to ensuring both accessibility and security in our elections.

Sincerely

Susannah Goodman
Director
Election Security Program
Common Cause

[4] SSCI, Russian Active Measures, Vol. 1.

[5] UC Berkeley CSP, Working Group Statement on Internet Ballot Return, 2022.

[6] Ibid.

[7] Appel, Andrew, "Internet Voting Is Insecure and Should Not Be Used in Public Elections - CITP Blog, 2026."

SB 727_HB 1066_ Municipal Elections - Qualified E
Uploaded by: Trudy Tibbals
Position: UNF

SB 727/HB 1066: Municipal Elections - Qualified Electronic Transmission Systems - Authorization for Use: Please vote to **OPPOSE** this bill.

Dear Government, Labor & Elections Committee & Education, Energy & the Environment Committee:

I am writing to express my strong **opposition** to **SB 727/HB 1066**, "Municipal Elections - Qualified Electronic Transmission Systems - Authorization for Use."

While the bill includes some security features in its definition of a "qualified electronic transmission system," **authorizing municipalities to conduct entire local elections electronically—allowing voters to receive, mark, and return ballots via an online platform—introduces unacceptable risks to election integrity, security, and public trust.**

Key concerns include:

- **Vulnerability to cyber threats**: Even with encryption, multi-factor authentication, air-gapping, and auditability requirements, no electronic system is immune to hacking, malware, phishing, insider threats, or sophisticated state/nation-state attacks. A breach in a municipal election could alter results, disenfranchise voters, or erode confidence in all elections.
- **Lack of a universal, verifiable paper trail for all voters**: While the bill mentions a process for printing decrypted ballots to create a paper record, it does not guarantee that every electronic vote produces an auditable voter-verified paper ballot before transmission, **as recommended by election security experts.** Without mandatory hand-marked paper ballots or robust post-election audits, recounts become unreliable or impossible.
- **Disproportionate impact on smaller municipalities**: Many Maryland towns and cities lack the resources, expertise, or funding to implement, test, secure, and audit complex electronic voting systems effectively. This could lead to inconsistent standards, unequal access, or failures in smaller jurisdictions.
- **Potential for coercion, privacy erosion, or accessibility issues**: Electronic transmission raises risks of voter coercion (e.g., in shared households), device compromise, or exclusion of voters without reliable internet/technology. While the bill prohibits misuse of voter data, it does not fully address broader privacy or equity concerns in remote electronic voting.
- **Unnecessary expansion**: Maryland already has absentee/mail-in and in-person options for municipal elections. **Introducing internet-based voting for entire elections is misguided, especially given ongoing national concerns about**

electronic voting vulnerabilities and the absence of widespread, proven secure systems at the municipal level.

Municipal elections are foundational to local democracy and deserve the highest standards of security and verifiability. **Hand-marked paper ballots, counted publicly with oversight, remain the gold standard for preventing fraud and enabling trustworthy audits.** Allowing electronic transmission systems at this stage could invite problems rather than solve them.

I urge the Committee to **give SB 727/HB 1066 an unfavorable report** and prevent its passage. Preserving secure, transparent, and verifiable election processes is essential for maintaining public confidence in our democracy.

Thank you for your consideration.

Sincerely,

Trudy Tibbals

MDOD_HB1066_SB727_LOI_ATT.pdf
Uploaded by: Anne Blackfield
Position: INFO

Voluntary Voting System Guidelines VVSG 2.0

Requirements for the Voluntary Voting System Guidelines 2.0

February 10, 2021

Prepared for the ***Election Assistance Commission***

At the direction of the
Technical Guidelines Development Committee

Principle 5
Equivalent and Consistent Voter Access

All voters can access and use the voting system regardless of their abilities.

5.1 - Voters have a consistent experience throughout the voting process within any method of voting.

5.2 - Voters receive equivalent information and options in all modes of voting.

Principle 5
EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities.

Principle 5 ensures that all voters can cast their votes easily and accurately, regardless of any disabilities they may have. This fulfills the requirements of the *Help America Vote Act (HAVA), Section 301(a)(3) [HAVA02]* which states, "The voting system shall (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."

It also addresses *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]* which requires that electronic and information technology be accessible to people with disabilities, and the language access requirements in the *Voting Rights Act (VRA) [VRA65]*.

The goal of both guidelines in *Principle 5* is to ensure that everyone can use the voting system, regardless of their abilities or preferences. Voting equipment can present ballot choices in a variety of ways which make it possible for people with a wide range of disabilities to vote. The equipment must also fully support all the languages that the manufacture claims to support. The big differences are that guidelines:

1 – Consistent experience also covers the requirement that all vote records must be auditable by those who speak only English. Also, in addition to actually casting their votes, voters must have access to those same display formats and interaction modes for all information and instructions related to casting those votes.

2 – Equivalent information also addresses the requirement that these display formats (visual, audio, enhanced visual) and interaction modes (touch, tactile, limited dexterity) must offer consistent and equivalent support for the actions required to vote, and offer them in a way that does not introduce bias. In addition, if the voter switches formats mid-stream, for example from visual to audio or from Spanish to English, the system must preserve all settings and votes cast.

Finally, note that this principle's requirements, including supporting the display formats and interaction modes listed in *5.1-A – Voting methods and interaction modes*, also apply to all of the usability and accessibility requirements in *Principles 6-8*.

5.1 – Voters have a consistent experience throughout the voting process within any method of voting.

5.1-A – Voting methods and interaction modes

Within any method of voting, all display formats including enhanced visual and audio and all interaction modes including tactile and limited dexterity must have the same functionality as the visual format and touch mode including voting, verification, and casting.

Discussion

Methods of voting that a voting system might support include in-person voting, vote-by-mail, remote ballot marking, among others. The VVSG scope is in-person voting. For voting systems to meet this requirement they would need to include, for example:

- Features that support limited dexterity interaction to enable voters who lack fine motor control or the use of their hands, to submit their ballots privately and independently without manually handling the ballot.
- Features for paper ballots or paper verification records that assist voters with poor reading vision to read these ballots and records.
- Features to allow blind voters and voters with limited dexterity to perform paper-based verification or feed their own optical scan ballots into a scanner, if all other voters do so. For example, ballot papers or smart cards might provide tactile cues that allow the correct insertion of the card.
- Support for all voting variations. For example, if a visual ballot supports voting a straight-party ticket and then changing the vote for a single contest, so do all other display formats and interaction modes.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

5.1-B – Languages

The voting system must be capable of displaying and printing the ballot, contest options, review screens, voter verifiable paper records, and voting instructions in all languages the manufacturer has declared the system supports, in both visual and audio formats where applicable.

Discussion

Both written and unwritten languages are within the scope of this requirement.

The system will be tested in all languages that the manufacturer claims it is capable of supporting.

This requirement originates with the *VRA [VRA65]*.

5.1-C – Vote records

All records, including paper ballots and voter verifiable paper records, must have the information required to support auditing by election workers and others who can only read English.

Discussion

Although the system needs to be easily usable by voters using an alternative language, records of the vote also need to be fully available to English-only readers to support election administration and auditing. See *9.4 - The voting system supports efficient audits* for related requirements.

To meet this requirement, a paper ballot may not be a fully bilingual ballot. For instance, the full text of a ballot question might appear only in the alternative language, but the contest option (for example, “yes / no”) needs to be readable by English-only readers.

5.1-D – Accessibility features

Accessibility features must be integrated into the manufacturer’s voting system so accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting.

Discussion

This requirement ensures accessibility to the voter throughout the entire session. Not only are individual system components (such as ballot markers, paper records, and optical scanners) accessible, but they also support voters with disabilities throughout the process of voting from activation through casting. Requirements for individual system components are described in *Principle 7: Marked, Verified, and Cast as Intended*. This general requirement supports *HAVA [HAVA02].*

Related requirements: 6.1-B – Warnings

5.1-E – Reading paper ballots

If the voting system generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record, then the voting system must allow the voter to verify the paper record using the same access features they used to mark the ballot, including enhanced visual and audio formats and tactile and limited dexterity modes.

Discussion

Paper records present difficulties for voters who use large font, high contrast, alternative languages, and other settings. The purpose of this requirement is to ensure that all voters have a similar

opportunity for vote verification. For ballot marking devices, for example, if the voter is using audio to make their selections, the voter verifiable paper record, not the stored voter selections, must be read back.

This requirement allows the voter to use the same access features throughout the entire voting session. It also does not preclude the voter from choosing a different access feature to verify the record. For example, the voting system might provide a reader that converts the paper record contents into audio output.

This requirement supports *HAVA [HAVA02]*.

Related requirements: 7.1-I – Text size (paper)

5.1-F – Accessibility documentation

As part of the overall system documentation the manufacturer must include descriptions and instructions for all accessibility features that describe:

- recommended procedures that fully implement accessibility for voters with disabilities, and
- how the voting system supports those procedures.

Discussion

The purpose of this requirement is for the manufacturer not simply to deliver system components, but also to describe the accessibility scenarios they are intended to support, so that election offices have the information they need to effectively make accessibility features available to voters with disabilities.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

Related requirements: 7.3-N – Instructions for voters
7.3-O – Instructions for election workers

MDOD_HB1066_SB727_LOI_ATT.pdf
Uploaded by: Anne Blackfield
Position: INFO

Voluntary Voting System Guidelines VVSG 2.0

Requirements for the Voluntary Voting System Guidelines 2.0

February 10, 2021

Prepared for the ***Election Assistance Commission***

At the direction of the
Technical Guidelines Development Committee

Principle 5
Equivalent and Consistent Voter Access

All voters can access and use the voting system regardless of their abilities.

5.1 - Voters have a consistent experience throughout the voting process within any method of voting.

5.2 - Voters receive equivalent information and options in all modes of voting.

Principle 5
EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities.

Principle 5 ensures that all voters can cast their votes easily and accurately, regardless of any disabilities they may have. This fulfills the requirements of the *Help America Vote Act (HAVA), Section 301(a)(3) [HAVA02]* which states, "The voting system shall (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."

It also addresses *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]* which requires that electronic and information technology be accessible to people with disabilities, and the language access requirements in the *Voting Rights Act (VRA) [VRA65]*.

The goal of both guidelines in *Principle 5* is to ensure that everyone can use the voting system, regardless of their abilities or preferences. Voting equipment can present ballot choices in a variety of ways which make it possible for people with a wide range of disabilities to vote. The equipment must also fully support all the languages that the manufacture claims to support. The big differences are that guidelines:

1 – Consistent experience also covers the requirement that all vote records must be auditable by those who speak only English. Also, in addition to actually casting their votes, voters must have access to those same display formats and interaction modes for all information and instructions related to casting those votes.

2 – Equivalent information also addresses the requirement that these display formats (visual, audio, enhanced visual) and interaction modes (touch, tactile, limited dexterity) must offer consistent and equivalent support for the actions required to vote, and offer them in a way that does not introduce bias. In addition, if the voter switches formats mid-stream, for example from visual to audio or from Spanish to English, the system must preserve all settings and votes cast.

Finally, note that this principle's requirements, including supporting the display formats and interaction modes listed in *5.1-A – Voting methods and interaction modes*, also apply to all of the usability and accessibility requirements in *Principles 6-8*.

5.1 – Voters have a consistent experience throughout the voting process within any method of voting.

5.1-A – Voting methods and interaction modes

Within any method of voting, all display formats including enhanced visual and audio and all interaction modes including tactile and limited dexterity must have the same functionality as the visual format and touch mode including voting, verification, and casting.

Discussion

Methods of voting that a voting system might support include in-person voting, vote-by-mail, remote ballot marking, among others. The VVSG scope is in-person voting. For voting systems to meet this requirement they would need to include, for example:

- Features that support limited dexterity interaction to enable voters who lack fine motor control or the use of their hands, to submit their ballots privately and independently without manually handling the ballot.
- Features for paper ballots or paper verification records that assist voters with poor reading vision to read these ballots and records.
- Features to allow blind voters and voters with limited dexterity to perform paper-based verification or feed their own optical scan ballots into a scanner, if all other voters do so. For example, ballot papers or smart cards might provide tactile cues that allow the correct insertion of the card.
- Support for all voting variations. For example, if a visual ballot supports voting a straight-party ticket and then changing the vote for a single contest, so do all other display formats and interaction modes.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

5.1-B – Languages

The voting system must be capable of displaying and printing the ballot, contest options, review screens, voter verifiable paper records, and voting instructions in all languages the manufacturer has declared the system supports, in both visual and audio formats where applicable.

Discussion

Both written and unwritten languages are within the scope of this requirement.

The system will be tested in all languages that the manufacturer claims it is capable of supporting.

This requirement originates with the *VRA [VRA65]*.

5.1-C – Vote records

All records, including paper ballots and voter verifiable paper records, must have the information required to support auditing by election workers and others who can only read English.

Discussion

Although the system needs to be easily usable by voters using an alternative language, records of the vote also need to be fully available to English-only readers to support election administration and auditing. See *9.4 - The voting system supports efficient audits* for related requirements.

To meet this requirement, a paper ballot may not be a fully bilingual ballot. For instance, the full text of a ballot question might appear only in the alternative language, but the contest option (for example, “yes / no”) needs to be readable by English-only readers.

5.1-D – Accessibility features

Accessibility features must be integrated into the manufacturer’s voting system so accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting.

Discussion

This requirement ensures accessibility to the voter throughout the entire session. Not only are individual system components (such as ballot markers, paper records, and optical scanners) accessible, but they also support voters with disabilities throughout the process of voting from activation through casting. Requirements for individual system components are described in *Principle 7: Marked, Verified, and Cast as Intended*. This general requirement supports *HAVA [HAVA02].*

Related requirements: 6.1-B – Warnings

5.1-E – Reading paper ballots

If the voting system generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record, then the voting system must allow the voter to verify the paper record using the same access features they used to mark the ballot, including enhanced visual and audio formats and tactile and limited dexterity modes.

Discussion

Paper records present difficulties for voters who use large font, high contrast, alternative languages, and other settings. The purpose of this requirement is to ensure that all voters have a similar

opportunity for vote verification. For ballot marking devices, for example, if the voter is using audio to make their selections, the voter verifiable paper record, not the stored voter selections, must be read back.

This requirement allows the voter to use the same access features throughout the entire voting session. It also does not preclude the voter from choosing a different access feature to verify the record. For example, the voting system might provide a reader that converts the paper record contents into audio output.

This requirement supports *HAVA [HAVA02]*.

Related requirements: 7.1-I – Text size (paper)

5.1-F – Accessibility documentation

As part of the overall system documentation the manufacturer must include descriptions and instructions for all accessibility features that describe:

- recommended procedures that fully implement accessibility for voters with disabilities, and
- how the voting system supports those procedures.

Discussion

The purpose of this requirement is for the manufacturer not simply to deliver system components, but also to describe the accessibility scenarios they are intended to support, so that election offices have the information they need to effectively make accessibility features available to voters with disabilities.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

Related requirements: 7.3-N – Instructions for voters
7.3-O – Instructions for election workers

MDOD_SB0727_LOI_EEE_2026.02.20.pdf
Uploaded by: Anne Blackfield
Position: INFO

Carol A. Beatty, Secretary
Anne Blackfield, Deputy Secretary

Wes Moore, Governor
Aruna Miller, Lt. Governor

Maryland
DEPARTMENT OF DISABILITIES

BILL: **SB 727**
POSITION: **INFO – Letter of Information**
COMMITTEE: Education, Energy, and the Environment
DATE: February 23, 2026

SUBMITTED BY: Maryland Department of Disabilities
217 East Redwood Street, Suite 1300, Baltimore, MD 21202

Dear Chair Feldman,

The Maryland Department of Disabilities (MDOD) is submitting a letter of information for **SB 727, Municipal Elections – Qualified Electronic Transmission Systems – Authorization for Use**. This legislation establishes the criteria for a 'qualified electronic transmission system' for the purposes of receiving, marking, and returning a voting ballot. It also authorizes a municipality to conduct a municipal election through the use of such a system.

Under laws such as the federal Help America Vote Act (HAVA) and Title II of the Americans with Disabilities Act (ADA), voting systems - including those for municipal elections - must be accessible to voters with disabilities. Section 301(a) of HAVA requires that voting systems shall "be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters." Title II of the ADA requires that individuals with disabilities have equal access to government information and services, including the voting process.

Additionally, the U.S. Election Assistance Commission, in its Voluntary Voting System Guidelines, has set out standards for ensuring equal access to voting systems under Principle 5, "Equivalent and Consistent Voting Access." In particular, Principle 5.1-D states, "Accessibility features must be integrated into the manufacturer's voting system so accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting." A sample of the relevant section of the U.S. Election Assistance Commission's guidelines are attached to this letter. We are happy to provide additional information about the accessibility requirements and specifications included in the Voluntary Voting System Guidelines.

One way to demonstrate Maryland's commitment to ensuring accessible voting at all levels of government is by adding an eighth element to the definition of "qualified electronic voting transmission system" under proposed Local Government Article § 4701.1, such as "accessible to

Carol A. Beatty, Secretary
Anne Blackfield, Deputy Secretary

Wes Moore, Governor
Aruna Miller, Lt. Governor

Maryland
DEPARTMENT OF DISABILITIES

voters with physical or print disabilities." While the accessibility obligations for these systems would exist regardless of whether they are explicitly codified under § 4701.1, including this element could serve as a clarifying reminder to municipalities of their legal and civic duties to ensure inclusion and access for voters with disabilities.

Thank you for reviewing this letter of information.

Sincerely

Carol A. Beatty

Carol A. Beatty
Secretary, Department of Disabilities

217 EAST REDWOOD STREET, SUITE 1300, BALTIMORE, MARYLAND 21202
VOICE/TTY 410-767-3660 VOICE/TTY 1-800-637-4113 FAX 410-333-6674 EMAIL info.mdod@maryland.gov