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.