Testimony of Susan Greenhalgh
Senior Advisor on Election Security
Free Speech For People
before the
Ways and Means Committee
Maryland General Assembly
Contact: susan@freespeechforpeople.org

Re: HB0645-UNFAVORABLE

February 28, 2023

Thank you for the opportunity to submit testimony on SB0488.

Free Speech For People is a national, non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions and advocacy, secure, transparent, trustworthy, and accessible voting policies for all voters. For example, we launched a legal challenge to voter registration restrictions in Arizona, resulting in tens of thousands of additional voters being able to register to vote. We avidly support the responsible use of technology to improve access to the ballot for all voters, of all abilities, and support the exploration of increased accessible voting options and improvements for voters with disabilities. But we vigorously oppose the adoption of policies that permit 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, expanding dangerously insecure electronic ballot return will degrade not just the security of Maryland's elections, but also confidence in elections and trust in government. We urge the Committee to vote NO on HB0645 and not advance it from Committee.

Ballots returned online are at high risk for manipulation or fraud.

Quite plainly, ballots cannot be securely returned electronically. Proponents of electronic ballot return may suggest, erroneously, that secure online return of voted ballots is possible with today's computer security tools, or that the use of

cloud storage or a portal will adequately protect ballot security. All this is incorrect.

In 2020, 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[1] which "*recommends paper ballot return, as electronic ballot return technologies are high risk even with controls in place*."[2]** [Emphasis added.] **In other words, the Department of Homeland Security recommends 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."[3]

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.[4] Many studies have reviewed specific internet voting systems and consistently, all have found that despite their claims of innovation and security, these systems have fundamental vulnerabilities.

Before the 2020 election, the U.S. Postal Service secretly developed and tested an online voting system that used **blockchain** in an effort to secure the ballots.[5] The Postal Service engaged security researchers at the University of Colorado to test

---

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

[2] *Ibid*.

[3] 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*

[4] 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*

[5] Joe Marks, Jacob Bagoge, "USPS built and secretly tested a mobile voting system before 2020," *The Washington Post,* December 13, 2021. *Available at: https://www.washingtonpost.com/nation/2021/12/13/usps-built-secretly-tested-mobile-voting-system-before-2020/*

the system for security. The researchers were able to compromise the blockchain and tamper with ballots undetectably in multiple ways.

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. Furthermore, with the ongoing conflict in Ukraine, the threat of Russian cyber attacks on our election infrastructure has increased.[6] Election security is a matter of the highest U.S. national security, so we would be taking a very grave risk to our democracy any time the threat of foreign interference is escalated, as it is now.

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.[7] 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.

And even if an attack was detected, there would be no way for election officials to determine which ballots were manipulated and which are legitimate, making an online attack uncorrectable. Such systems are, by definition, not auditable; since there is no indelible, source record of voter intent, there is no audit record. In addition, banks may calculate an acceptable level of fraud and factor that into the cost of doing business, or take out insurance to cover their losses, but we cannot accept any illegitimate ballots. Finally, 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.[8] High profile hacks like that on Citibank, JP Morgan Chase, and Bank of America prove that even system with high cyber

---

[6] Joseph Marks, "Russian hacking threats aren't over, Congress was warned last night," *The Washington Post*, March 9, 2022. *Available at: https://www.washingtonpost.com/politics/2022/03/09/russian-hacking-threats-arent-over-congress-was-warned-last-night/*

[7] "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/*

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

security budgets (much higher than Washington's), cannot resist determined attackers.

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

It's true that over two dozen states currently permit electronic ballot return, but that does not mean it's secure or trustworthy.

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,[9] the Department of Defense and federal government abandoned the effort.

It's important to also understand that most of these states enacted policies to allow online return of voted ballots when cyber crime was much less commonplace and mature. Cyber crime 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 current threat model.

Alternative accessible voting options should be explored.

At present, voters with disabilities still experience significant barriers to casting their votes privately and securely,[10] and we should make efforts to resolve these challenges. We understand the profound difficulties you face to assure every voter's ability to vote and strongly support interventions to assure voters' equal opportunity and access to cast their vote – securely and verifiably. Recognizing that no current solution is ideal for all voters, we support thoughtful consideration

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

[10] "Disability and Voting Accessibility in the 2020 Elections, Final Report on Survey Results." February 16, 2021. Rutgers University; U.S. Election Assistance Commission. *Available at: https://smlr.rutgers.edu/sites/default/files/Documents/Centers/Program_Disability_Research/Disability_and_voting_accessibility_2020_election_Final_Report_survey_results.pdf*

to improve secure innovations, such as mobile accessible voting. Mobile accessible voting is offered in some states where election workers bring accessible ballot marking devices to the residences and workplaces of voters with disabilities. These accessible devices allow disabled voters to privately and independently cast a secured, verifiable paper ballot with accessible technology. (Currently Oregon and San Francisco and its neighboring counties have launched such an effort.[11])

However, electronic ballot return is not the answer. The 2020 election underscores the importance of being able to examine voted paper ballots, not just digital artifacts. A recent report published in the Journal of Cybersecurity warns, "While current election systems are far from perfect, Internet- and blockchain-based voting would greatly increase the risk of undetectable, nation-scale election failures."[12]

We would welcome the opportunity to provide the Committee with further information on technical aspects of electronic ballot return. We strongly urge the Committee to vote NO on HB0645, and seek alternative, accessible voting options.

Thank you for your consideration.

[11] San Francisco, Oakland, San Jose and some of the twelve counties that surround it have invested a $1 million federal grant to provide Mobile Voting Vehicles to increase voting access to disabled and underserved voters. See: http://www.bayareauasi.org/sites/default/files/resources/approval_2022_january_meeting_master.pdf, page 57.

[12] Sunoo Park, Michael Specter, Neha Narula, Ronald L Rivest, MIT, Going from bad to worse: from Internet voting to blockchain voting, Journal of Cybersecurity, Volume 7, Issue 1, 2021, https://doi.org/10.1093/cybsec/tyaa025