Verified Voting

February 28, 2022

Senate State and Local Government Committee
State of Tennessee
600 Dr. MLK Jr. Blvd
Nashville, TN 37243
via email

Multiple Cybersecurity Experts Have Concluded That Internet Voting is Unsafe and Insecure

Dear Committee Members,

On behalf of Verified Voting, I am writing in opposition to Senate Bill 2255 which would allow ballot return via the internet. 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) undermines that trust.

The National Academies of Sciences, Engineering and Medicine released a report in 2018 stating that the technology to return marked ballots securely and anonymously over the internet does not exist.[1] Additionally, in the lead-up to the 2020 General Election, DHS, EAC, FBI, and NIST told states and election officials that electronic ballot return "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** [emphasis added]."[2] Nothing has changed; no new internet technology has been created to mitigate this risk.

Many believe that with changing technology the time has come to introduce internet voting into the voting process. Researchers from the Massachusetts Institute of Technology and the University of Michigan conducted a security review of the Democracy Live online voting system. They found that "OmniBallot uses a simplistic approach to Internet voting that is vulnerable to vote manipulation by malware on the voter's device and by insiders or other attackers… In addition, Democracy Live, which appears to have no privacy policy, receives sensitive personally identifiable information—including the voter's identity, ballot selections, and browser

[1] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.
[2] DHS Memo, 2020. https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001

fingerprint— that could be used to target political ads or disinformation campaigns."[3] Other analyses of like systems have also been performed with each finding that such systems are insecure.[4] Unlike other internet transactions, voting must simultaneously maintain ballot secrecy while still providing a verifiable record of the voter's intent. Internet voting simply does the opposite. There is currently no internet technology available that allows for the secure transmission of voted ballots while also maintaining voter privacy and ballot verifiability.

Language within the bill seems to suggest that if an approved system is used, one that meets certain requirements, it can be deemed safe and secure. Sadly, no system can meet such requirements. Today's internet simply is not equipped with the needed safeguards to transmit voted ballots electronically in a secure manner.

We understand the profound challenges you face to assure every voter's ability to vote. Verified Voting strongly supports interventions to assure voters' equal opportunity and access to cast their vote – securely and verifiably. However, internet voting of any kind is not the answer. Recognizing that no one solution is ideal for all voters, we support thoughtful consideration of secure alternatives, such as Remote Accessible Vote by Mail (RAVBM). RAVBM allows for electronic delivery of a blank ballot to the voter so they may use their own equipment to mark their ballot, print it out and return the paper ballot to their elections office. The contested 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."[5]

At a time when election security and public confidence are under unprecedented attack, expanding use of insecure technology in the voting process would result in unprovable election results. We urge this Committee to reject Senate Bill 2255.

Respectfully submitted,

Pamela Smith
President & CEO

[3] Security Analysis of Democracy Live Online Voting System, 2020. https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf

[4] Security Analysis of Democracy Live Online Voting System, 2020. https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf

[5] 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