Verified Voting

August 5, 2021

Council of the District of Columbia
1350 Pennsylvania Avenue, NW
Washington, D.C. 20004
Via email

Verified Voting Urges Rejection of Bill 24-353 - Voter Mobile App Amendment Act of 2021

Dear Council Members,

On behalf of Verified Voting, I write in opposition to Bill 24-353 that would allow electronic ballot return. 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. With this in mind we oppose allowing voted ballots to be returned electronically through insecure means.

Multiple cybersecurity experts have concluded that internet and mobile voting is insecure. 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, the Department of Homeland Security, the Election Assistance Commission, the Federal Bureau of Investigation, and the National Institute of Standards and Technology 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.

Blockchain does not solve the security issues inherent to internet voting.

The National Academies report states that "blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities." Blockchain technology is designed to keep information secure once it is

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

received. It cannot defend against the multitude of threats to that information before it is entered in the blockchain, and voters cannot verify their votes are entered into the blockchain correctly without compromising ballot secrecy. Recording ballots on a blockchain also risks ballot secrecy if encryption keys are not properly protected or software errors allow decryption of individual ballots.

We know that there are vendors of online and mobile election systems that make bold statements about how safe and secure their systems are. Unfortunately, these vendors do not reliably assess the security risks of the products they sell. Their public relations, marketing, and lobbying efforts consistently downplay the inherent risks of internet voting. Multiple studies have been performed on these types of systems and the conclusion is always the same: the risks are significant and no good solution yet exists to mitigate those risks.[3]

Washington, D.C. is uniquely positioned to reject internet and mobile voting. In 2010 the District of Columbia held a mock election using an internet voting system and invited participants to try and compromise the security of that system. According to researchers who successfully compromised the system, "Within 48 hours of the system going live, we had gained near-complete control of the election server. We successfully changed every vote and revealed almost every secret ballot. Election officials did not detect our intrusion for nearly two business days—and might have remained unaware for far longer had we not deliberately left a prominent clue."[4] The internet is the same today as it was then. By rejecting Bill 24-353, you will prevent anything like this from happening during a real election.

At a time when election security and public confidence are under attack, electronic return of voted ballots presents a slippery slope to vulnerable and insecure elections. We therefore urge you to reject Bill 24-353.

Respectfully,

Mark Lindeman
Acting Co-Director

Cc: Mayor Muriel Bowser

[3] See https://verifiedvoting.org/internet-voting-resources/#currentsystems
[4] Wolchok, Scott & Wustrow, Eric & Isabel, Dawn & Halderman, J. (2012). Attacking the Washington, D.C. Internet Voting System. 10.1007/978-3-642-32946-3_10.