Verified Voting

September 16, 2022

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

Verified Voting Urges Rejection of Internet Voting

Dear Council Members,

On behalf of Verified Voting, I write to oppose proposals to weaken D.C. elections by adopting insecure online voting. Verified Voting is a non-partisan, non-profit organization that works to strengthen democracy for all voters by promoting the responsible use of technology in elections. Given the present vulnerabilities of the internet and electronic systems, voter-verified paper ballots are integral to public confidence in elections. Election and cybersecurity leaders acknowledge that paper ballots crucially contributed to U.S. election security and resilience in 2020; they warn that internet ballot return is unsafe. Implementing unrestricted online voting in spite of these realities would harm D.C. voters and U.S. democracy.

Bill 24-672, introduced in February, would require the District to implement, by 2024, a system enabling all D.C. voters to vote from a smartphone, tablet, or computer. We honor the intention of this proposal to make voting more accessible, but it contradicts the considered judgment of cybersecurity experts. In its 2018 consensus report, *Securing the Vote*, the National Academies of Sciences, Engineering and Medicine stated bluntly:

> At the present time, the Internet (or any network connected to the Internet) **should not be used for the return of marked ballots**. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as **no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.**[1] [emphasis added, footnotes omitted]

Similarly, in the lead up to the 2020 General Election, the Department of Homeland Security and three other federal agencies 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**

[1] National Academies of Science, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (National Academies Press, 2018), page 8. Available at https://doi.org/10.17226/25120.

electronic ballot return as high risk. [emphasis added]."[2] Note that these risks are posed to voters individually—to their privacy, to their capacity to vote, and to their votes being recorded and counted accurately—and collectively, as the basis for public confidence in elections erodes. Opening the system to all voters magnifies this collective risk far beyond any current U.S. implementation of internet voting.

No new technology has been created since 2018 to provide the robust guarantees that the National Academies called for. The bill's cover letter posits that "rapid advancements in cryptography in recent years" can provide for security and verifiability, but no independent assessment supports that hope. Blockchain technology has been widely touted as a game-changer for elections – but it isn't. 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."[3] As tempting as it may be to accept brash claims about technical breakthroughs, betting against cybersecurity leaders with elections at stake is a bad gamble for D.C. voters.

The District of Columbia has been here before. In 2010, the District held a mock election using an internet voting system and invited participants to attempt to compromise the security of that system. Researchers swiftly succeeded: "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 next time could be far worse. Attackers may be able to tamper with votes without being detected, or to irretrievably disrupt an election.

In the *best* case, a turn away from voter-verified paper ballots would undermine elections by failing to provide physical evidence of voter intent to resolve doubts or disputes. After the 2020 election, national election and cybersecurity leaders described the election as "the most secure in American history." They explained that key states "have paper records of each vote, allowing the ability to go back and count each ballot if necessary. This is an added benefit for security and resilience."[5] The nation needed that margin in 2020, and needs it for the foreseeable future.

[2] Election Assistance Commission, National Institute of Standards and Technology, Federal Bureau of Investigation, and Cybersecurity & Infrastructure Security Agency (Department of Homeland Security), "Risk Management for Electronic Ballot Delivery, Marking, and Return," May 2020. Available at https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001.

[3] *Securing the Vote*, page 104. The report elaborates on this point in detail.

[4] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, "Attacking the Washington, D.C. Internet Voting System," *Proceedings of the 16th Conference on Financial Cryptography & Data Security*, February 2012. Available at https://jhalderm.com/pub/papers/dcvoting-fc12.pdf.

[5] "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," November 12, 2020. Available at https://www.google.com/url?q=https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

At a time when election security and public confidence are under relentless attack, the District should not rely on insecure technology for voters that produces unprovable election results. We urge the Council to reject any proposal that includes electronic return of voted ballots.

Respectfully,

Mark Lindeman, Ph.D.
Policy & Strategy Director

Cc: Mayor Muriel Bowser