December 21, 2021

Hon. Charles Allen, Chair
Committee on the Judiciary and Public Safety
Council of the District of Columbia
1350 Pennsylvania Avenue, NW
Washington, D.C. 20004

Dear Chair Allen and Judiciary Committee Members:

We are writing to share information on the scientific evidence regarding the insecurity of internet voting and urge you to consider the profound risks of adopting mobile or internet voting in the District of Columbia.[1]

We have long supported responsible uses of technology to facilitate voting and increase access to the ballot box for all voters. But the electronic return of voted ballots creates serious and presently unsolvable security vulnerabilities. At a time when election security and public confidence of our elections are under attack, increased electronic return of voted ballots, whether from a phone, tablet, or computer, is simply not safe or secure, and will undermine confidence and trust in elections.

Online voting has been rejected as unacceptably insecure by DHS, FBI, NIST, the Senate Select Committee on Intelligence and the National Academies of Science, Engineering and Medicine.

Among computer scientists and national election security experts there is no debate: online voting cannot be adequately secured for governmental elections. Last year, the Department of Homeland Security (DHS), the U.S. Election Assistance Commission, the Federal Bureau of Investigation, and the National Institute of Standards and Technology specifically advised "we recommend paper ballot return as **electronic ballot return technologies are high-risk even with [risk-management] controls in place**."[2] In other words, the security tools currently available such as end-to-end verifiability, encryption, cloud-based services, and distributed ledger technology (blockchain), are unable to secure online voting systems.

---

[1] Martin Austermuhle, "There's a New Push to Let DC Voters Cast Ballots from Their Phones," *DCist,* Dec. 2, 2021. *Available at: https://dcist.com/story/21/12/02/theres-a-new-push-to-let-dc-voters-cast-ballots-from-their-phones/*

[2] Available at: https://epic.org/privacy/voting/Risk-Management-Electronic-Ballot-May2020.pdf

The risk assessment went on to warn 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."**[3]

DHS's blunt warning against the use of online voting echoed bipartisan recommendations from the Senate Select Committee on Intelligence published in response to findings that foreign governments were actively trying to attack U.S. election systems. The Committee wrote: "States should resist pushes for online voting. One main argument for voting online is to allow members of the military easier access to their fundamental right to vote while deployed. While the Committee agrees states should take great pains to ensure members of the military get to vote for their elected officials, no system of online voting has yet established itself as secure."[4]

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**.[5] Many studies have reviewed specific internet voting systems and consistently, all have found that despite their claims of innovation, these systems have fundamental vulnerabilities.[6]

We understand the profound challenges 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 of other secure innovations, such as Remote Accessible Vote by Mail (RAVBM). This innovation allows for electronic delivery of a blank ballot to the voter so they may use their own equipment at home to mark their ballot, print it out and return the paper ballot to their elections office. However, internet voting, with or without blockchain, 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."[7]

---

[3] Ibid.

[4] 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

[5] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

[6] 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

[7] 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

We would welcome the opportunity to provide the Council with further information on technical aspects of end-to-end verification and internet voting. For the present, we urge the District of Columbia in the strongest possible terms not to adopt, test or develop internet voting of any kind to preserve the security and accuracy of voting in the District of Columbia and voters' confidence in the elections process.

Respectfully submitted,

Michael D. Fernandez, Director
Center for Scientific Evidence in Public Issues (EPI Center), American Association for the Advancement of Science

Jeremy Epstein, Chair
U.S. Technology Policy Committee
Association for Computing Machinery

Karen Hobert Flynn, President
Common Cause

John Bonifaz, President & Co-Founder
Free Speech for People

Susan Dzieduszycka-Suinat, President and CEO
U.S. Vote Foundation and Overseas Vote

Sangita Sigdyal, President and CEO
Verified Voting

cc: Councilmember Anita Bonds
Councilmember Mary Cheh
Councilmember Vincent C. Gray
Councilmember Brook Pinto