EPI Center
CENTER FOR SCIENTIFIC EVIDENCE IN PUBLIC ISSUES
AAAS

acm U.S. Technology Policy Committee

Common Cause

PUBLIC CITIZEN

FREE SPEECH FOR PEOPLE .ORG

verifiedvoting

March 22, 2022

Hon. Kelly M. Burke, Chair
Hon. Katie Stuart, Vice-Chair
Members of Ethics and Elections Committee
Illinois General Assembly
409 Capitol Avenue
Springfield, Illinois

Dear Chair Burke, Vice-Chair Stuart and Members of the Committee on Ethics and Elections:

We are writing to share information on the scientific evidence regarding the insecurity of internet voting, and urge you to contemplate the profound risks associated with mobile or internet voting.[1]

We have long supported responsible uses of technology to facilitate voting and increase access to the ballot box for all voters, especially voters with disabilities. Presently, voters with disabilities still experience significant barriers to casting their vote privately and securely.[2] In particular, we strongly support remote accessible vote by mail (RAVBM) to expand access when more voters are using vote by mail in Illinois and across the country. 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

[1] Lizzie Seils, "House committee considers measure to expand voting accessibility for visually impaired," *Week.com,* March 15, 2022. *Available at: https://www.week.com/2022/03/15/house-committee-considers-measure-expand-voting-accessibility-visually-impaired/*

[2] "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*

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.

Furthermore, with the ongoing conflict in Ukraine, the threat of Russian cyber attacks on our election infrastructure has escalated.[3] Now is not the time to adopt election processes that are known to be vulnerable to hackers.

Online voting creates insurmountable security risks to elections, as assessed by the Department of Homeland Security, the FBI, and the National Institute of Standards and Technology,[4] the Senate Select Committee on Intelligence[5] and the National Academies of Science, Engineering and Medicine.[6]

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**."[7] **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.**

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."[8]**

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

[3] 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/*

[4] "Risk Management for Electronic Ballot Delivery and Marking," Cyber Security and Infrastructure Security Agency, Federal Bureau of Investigation, National Institute of Standards and Technology, U.S. Election Assistance Commission. *Available at: https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001*

[5] 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*

[6] 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*

[7] See *supra* note 4.

[8] Ibid.

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."[9]

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**.[10] Many studies have reviewed specific internet voting systems and consistently, all have found that despite their claims of innovation, these systems have fundamental vulnerabilities.[11]

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 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."[12]

We would welcome the opportunity to provide the Committee with further information on technical aspects of internet voting. For the present, we urge the Illinois legislature 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 Illinois 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

[9] See *supra* note 5.
[10] See *supra* note 6.
[11] 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
[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

Karen Hobert Flynn
President
Common Cause

John Bonifaz
President and Co-Founder
Free Speech for People

Aquene Freechild
Campaign Co-Director, Democracy
Public Citizen

Pam Smith
President and CEO
Verified Voting