November 9, 2021

Voting Accessibility Task Force
State of Rhode Island
via email

RE: Verified Voting Opposes Internet Voting

Dear Task Force Members,

On behalf of Verified Voting, I am writing in opposition to 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) fails to confer that trust.

Multiple cybersecurity experts have concluded that internet voting is unsafe and 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.

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] 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.

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 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.

Earlier this summer the Rhode Island Board of Elections voted to oppose legislation at the time that would have allowed for expansion of electronic ballot return. We would call on this Task Force to uphold that position. There is currently no internet technology available that allows for the secure transmission of voted ballots while also maintaining voter privacy and ballot verifiability. **Rhode Island has pioneered the use of risk-limiting audits to verify election results, yet expanding electronic ballot return jeopardizes your ability to conduct those audits effectively.**

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 current solution is ideal for all voters, we support thoughtful consideration of other secure innovations, such as Remote Accessible Vote by Mail (RAVBM) or go-to voter services. RAVBM 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. Go-to voter services would enable bipartisan teams to bring accessible, certified voting equipment directly to voters to allow them to cast their vote independently, securely and verifiably. 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."[4]

We realize that UOCAVA voters are currently permitted to return their voted ballots via fax or email. We regard this as a dangerous precedent to be reversed, not expanded. At a time when election security and public confidence are under attack, expanding use of insecure technology

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

[4] 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

in the voting process would result in unprovable election results. We urge this task force not to adopt, test, promote or develop internet voting.

Respectfully submitted,

Mark Lindeman, Ph.D.
Director

Cc:
Jason Martiesian, Deputy Secretary of State
Rob Rock, Director of Elections, Secretary of State's Office
Robert Rapoza, Executive Director, Board of Elections
Miguel Nunez, Deputy Director of Elections, Board of Elections
Rhode Island Board of Elections