Verified Voting

State, Veterans, & Military Affairs Committee
Colorado Senate
200 E Colfax Avenue
Denver, CO 80203
via electronic submission

April 2, 2021

RE: Verified Voting Opposition to Senate Bill 21-188

Dear Committee Members,

On behalf of Verified Voting, I write in opposition to Senate Bill 21-188 regarding 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. It is with this in mind that we oppose allowing voted ballots to be returned electronically through insecure means, a dangerous practice that SB 21-188 regrettably expands.

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

The City of Denver participated in an electronic ballot return pilot for UOCAVA voters in 2019. The Massachusetts Institute of Technology performed a security analysis of the vendor chosen to conduct that pilot and found that the vendor "has vulnerabilities that allow different kinds of

[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

adversaries to alter, stop, or expose a user's vote, including a sidechannel attack in which a completely passive network adversary can potentially recover a user's secret ballot."[3]

We must also point out that the actual device (e.g. smartphone) that voters cast their votes on has security vulnerabilities. The voter's device may already be corrupted with malware or viruses that could interfere with ballot transmission or even spread that malware to the computer at the elections office on the receiving end of the online ballot. Unlike other internet transactions, voting must simultaneously maintain ballot secrecy while still providing a verifiable record of the voter's intent. Internet voting does not allow the voter to verify that the record received by the elections office in fact reflects the voter's choices and thus those votes are not auditable.

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.

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. Electronic return fails to confer this equality, and it threatens the trustworthiness of the election itself. Recognizing that no current solution is ideal for all voters, we support thoughtful consideration of other secure innovations. We would be happy to participate in further discussions of how to meet the standard of equal access and uncompromised security.

We realize that Colorado 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, electronic return of voted ballots presents a slippery slope to vulnerable and insecure elections. We therefore urge that SB 21-188 be rejected.

Respectfully submitted,

Mark Lindeman
Acting Co-Director

[3] 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