Verified Voting

April 6, 2022

Senate Committee on State Affairs
State of Alaska
120 4th Street
Juneau, AK 99801
*Via email*

RE: Verified Voting Opposes Senate Bill 205

Dear Chair Shower and Committee Members:

On behalf of Verified Voting, I am writing to oppose Senate Bill 205 as written due to the profound risks of adopting mobile or internet voting. 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.

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.

**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. In the lead up to the 2020 General Election, the Department of Homeland Security, 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**."[1] 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] 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."**[2]

DHS's 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."[3]

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

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. 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."[6]

Language within the bill seems to suggest that if an approved system is used, one that

---

[2] Ibid.

[3] 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

[4] 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

[5] 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/wpcontent/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

[6] 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

meets certain requirements, it can be deemed safe and secure. Sadly, no system can meet such requirements. Today's internet simply is not equipped with the needed safeguards to transmit voted ballots electronically in a secure manner. Similarly, producing a paper ballot corresponding to each digital absentee ballot does not inherently improve security. If the paper ballot is produced *after* the digital ballot has been received by the elections office – if the voter can never verify the paper ballot – it is no more trustworthy than the digital record on which it depends.

We would welcome the opportunity to provide the Committee with further information on technical aspects of end-to-end verification and internet voting and to brainstorm other, more secure means and methods to ensure equal access to the ballot. We especially recommend consideration of Remote Accessible Vote by Mail (RAVBM). RAVBM allows for electronic delivery of a blank ballot to the voter so they may use their own equipment to mark their ballot, print it out and return the paper ballot to their elections office. With appropriate security requirements such as those successfully implemented in California,[7] RAVBM allows voters to mark and verify their ballots with accessible technology without sacrificing privacy or security.

We urge this Committee in the strongest possible terms to reject Senate Bill 205.

Respectfully submitted,

Mark Lindeman, Ph.D.
Director

[7] See the California Elections Code, Division 19, Chapter 3.5, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=ELEC&division=19.&title=&part=&chapter=3.5. In particular, Section 19295 prohibits RAVBM systems from transmitting voter selections over the internet. Some RAVBM systems transmit voter selections as voters mark their ballots, compromising voter privacy. California has certified four RAVBM systems without that flaw.