Verified Voting

May 12, 2021

Senate Judiciary Committee
State of Rhode Island
82 Smith Street
Providence, RI 02903
via electronic submission

RE: Verified Voting Opposition to Senate Bill 738

Dear Committee Members,

On behalf of Verified Voting, I write in opposition to Senate Bill 738 regarding electronic ballot return. 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. With this in mind we oppose allowing voted ballots to be returned electronically through insecure means.

Multiple cybersecurity experts have concluded that internet voting is 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.

This bill says that ballots returned electronically can only be accepted through a system that, in part, "meets the National Institute of Standards and Technology (NIST) Cybersecurity Framework guidelines." It is exceptionally unclear just how electronic ballot return can meet those guidelines when NIST told states and local governments just last year that they "recommend paper ballot return as electronic ballot return technologies are high-risk even with controls in place."[2] Additionally, in 2011, NIST released a report which studied internet voting in detail that "concluded that internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems. Malware on voters' personal computers poses a

[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

serious threat that could compromise the secrecy or integrity of voters' ballots. And, the United States currently lacks a public infrastructure for secure electronic voter authentication."[3] This is as true today as it was in 2011. Rhode Island has pioneered the use of risk-limiting audits to verify elections results, yet expanding electronic ballot return jeopardizes your ability to conduct those audits effectively.

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 know that there are vendors of online election systems that make bold statements about how safe and secure their systems are. Unfortunately, these vendors do not reliably assess the security risks of the products they sell. Their public relations, marketing, and lobbying efforts consistently downplay the inherent risks of internet voting. Multiple studies have been performed on these types of systems and the conclusion is always the same: the risks are significant and no good solution yet exists to mitigate those risks.

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 ballot -- securely and verifiably. However, electronic return fails to confer this equality, and it threatens the trustworthiness of the election itself.

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 738 be rejected.

Respectfully submitted,

Mark Lindeman
Acting Co-Director

[3] National Institute of Standards and Technology. “NIST Activities on UOCAVA Voting.” https://www.nist.gov/uocava-voting