VerifiedVoting

May 9, 2023

Elections Committee
Michigan House of Representatives
124 North Capitol Avenue
Lansing, MI 48933
*via email*

**RE: Verified Voting Urges Rejection of House Bill 4210**

Dear Committee Members,

On behalf of Verified Voting, I write in opposition to House Bill 4210, which would expand the electronic return of voted ballots by spouses of active-duty members of the uniformed services. Verified Voting is a nonpartisan nonprofit organization whose mission is 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, a dangerous practice that HB 4210 regrettably would expand.

Four federal government agencies have concluded in a recent risk assessment that "electronic ballot return" is "High" risk, even with security safeguards and cyber precautions in place. The agencies warn that electronic ballot return "faces significant security risks to the confidentiality, integrity, and availability of voted ballots," and that these risks can "ultimately affect the tabulation and results and can occur at scale." The agencies instead explicitly recommend the use of paper ballots.[1] The risk assessment was issued by the Federal Bureau of Investigation (FBI), the Department of Homeland Security's Cybersecurity Infrastructure Security Agency (CISA), the U.S. Elections Assistance Commission (EAC) and the National Institute for Standards and Technology (NIST).

At a time where the integrity and veracity of election results are continuously called into question, it would be imprudent to ignore the security warning issued by the four government agencies charged with protecting our nation's election infrastructure.

Furthermore, there is broad consensus that electronic ballot return presents severe security risks to the integrity of our elections, because ballots cast over the internet can be intercepted, deleted and altered at scale—and can therefore change election results.

[1] U.S. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Institute of Standards and Technology and the U.S. Election Assistance Commission, Risk Management for Electronic Ballot Delivery, Marking, and Return 1 (2020), available at https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf?mo d=article_inline.

- In a letter dated April 17, 2023 to Secretary of State Jocelyn Benson, no fewer than 28 professors, employed at universities and colleges in Michigan, endorse how dangerously insecure electronic ballot return is.[2]

- In 2019, the bipartisan U.S. Senate Select Committee on Intelligence reported on its findings that foreign governments were actively trying to attack American election systems. As part of that report, the Committee determined "States should resist pushes for online voting. ...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]

- Just recently, experts convened by the University of California's Berkeley Center for Security in Politics concluded that creating standards for online ballot return, so that it can be done securely and privately, was not feasible. "When internet ballot return is employed," the Working Group wrote, "it may be possible for a single attacker to alter thousands or even millions of votes. And this lone individual could perpetrate an attack from a different continent from the one where the election is being held – perhaps even while under the protection of a rogue nation where there is no concern of repercussions."[4]

We know that there are vendors of online and mobile 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.[5]

At a time when election security and public confidence are under relentless attack, Michigan should not rely on insecure technology for voters that produces unverifiable election results. Again, we urge you to vote "no" on HB 4210 and reject any other proposal that includes electronic return of voted ballots.

Respectfully submitted,

C.Jay Coles
Senior Policy & Advocacy Associate

---

[2] See attached letter

[3] S. Rep. No. 116-290, vol. 1, at 59–60 (2019), available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[4] R. Michael Alvarez et al., University of California, Berkeley Center for Security in Politics, Working Group Statement on Developing Standards for Internet Ballot Return 10 (Dec. 14, 2022), available at https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement-on-Internet-Ballot-Return.pdf.

[5] See https://verifiedvoting.org/internet-voting%20resources/#currentsystems