



October 31, 2023

Oppose House Bill 4210: Electronic Ballot Return As Amended

Dear Members of the Senate:

Thank you for your work to expand and enhance voting access for Michigan voters. Our organizations share your commitment to ensure that all voters—including military and overseas voters—can exercise their right to vote.

However, we write to you with grave concerns regarding HB 4210 as passed in the House. This legislation expands internet voting in the state of Michigan. **This legislation will put the security of Michigan's elections at high risk for cyber incidents, and undermine the fragile public confidence in election results.**

It is worth noting that Proposition 2, passed last year, and Senate Bill 259, signed into law in May, provide an additional six days for military and overseas ballots to be received and counted, if they are postmarked by election day. **We urge the Legislature to evaluate the impact of this deadline extension in reducing the number of overseas/military ballots that are not counted, rather than approving the electronic voting provisions in House Bill 4210.**

Amendments Will Not Increase Security

While amendments in this bill are well-meaning and intended to lessen the risk to the validity of our elections, in practice, the amendments do little to assuage security concerns.

For example, HB 4210 amends current law to allow military spouses, in addition to active duty military voters, to use an internet voting system to receive, mark, and return a digital ballot over the internet. The amendment to this bill appears to

require that voters also send in a paper ballot to the election office. However, as the electronic ballots will be counted regardless of whether the paper ballot is received, voters will have little incentive to send the paper ballot back in. This provision is little more than a smoke screen designed to make the system of internet voting appear more secure, when in reality it is not.

A similar law in New Jersey, which allows overseas and military voters to return a voted ballot electronically, also requires the voter to send a paper ballot to their county board.¹ Unlike HB 4210, the NJ law does not indicate that the electronically returned ballot will be counted regardless of whether the paper ballot is received. In practice, however, those electronic ballots have been counted despite the language of the law, demonstrating that no such provision is secure.²

Federal Agencies, Authorities, Oppose Internet Voting

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,**” and explicitly recommends paper ballots.³ The bulletin 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).

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

¹ NJ Rev. Stat. § 19:59-15.

² See Penny Venetis et al., *The Perfect Storm: Voting in New Jersey in the Wake of Superstorm Sandy*, Rutgers School of Law Rutgers School of Law Constitutional Rights Clinic 33–29 (2014), available at <https://web.archive.org/web/20150127111115/https://law.newark.rutgers.edu/files/RutgersLawHurricaneSandyReport.pdf>.

³ 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), https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf?mod=article_inline.

results.⁴

- NIST, the federal agency responsible for issuing cybersecurity standards, has also conducted research on ways to enhance accessibility for voters with disabilities. Its 2022 report, *Promoting Access to Voting*, did not recommend electronic ballot return, instead concluding, “there remain **significant security, privacy, and ballot secrecy challenges**.”⁵
- 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.”⁶
- **Michigan’s Election Security Advisory Commission** specifically did not recommend electronic ballot return in its 2020 report, because “**there is no method to reliably secure the ballot** all the way to the local jurisdiction.”⁷
- 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.”⁸

⁴ See Verified Voting, *Casting Votes Safely: Examining Internet Voting’s Dangers and Highlighting Safer Alternatives* 5–7 (2023), <https://verifiedvoting.org/publication/casting-votes-safely-oct-2023/>.

⁵ National Institute of Standards and Technology, *Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities* 48 (Mar. 2022), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1273.pdf>.

⁶ S. Rep. No. 116-290, vol. 1, at 59–60 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

⁷ Michigan Election Security Advisory Commission, *Report and Recommendations* 34 (2020), https://www.michigan.gov/sos/-/media/Project/Websites/sos/31lawens/ESAC_Report_Recommendations.pdf.

⁸ 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), <https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement-on-Internet-Ballot-Return.pdf>.

Some overseas and military voters face unique challenges to returning their ballots that concern us all. But, electronic ballot return is not the answer. Michigan, along with Minnesota, Vermont, and New York, has often led the nation in overseas and military voter participation, without permitting electronic ballot return.⁹

In Michigan in 2022, 132 overseas and military ballots were not counted because they were returned after the election day deadline.¹⁰ As discussed above, Proposition 2, passed last year, and Senate Bill 259, signed into law in May, provide an additional six days for military and overseas ballots to be received and counted, if they are postmarked by election day, a measure adopted specifically to improve military and overseas voter participation. **We urge the Legislature to evaluate the impact of this deadline extension in reducing the number of overseas/military ballots that are not counted, rather than approving the electronic voting provisions in House Bill 4210.**

We urge the Legislature to also invest resources in improving access for overseas and military voters, *without returning ballots over the internet*. For example, the Federal Voting Assistance Program has a variety of resources to help election officials to do outreach to overseas and military voters, and to communicate with them about various voting options and deadlines;¹¹ the Legislature might consider funding such outreach and communications efforts by election officials.

Internet Voting Systems Can Throw Entire Elections into Chaos

The transmission of electronic ballots exposes not just the ballots, but the election itself. As we saw in Ecuador just two months ago and Australia in 2021, internet voting systems can fail dramatically and throw entire elections into chaos. After Ecuador's internet voting system failed during August's presidential election, the country switched to in-person voting only.¹² The failure of Australia's online voting

⁹ See generally U.S. Election Assistance Commission, *Election administration and Voting Survey 2020 Comprehensive Report* (2020),

https://www.eac.gov/sites/default/files/document_library/files/2020_EAVS_Report_Final_508c.pdf.

¹⁰ U.S. Election Assistance Commission, *Studies and Reports* (Oct. 19, 2023),

<https://www.eac.gov/research-and-data/studies-and-reports> (follow EAVS Datasets Version 1.0 (released June 29, 2023) hyperlink).

¹¹ See e.g., Federal Voting Assistance Program, *2022 Election Outreach Toolkit For Election Offices Serving UOCAVA Voters* (2022),

[https://www.fvap.gov/uploads/FVAP/Outreach-Materials/OutreachToolkit_EO_2022-\(1\).pdf](https://www.fvap.gov/uploads/FVAP/Outreach-Materials/OutreachToolkit_EO_2022-(1).pdf).

¹² *Foreign Ministry must rent 59 premises abroad so that 390,000 migrants can vote*, *Ecuador Times* (Sept. 13, 2023),

<https://www.ecuadortimes.net/foreign-ministry-must-rent-59-premises-abroad-so-that-390000-migrants-can-vote/>.

system in 2021 disenfranchised enough voters that a court ordered three local elections to be re-run¹³—and the system was not used in this year’s elections.¹⁴

We are very interested in working collaboratively and creatively with you to improve voting for military voters in ways that do not create risk to our elections.

We would welcome the opportunity to provide you further information about the technical aspects and unavoidable and severe inherent risks of electronic ballot return. We would also welcome the opportunity to collaborate with you on implementing access improvements that do not present security risks.

At a time when election security and public confidence are under relentless attack, Michigan should not rely on insecure technology for voters that produces unprovable election results. Again, we **urge you to remove the electronic ballot return provisions from House Bill 4210 and reject any other proposal that includes electronic return of voted ballots.**

Respectfully submitted,

Susannah Goodman
Director of Election Security
Common Cause

Quentin Turner
Michigan Executive Director
Common Cause

Susan Greenhalgh
Senior Advisor on Election Security
Free Speech for People

¹³ Ainslie Drewitt-Smith & Tim Fernandez, *Supreme Court orders re-vote after iVote crash in NSW local government elections*, Australian Broadcasting Corporation Illawarra (Mar. 16, 2022; updated Mar. 17, 2022), <https://www.abc.net.au/news/2022-03-17/ivote-revote-ordered-supreme-court-judgement/100917050>.

¹⁴ Narelle Miragliotta & Sarah Murray, *iVote, the 2021 NSW Government Elections and the Future of Internet Voting*, *Australian Public Law* (June 1, 2022), <https://www.auspublaw.org/blog/2022/06/ivote-the-2021-nsw-government-elections-and-the-future-of-internet-voting>.

Aquene Freechild
Co-Director, Democracy Campaign
Public Citizen

Pamela Smith
President & CEO
Verified Voting