Verified Voting

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

EPI Center | AAAS
CENTER FOR SCIENTIFIC EVIDENCE IN PUBLIC ISSUES

acm U.S. Technology Policy Committee

April 17, 2023

By Electronic Mail

Hon. Jocelyn Benson, Secretary of State
State of Michigan
Richard H. Austin Building
430 W. Allegan St. - 4th Floor
Lansing, MI 48918

Re: The Continued Inherent Insecurity of Internet Voting

Dear Secretary Benson:

We are writing from the American Association for the Advancement of Science's (AAAS) Center for Scientific Evidence in Public Issues and the U.S. Technology Policy Committee of the Association for Computing Machinery (USTPC) regarding the Michigan legislature's consideration of authorizing insecure internet voting. AAAS, the world's largest multidisciplinary scientific society, and ACM, the world's largest computing society, work apolitically to promote the responsible use of science and technology in public policy.

As the legislature considers the issue, we write to caution unequivocally that ***internet voting*** – referring primarily to the electronic return of a marked ballot via email, fax, web-based portal, or mobile apps – ***is not a secure solution for voting in Michigan or elsewhere in any form, nor will it be in the foreseeable future***. Indeed, those facts have not changed since April of 2020 when we jointly wrote to every governor, secretary of state, and state election director across the country detailing the scientific and technical risks of internet voting and urging officials to refrain from allowing the use of any internet voting system. More than 80 leading organizations, scientists, and security experts also signed that letter, which documents that:

- All internet voting systems and technologies are inherently insecure.
- No technical evidence exists that any internet voting technology is safe or can be made so in the foreseeable future; rather, all research performed to date demonstrates the opposite.
- Blockchain technology cannot mitigate the profound dangers inherent in internet voting.
- No mobile voting app is sufficiently secure to permit its use.

These statements distill the findings of more than two decades of rigorous, science-based analysis.

In 2020, the Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) jointly released additional guidance describing the electronic return of ballots as "high-risk even with controls in place." The guidance explains that "***electronic ballot return, the digital return of a voted ballot by the voter, 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***… 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."

These concerns echo a 2018 consensus study report on election security by the National Academies of Science, Engineering, and Medicine (NASEM), the most definitive and comprehensive report on the scientific evidence behind voting security in the U.S. to date, which stated:

> "***At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots.*** Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as ***no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet***."

Moreover, despite these profound risks, a recent report by MIT researchers concluded that "online voting may have little to no effect on turnout in practice, and it may even increase disenfranchisement."

We share legislators' desire to expand ballot access for all but respectfully submit that Michigan can best demonstrate leadership in election security by committing to scientifically sound election systems that embrace both accessibility and security. As noted in these remote voting recommendations, ***more secure alternatives exist to provide accessible remote voting for overseas uniformed personnel, individuals with disabilities, and others who may have difficulty accessing the ballot***.

We would welcome the opportunity to discuss more secure alternatives to internet voting with you and your colleagues, including accessible remote voting by mail, and to connect you with leading experts on these technologies. To arrange for such briefings, please don't hesitate to contact us directly.

Thank you for your time, consideration, and assistance.

Respectfully submitted,

Michael D. Fernandez, Director
Center for Scientific Evidence in Public Issues
American Association for the
Advancement of Science
1200 New York Avenue, NW
Washington, DC 20005
202-326-7056
mdfernandez@aaas.org

Jeremy J. Epstein, Chair
U.S. Technology Policy Committee
Association for Computing Machinery
1701 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006
202-580-6555
acmpo@acm.org

cc: Jonathan Brater, Bureau of Elections Director

INDIVIDUAL ENDORSEMENTS OF AAAS/ACM USTPC LETTER OF APRIL 17, 2023*

Nathaniel S. Borenstein, Ph.D.
Research Faculty
School of Information
University of Michigan

Dallas Card
Assistant Professor
School of Information
University of Michigan

Steven M. Carr
Professor and Chair, Computer Science
Assoc. Dean for Research and Grad. Educ., CEAS
Western Michigan University

Mahdi Cheraghchi
Associate Professor
Computer Science and Engineering
University of Michigan—Ann Arbor

Scott Dexter
Professor
Computer Science
Alma College

Tawanna Dillahunt, Ph.D.
Associate Professor
School of Information
University of Michigan - Ann Arbor

Ron Eglash
Professor
School of Information
University of Michigan - Ann Arbor

Roya Ensafi
Morris Wellman Asst. Prof. of Computer Science
University of Michigan - Ann Arbor

Birhanu Eshete
Assistant Professor
Computer Science
University of Michigan - Dearborn

Ajay Gupta
Professor
Computer Science
Western Michigan

Yuri Gurevich
Prof. Emeritus
Computer Science & Engineering
University of Michigan - Ann Arbor

J. Alex Halderman
Co-chair
Michigan Secretary of State's
Election Security Advisory Commission
and
Director
Center for Computer Security and Society
Professor, Computer Science and Engineering
University of Michigan - Ann Arbor

John P. Hayes
Professor of Electrical Engineering
and Computer Science
University of Michigan - Ann Arbor

Peter Honeyman
Research Professor, Emeritus
Computer Science & Engineering
University of Michigan - Ann Arbor

H. V. Jagadish
Director
Michigan Institute for Data Science
and
Edgar F Codd Distinguished University Professor
Bernard A Galler Collegiate Professor
of Electrical Engineering and Computer Science
University of Michigan - Ann Arbor

Dr. John Kloosterman
Lecturer
Computer Science
University of Michigan - Ann Arbor

Eric Gilbert
John Derby Evans Associate Professor
School of Information
University of Michigan - Ann Arbor

Benjamin Kuipers
Professor
Computer Science and Engineering
University of Michigan - Ann Arbor

Trevor Mudge
Bredt Family Professor of
Computer Science & Engineering
University of Michigan - Ann Arbor

Luis Ortiz, Ph.D.
Associate Professor
Computer and Information Science
University of Michigan - Dearborn

Chris Peikert
Professor
Computer Science and Engineering
University of Michigan - Ann Arbor

Karem A. Sakallah
Professor
Electrical Engineering and Computer Science
University of Michigan - Ann Arbor

Florian Schaub
Associate Professor of Information and of
Electrical Engineering and Computer Science
University of Michigan - Ann Arbor

Dr. Michael Kowalczyk
Professor
Computer Science
Northern Michigan University

Ben Torralva
Lecturer and Adjunct Research Scientist
Computer & Materials Science and Engineering
University of Michigan - Ann Arbor

Kentaro Toyama
W. K. Kellogg Prof. of Community Information
School of Information
University of Michigan

Dr. Westley Weimer
Professor
Electrical Engineering and Computer Science
University of Michigan - Ann Arbor

Joshua Welch, Ph.D.
Assistant Professor
Computer Science and Engineering
University of Michigan - Ann Arbor

Michael Wellman
Professor and Chair
Computer Science & Engineering
University of Michigan - Ann Arbor

Jeffrey J. Yackley, Ph.D.
Assistant Professor
Information Technology
University of Michigan - Flint

**** NOTE: Affiliations listed above are for identification purposes only and do not imply institutional endorsement.***