Testimony of J. Alex Halderman Regarding H.B. 4210[1]
Before the Michigan House Committee on Elections
May 9, 2023

Contact: jhalderm@umich.edu; https://jhalderm.com

Thanks to Chair Tsernoglou and the entire Committee for the opportunity to submit this testimony.

My name is J. Alex Halderman, and I am professor of computer science and engineering at the University of Michigan in Ann Arbor, where I lead U-M's cybersecurity research group. I have testified to the U.S. Senate and House about election cybersecurity issues, and I was appointed by Secretary Benson to co-chair Michigan's Election Security Advisory Commission, which consisted of local and state election officials from Michigan and nationally leading cybersecurity experts. My full C.V. is available online [1].

HB 4210 is well intentioned, but I am concerned that the bill as written would seriously undermine the security of Michigan's elections. The bedrock of Michigan elections has long been the simple fact that every vote is cast on a piece of paper, which cannot later be changed in a cyberattack. Michigan's paper ballots can be audited or even recounted by hand, resolving any reasonable doubt about whether hacking or computer error could have affected results. Well-audited paper ballots are endorsed by practically every election security expert, and they provide assurance that is easy to explain to skeptical voters.

---

[1] Hearing agenda: https://www.legislature.mi.gov/(S(obtrvy2aldjw4q05ln4ld5tq))/mileg.aspx?page=mcommitteemeeting&objectname=fc7e896f46444806ab6aefaf6b573128&meetingchamber=House
Bill: https://www.legislature.mi.gov/(S(obtrvy2aldjw4q05ln4ld5tq))/mileg.aspx?page=getObject&objectname=2023-HB-4210
Thanks to Braden Crimmins for assistance with the preparation of this testimony.

In contrast to our paper-based system, there is overwhelming scientific consensus that electronic ballot return *cannot* be adequately secured. The National Academies [2], the U.S. Vote Foundation [3], a joint report by CISA, NIST, EAC, and FBI [4], and Michigan's own Election Security Advisory Commision [5] all agree that no existing technology can resolve such systems' inherent vulnerability to digital tampering. Just last year, an expert panel was convened at U.C. Berkeley to develop standards for secure electronic ballot return, in an effort funded by a major proponent of online voting, Tusk Philanthropies. This standards panel disbanded after concluding that securing electronically returned ballots was, at present, impossible [6].

Let me give you an illustration of the risks such a system presents. About a decade ago, Washington, D.C. implemented an online ballot return system for military and overseas voters. Just weeks before Election Day, they held a mock election, during which the public was invited to test the system's security. In just 48 hours, my team at U-M managed to remotely hack into the server and secretly change all the votes [7]. Online ballot return technology has not significantly changed since then—among many other risks, it remains vulnerable to the prospect of invisible vote-stealing attacks from anywhere in the world.

HB 4210 does not simply expand the scope of who is eligible to return ballots online, the bill would remove the most important security protection in the existing statute: the requirement that ballots be digitally signed utilizing the military's Common Access Card system.

I am encouraged that Secretary Benson has instead suggested requiring that voters return an auditable paper ballot along with an electronically transmitted version. Under one such "hybrid" model, the electronic ballot would be escrowed and used only in case the paper

ballot was not delivered in time to be counted. Relying on the electronic ballots would only rarely be necessary because of the new 6-day grace period for overseas voters, which would minimize the amount of electronic tampering possible. Unfortunately, HB 4210 as drafted *does not include* any kind of auditability or paper trail requirements. That's a truly unfortunate omission, as it would leave nothing in the law to ensure that the Secretary or future Secretaries fully implement these essential safeguards.

Under Secretary Benson's administration, Michigan has established itself as a leader in election security. HB 4210 risks jeopardizing that position, and on the eve of a presidential election that will likely place the state again in the national spotlight. I urge you to consult a wider range of scientists and experts before proceeding with this legislation.

To that end, I'd like to direct you to a letter opposing the expansion of electronic ballot return in Michigan, which you received last month from the American Association for the Advancement of Science and the Association for Computing Machinery, two of the leading scientific professional societies. The letter, which I have attached below, was signed by 30 of Michigan's most preeminent computing researchers, including the Chair of Computer Science at U-M. I and these other experts are available to work with you to collaboratively identify policies which can accomplish the laudable goals of HB 4210 without introducing undue risk to Michigan elections.

Some other states are not following the science on the issue of electronic ballot return, but this is no reason for Michigan to do the same. At a time when elections continue to face potential attacks from America's adversaries—and when voter confidence is being undermined for political advantage—Michigan cannot afford to expose our democracy to such grave risks. Thank you.

References:

[1] J. Alex Halderman. CV. jhalderm.com/home/halderman-cv.pdf

[2] National Academies of Sciences, Engineering, and Medicine, “Securing the Vote: Protecting American Democracy.” 2018. https://nap.nationalacademies.org/catalog/25120/securing-the-vote-protecting-american-democracy

[3] U.S. Vote Foundation, “The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study.” 2015. https://www.usvotefoundation.org/E2E-VIV

[4] Cybersecurity and Infrastructure Security Agency (CISA), Election Assistance Commission (EAC), Federal Bureau of Investigation (FBI), and National Institute of Standards and Technology (NIST), “Risk Management for Electronic Ballot Delivery, Marking, and Return.” 2020. https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf

[5] Michigan Election Security Advisory Commission, “Report and Recommendations.” Oct. 2020. https://www.michigan.gov/-/media/Project/Websites/sos/31lawens/ESAC_Report_Recommendations.pdf

[6] Center for Security in Politics, University of California, Berkeley., “Working Group Statement on Developing Standards for Internet Ballot Return.” Dec. 2022. https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement-on-Internet-Ballot-Return.pdf

[7] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. A. Halderman, “Attacking the Washington, D.C., Internet Voting System.” In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security (FC)*, volume 7397 of *Lecture Notes in Computer Science*, pages 114–128. Springer, 2012. https://jhalderm.com/pub/papers/ dcvoting-fc12.pdf

April 20, 2023

By Electronic Mail

Hon. Penelope Tsernoglou, Chair
Hon. Dylan Wegela, Majority Vice Chair
Hon. Rachelle Smit, Minority Vice Chair
House Elections Committee
Anderson House Office Building, Room 327
124 North Capitol Ave
Lansing, MI 48933

Hon. Erin Byrnes
Hon. Jaime Churches
Hon. Jay DeBoyer
Hon. Kara Hope
Hon. Matt Koleszar

Re: Continued Inherent Insecurity of Internet Voting

Dear Chairwoman Tsernoglou, Vice Chairs Wegela and Smit, and Members of the Committee:

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 issue of 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.

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 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: Hon. Joe Tate, Speaker of the House
Hon. Matt Hall, House Minority Leader

INDIVIDUAL ENDORSEMENTS OF AAAS/ACM USTPC LETTER OF APRIL 20, 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

Dr. Michael Kowalczyk
Professor
Computer Science
Northern Michigan University

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

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

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

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

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

Charles Wallace
Associate Professor
Computer Science
Michigan Technological University

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

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

Karem A. Sakallah
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

Florian Schaub
Associate Professor of Information and of
Electrical Engineering and Computer Science
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.*