EPI Center | AAAS
CENTER FOR SCIENTIFIC EVIDENCE IN PUBLIC ISSUES

acm U.S. Technology Policy Committee

April 19, 2021

Re: The insecurity of internet voting

Dear Legislator,

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 Colorado's consideration of an expansion of insecure internet voting.[1]

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 Colorado or elsewhere in any form, nor will it be in the foreseeable future. Last April, we 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. To date, more than 80 leading organizations, scientists, and security experts have signed the letter, which documents that:

- All commercially available internet voting systems and technologies are currently inherently insecure.[2]
- No technical evidence exists that any internet voting technology is safe or can be made so in the foreseeable future[3]; rather, all research performed to date demonstrates the opposite.
- No blockchain technology can mitigate the profound dangers inherent in internet voting.
- No mobile voting app is sufficiently secure to permit its use.

These statements reflect the findings of both recent and two decades of rigorous, science-based analysis. In May 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) released additional guidance describing the electronic return of marked 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…

[1] AAAS, the world's largest multidisciplinary scientific society, and ACM, the world's largest computing society, work to provide a voice for science on societal issues and promote the responsible use of science and technology in public policy.

[2] Certain experimental systems have been used in academic and other intra-organizational elections, but their inventors strongly discourage their use in government elections due to the risks from determined adversaries and threats that cannot be mitigated with known technology.

[3] Some experimental systems have promise for the long-term, but as noted in the previous footnote, their inventors strongly discourage their use in elections of public consequence.

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. 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."

Rather than enhancing security, the 2018 NASEM report described the addition of blockchains to voting systems as "added points of attack for malicious actors." As described in our open letter, analysis of one blockchain voting system revealed vulnerabilities where "information captured from voters exposes them to serious risk of identity theft, and information from overseas military voters risks potentially providing adversaries with intelligence regarding military deployments, endangering the lives of service members and national security." Despite these profound risks, a 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 your desire to expand ballot access for all. Colorado's embrace of vote by mail and risk-limiting audits 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, secure alternatives exist to provide accessible remote voting for overseas uniformed personnel, individuals with disabilities, and others who may have difficulty accessing the ballot.

Of course, some individuals may lack the ability to print their ballots and return them by mail. In these cases, electronic ballot return may be necessary to allow independent ballot access, a fundamental right of Colorado residents. Any implementation of electronic ballot return should adopt the best security practices possible and limit access only to those who absolutely require the option. Unfortunately, even following best practices, increasing the proportion of electronically returned ballots reduces the effectiveness of other election safeguards, such as risk-limiting audits, and increases the threat to election accuracy, security, and validity. Because electronically returned ballots violate essential security principles, such as software independence, you cannot validly audit these ballots. Without proper safeguards limiting the use of electronic ballot return, Colorado elections face significant risk moving forward.

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

Thank you,

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

James A. Hendler, 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