Testimony of Susan Greenhalgh
Senior Advisor on Election Security
Free Speech For People
before the
Colorado General Assembly
State, Civic, Military and Veterans Affairs Committee
Contact: susan@freespeechforpeople.org

Re: SB 21-188- OPPOSE
April 29, 2021

Thank you for the opportunity to submit testimony on SB 21-188.

Free Speech for People is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions and advocacy, secure, transparent, trustworthy, and accessible voting systems for all voters. We oppose systems that permit voting over the Internet because ballots cast over the Internet are at high risk for manipulation or fraud, and degrade trust and security in elections. We urge the Committee to vote NO on SB 21-188.

Proponents of this bill suggest, erroneously, that secure online return of voted ballots is possible with today's computer security tools. This is incorrect. Last year the **Department of Homeland Security, the Federal Bureau of Investigation, the National Institute of Standards and Technology and the U.S. Election Assistance Commission published a risk-assessment[i] which "*recommends paper ballot return, as electronic ballot return technologies are high risk even with controls in place*."[ii]** Emphasis added.] In other words, the Department of Homeland Security recommends states should continue to rely on paper ballots because serious and significant security risks remain that cannot be adequately mitigated with the security tools and controls available, and ballots returned online are at high risk of tampering or manipulation.

Federal and State research has established that online voting is not secure.

Election officials and policy makers may assume that online voting is not offered nationally because there has been no federal effort to develop and deploy online voting broadly but that is inaccurate. Researchers for the federal government have spent a decade and a half and over 100 million dollars to conduct pilot projects and research the security of online voting,[iii] and have concluded that it is currently not possible to ensure the security, privacy, auditability and integrity of ballots cast over the Internet.[iv] Moreover, because federal researchers determined that secure online voting is not currently feasible, the Department of Defense (DoD) cancelled deployment of an online voting system,[v] and, after further research, suspended its effort to develop an online voting system for military voters. The conclusive evidence led Congress to abandon an initiative to develop an online voting service for the military. In 2015 Congress repealed a long-standing provision in the National Defense Authorization Act, ending the federal effort to develop an online voting system.[vi]

The question of how to develop a secure online voting system has been asked and answered by researchers at the federal government. Secure online voting is not yet achievable. Vendors of online voting systems may claim that their systems are secure but these security claims are backed solely by the vendors' promises and are completely unsubstantiated by any independent evaluation. Further, whenever examined, academic research has found significant security vulnerabilities in these systems.[vii],[viii],[ix]

In response to these spurious claims, we have recommended investigations by Attorney General Weiser, into potential false claims and deceptive marketing by the online voting system vendors.[x] ***Any claim by a for-profit vendor that it has developed a secure Internet voting system is in direct contradiction to the best assessment of federal researchers after years of research and analysis.***

The federal government is not alone in its assessment that secure online voting is not presently possible. Utah's Lieutenant Governor has been a proponent of expanding Internet voting in his state, supporting its use for military, overseas, and disabled voters. In 2014 he assembled an advisory committee consisting of legislators, election officials, county clerks, and security and technology experts, to explore extending online voting to all voters in the state. The Lt. Governor's own committee released its report that stated in no uncertain terms that Utah's current practice of online ballot return is not secure.[xi] The report went on to illustrate exactly how unrealistic the challenge of creating a secure online voting system continues to be.

> *"Given that sufficiently secure Internet voting systems do not yet exist, they would need to be built. Of course, some systems, like a stone bridge to the moon, are impossible to build. Others, like a stone bridge to Hawaii, are so exorbitantly expensive as to remain a fool's errand. However, other systems, like spacecraft, aircraft, and the newer Sam White Bridge, are much more affordable. Unfortunately, with the four challenges mentioned in the preceding section, the unconstrained nirvana of Internet voting, "from any device, entirely online," is so impossible, or at least infeasible, as to be a fool's errand*."[xii]

<u>Online voting is not comparable to online banking.</u>

The public may ask, 'I can bank online, why can't I vote online?' But voting involves critical differences that make it a much more difficult enterprise to secure than online banking or commerce.[xiii] Online transactions are not secret or anonymous; a customer can check her statement to detect and address fraudulent charges. But we vote by secret ballot; there is no mechanism for the voter or election official to check to ensure ballots were not manipulated or hacked in transit and that the votes are legitimate. This makes online elections especially vulnerable to <u>undetectable</u> hacking.

And even if an attack was detected, there would be no way for election officials to determine which ballots were manipulated and which are legitimate, making an online attack <u>uncorrectable</u>. Such systems are, by definition, not auditable; since there is no indelible, source record of voter intent, there is no audit record. In addition, banks may calculate an acceptable level of fraud and factor that into the cost of doing business, or take out insurance to cover their losses, but we cannot accept any illegitimate ballots. Finally, the assumption that online banking can be done securely is faulty. It is estimated that banks lose millions or even billions of dollars every year to online attacks.[xiv] High profile hacks like that on Citibank, JP Morgan Chase, and Bank of America prove that even system with high cyber security budgets (much higher than Colorado's), cannot resist determined attackers.

<u>Use of online voting is not evidence that it is secure.</u>

It's true that over two dozen states currently permit online voting, but that does not mean it's secure or trustworthy.

As described above, during the early 2000's, there was a reasonable expectation that the Department of Defense would soon develop and offer a secure online voting system for military voters. Consequently, many states passed laws to permit electronic ballot return, planning to opt into the system provided by the Department of Defense, which never came.

It's important to also understand that most of these states enacted policies to allow online return of voted ballots when cyber crime was much less commonplace and mature. Cyber crime has matured significantly in the last decade, and by all expert accounts, the expertise and sophistication of today's cyber criminals has far out-paced our defenses. We know much more today than we did then, and today's policy decisions should be based on the current threat model.

Estonia

Supporters of online voting often cite Estonia as an example of secure online voting but there are some important caveats and differences to consider. First, the Estonian system cannot correctly be described as "secure" as computer security researchers have identified vulnerabilities in the system that make it susceptible to manipulation and undetectable hacking.[xv] In addition, it is important to note that there is considerable public distrust of the system in Estonia. Public confidence in our election process is essential. We should not be willing to accept a system that cannot be trusted to be legitimate.

Conclusion

We know much more today than we did ten or twenty years ago about the insecurity of systems on the Internet. Twenty years ago, secure Internet voting seemed an attainable goal but today, computer security experts and national security agencies have come the consensus that the secure online return of voted ballots is a much more difficult problem to solve and that the likelihood of a malicious attack is all too real. SB 21-188 would expand the electronic return of voted ballots over the Internet in Colorado, a process that we know now is highly vulnerable to manipulation or tampering. Now is the time to follow the guidance of our national security experts and not expand the electronic return of voted ballots.

We urge the committee to vote NO on SB 21-188.

---

[i] Available at: https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001

[ii] *Ibid*.

[iii] Department of Defense Fiscal Year (FY) 2015 Budget Estimates March 2014, DoD Human Resources Activity *Defense Wide Justification Book Volume 5 of 5 Research, Development, Test & Evaluation, Defense-Wide*

[iv] In 2012 NIST issued a statement which said, "The study concluded that Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems. Malware on voters' personal computers poses a serious threat that could compromise the secrecy or integrity of voters' ballots. And, the United States currently lacks a public infrastructure for secure electronic voter authentication. Therefore, NIST's research results indicate that additional research and development is needed to overcome these challenges before secure Internet voting will be feasible. NIST plans to continue to work with our partners in the public and private sectors on these issues. Available at: http://www.nist.gov/itl/vote/uocava.cfm

[v] Garamone, Jim, "Pentagon decides against Internet voting this year," *Armed Forces Press Services,* Feb. 6, 2004 http://archive.defense.gov/news/newsarticle.aspx?id=27362

[vi] In the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113-291) Congress repealed a directive initiated in 2002 to the Department of Defense directing it to develop an Internet voting demonstration project for military and overseas voters.

[vii] Michael A. Spector, J. Alex Halderman, Security Analysis of the Democracy Live Online Voting System," University of Michigan, June 7, 2020. *Available at: https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf*

[viii] Michael Spector, James Koppel, Daniel Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections," Massachusetts Institute of Technology, February 2020. Available at: https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

[ix] Sunoo Park, et al., "Going From Bad to Worse: Internet Voting to Blockchain Voting," Massachusetts Institute of Technology, November 6, 2020. Available at: https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf

[x] https://freespeechforpeople.org/fsfp-senior-advisor-on-election-security-susan-greenhalgh-issues-statement-on-eac-press-release-disavowing-false-claims-made-by-online-voting-system-vendors/

[xi] iVote Advisory Committee Final Report, Aug. 21, 2015, Utah Lt. Governor Spencer J. Cox. Available at: https://elections.utah.gov/Media/Default/Documents/Report/iVote%20Report%20Final.pdf

[xii] *Ibid.*

[xiii] "If I Can Shop and Bank Online, Why Can't I Vote Online?" *by David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory, member, Verified Voting Foundation Board, Board of Directors, California Voter Foundation https://www.verifiedvoting.org/resources/internet-voting/vote-online/*

[xiv] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[xv] Security Analysis of the Estonian Internet Voting System, Drew Springal, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Maggie MacAlpine, J. Alex Halderman. *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS '14), November 2014 https://estoniaevoting.org/findings/paper/