Verified Voting

June 1, 2023

Nevada State Senate
401 S Carson Street
Carson City, NV
via email

Dear Senators,

On behalf of Verified Voting, I write in opposition to electronic ballot return allowances within Senate Bill 60 as well as the removal of the pre-certification requirement for risk-limiting audits. 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 SB 60 regrettably would expand, and advocate strongly that risk-limiting audits be conducted prior to certification.

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 recommend 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.

- NIST, the federal agency responsible for issuing cybersecurity standards, has also conducted research on ways to enhance accessibility for voters with disabilities. Its 2022

[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.

report, Promoting Access to Voting, did not recommend electronic ballot return, instead concluding, “there remain significant security, privacy, and ballot secrecy challenges.”[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 are very interested in working collaboratively and creatively with you to improve voting accessibility in ways that do not create risk to our elections. We would welcome the opportunity to provide you—or other lawmakers—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 improvements that do not present security risks.

Separately, section 6.3 of the amendment weakens Nevada’s risk-limiting audit (RLA) provisions by removing the requirement for an RLA to take place prior to the certification of election results. This requirement (RLAs occurring pre-certification) was set to take effect at the start of 2024, in time for the next presidential election cycle. RLAs can detect and correct outcome-altering errors in the tabulation of ballots, but only if they take place *prior* to election results being finalized. We recommend that you consider reinstituting this requirement.

At a time when election security and public confidence are under relentless attack, Nevada should neither rely on insecure technology for voters that produces unverifiable election results nor lessen the effectiveness of RLAs. Again, we urge you to reject any proposal that includes electronic return of voted ballots and reinstate the requirement that RLAs be conducted pre-certification.

Respectfully submitted,

C.Jay Coles
Senior Policy & Advocacy Associate

[2] 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), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1273.pdf.

[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.