

To: Assembly Committee on Legislative Operations and Elections

Subj: **Exhibit in Opposition to SB74, Amendments 344 and 785**

Date: May 28, 2025

Dear Assembly Committee on Legislative Operations and Elections:

From 2022 - 2024 I have served as an election worker in Washoe County working full-time from the day prior to Early Voting to the close of election day. We have made extensive accommodations to allow residents to vote but we are exceeding reason and logic here. This bill, which increases the scope of electronic voting, ballot result transfers using the internet, and digital signatures increase the risks of fraud and the lack of confidence in our elections.

Before the 2020 election, the U.S. Postal Service developed and tested an online voting system that used blockchain (a digital database) in an effort to secure ballots. The Postal Service engaged security researchers at the University of Colorado to test the system for security. The researchers found that, not only was it possible to compromise the blockchain to change votes, but that the blockchain actually introduced additional avenues of attack. The researchers confirmed they were able to manipulate votes undetectably.

In 2020, the Department of Homeland Security, the FBI, the National Institute of Standards and Technology and the U.S. Election Assistance Commission published a risk-assessment which "recommends paper ballot return, as electronic ballot return technologies are high risk even with controls in place." In other words, the Department of Homeland Security recommends states should continue to use paper ballots because there are serious and significant security risks introduced with the electronic transmission of marked ballots that cannot be adequately mitigated with the security tools and controls available, and ballots returned online are at high risk of tampering or manipulation. DHS's warning against the use of online voting echoed **bipartisan** recommendations from the U.S. Senate Select Committee on Intelligence, published in response to findings that foreign governments were actively trying to attack U.S. election systems.

Four federal government agencies—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)—have concluded in a 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 recommends paper ballot return.

It’s important to understand that most of these states enacted policies to allow online return of voted ballots when cybercrime was much less commonplace and mature. Cybercrime has advanced significantly, and the expertise and sophistication of today’s cyber criminals has outpaced our defenses. We know much more today than we did then, and today’s policy decisions should be based on the current threat model.

Election security is a matter of the highest U.S. national security, so we would be taking a grave risk to our democracy any time the threat of foreign interference is escalated, as it is now. We must stop the expansion of electronic voting, the use of “digital” signatures and new processes for transmission of electronic data through the internet. We must increase the integrity of our elections and the confidence of our voters.

Please Oppose SB74.

Respectfully,

Nancy Carlson

Election Worker

Reno Retiree