Forrest Senti — Testimony in Support of SB727
Senate Education, Energy, and the Environment Committee
February 25, 1:00 p.m.

Chair and members of the Committee,

My name is Forrest Senti. I've spent my career building secure systems for the United States and working in cybersecurity in both the public and private sector. At the National Cybersecurity Center, I led the first independent security audits of mobile voting technology and have worked in several states on their first uses of this technology. I'm here as a cybersecurity consultant to address the security of what this bill contemplates.

You will likely hear that internet voting is insecure. For email. fax, and unsecured web portal ballot return, that is correct—I would oppose their use. But this bill requires something fundamentally different: end-to-end verifiable cryptography, the same mathematics protecting banking, military communications, and classified systems.

Here is the critical distinction. Traditional electronic systems ask you to *trust* that nothing went wrong. This system asks you to *verify*. Every ballot is encrypted on the voter's device and mathematically provable from submission to final count. If anything is tampered with—by malware, an insider, anyone—the math breaks and the discrepancy is detected. It fails loudly, not silently.

You may hear three specific objections. First, that malware could compromise a voter's phone—but verification happens on a *separate* device, requiring an attacker to compromise both independently. Second, that most voters won't check their ballots—but even a small percentage checking creates a statistical tripwire that makes large-scale undetected fraud mathematically improbable. Third, that there's no dispute resolution—but this bill requires paper records. Decrypted ballots are printed and enter the same audit and recount processes as every other paper ballot.

A lot has changed since 2020 when the federal Cybersecurity and Infrastructure Security Agency and the FBI warned that electronic ballot return is high-risk. That assessment evaluated email, fax, and basic web portals. The next generation mobile voting model is significantly more secure —encrypted, independently verifiable, and auditable. We are excited for an updated federal evaluation.

Mobile voting technology now exists to meet the standards of The National Academy of Sciences for robust security and verifiability. Today, malware and discrepancies are detectable through independent "Ballot Check" protocols and a public verification board.

This new technology meets the highest standard and I welcome skepticism, that's how good security works. I'm happy to answer your questions.