May 14, 2019

Senator Cory Gardner – CO
354 Russell Senate Office Building
Washington, DC 20510

Representative Derek Kilmer – WA
1410 Longworth House Office Building
Washington, DC 20515

Senator Mark Warner – VA
703 Hart Senate Office Building
Washington, DC 20510

Representative Michael McCaul – TX
2001 Rayburn House Office Building
Washington, DC 2051

RE: State Cyber Resiliency Act (H.R. 2130 and S. 1065)

Dear Senators Gardner and Warner and Representatives Kilmer and McCaul,

Thank you for introducing legislation aimed at increasing cybersecurity at the state and local levels of government. We recognize the need for this important legislation, which is aimed at hardening cyber resiliency efforts and preventing vulnerabilities from becoming nightmare realities. For the states that would respond to the proposed grants in H.R. 2130 and S.1065, and for the protection of the citizens who live in them, we applaud your support in the battle against cyberattacks.

At the same time that you are bolstering cybersecurity defenses, we encourage you to add provisions specifically prohibiting these funds from being used for internet-based voting. Cybersecurity experts agree that internet return of marked ballots lacks sufficient safeguards for security and privacy. We urge you to specifically name internet voting as a threat and prohibit the funding provided by your legislation from being used to support internet voting programs and pilots.

Cybersecurity experts agree that no current technology, including blockchain voting, can guarantee the secure, verifiable, and private return of voted ballots over the internet. Both because vote-rigging malware could already be present on the voter's computer and because electronically returned ballots could be intercepted and changed or discarded en route, local elections officials would be unable to verify that the voter's ballot accurately reflects the voter's intent. Furthermore, even if the voter's selections were to arrive intact, the voted ballot could be traceable back to the individual voter, violating voter privacy.

The National Academies of Science, Engineering, and Medicine in 2018 released the report entitled *Securing the Vote: Protecting American Democracy.* Here they give the following recommendation (quoted from the report):

> 5.11 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.

Anyone in the world, including foreign nation states, criminal organizations, or our domestic partisans, can attack any Internet voting system, attempt to change votes, violate privacy, or disrupt the election - possibly in a completely undetectable way. The kinds of attacks that are credible threats and elevate the risk of voting via the internet include the following:

- Voter authentication attacks (i.e. forged voter credentials)
- Malware on voters' devices (e.g., viruses, Trojan horses, malicious code embedded in software updates) that can modify votes undetectably
- Denial of service attacks (slowing some key part of the system to a crawl, or crashing it, either by overwhelming it with traffic or taking advantage of a bug)
- Server penetration attacks (remote break-in and control of the election server)
- Spoofing attacks (directing voters to a fake voting site instead of the real one)
- Widespread privacy violation (by any of several methods, taking advantage of the fact that online voters must transmit their names with their votes)
- Automated vote buying and selling schemes (with cryptocurrency payments, e.g. Bitcoin, in exchange for votes)

More importantly, the security of the device that voters use to cast their votes is unknowable. The device may already be corrupted with malware or viruses that could interfere with ballot transmission or even spread that malware to the computer at the elections office on the receiving end.

Many of the current internet voting programs are designed for overseas military personnel. Verified Voting supports the United States military - our staff members have family members who are currently serving. Because of our respect for those who risk their lives to protect our country, we oppose subjecting our service men and women to a voting system that puts the validity and privacy of their votes at greater risk than their civilian counterparts.

We thank you again for bringing forward the important cybersecurity issues surrounding elections and urge you to specifically name internet voting as a threat and prevent this critical funding from being used to support insecure practices.

Verified Voting is a national, non-profit non-partisan information and advocacy organization focused exclusively on ensuring the security, integrity, and trustworthiness of computerized election technology. Our mission is to strengthen democracy for all voters by promoting the responsible use of technology in elections. We protect the right to vote where voting intersects

technology to ensure that Americans can be confident their votes are cast as intended and counted as cast.

Respectfully submitted,

Marian K. Schneider, President
Verified Voting

The following organizations join us in urging you to add these provisions to H.R. 2130 and S. 1065.