April 2, 2026

The Honorable Scott Weiner
Chair
Senate Elections and Constitutional Amendments Committee
California State Senate
1020 N Street
Room 533
Sacramento, CA 95814

RE: SB 970 – opposing electronic ballot return

Dear Chair Weiner and Committee Members:

Brennan Center for Justice, California Voter Foundation, Free Speech for People, Public Citizen, and Verified Voting are writing in opposition to Senate Bill 970/Cervantes which would ultimately allow electronic return of absentee ballots via the internet for certain voters. Our organizations are committed to working to reduce barriers to voting and to ensuring accessible, resilient, secure elections.

We appreciate and share your commitment to ensuring that all California voters can exercise their right to vote. **However, legislation to allow electronic ballot return, via the language in SB 970, would put voters' ballots at risk and undermine confidence in election results.**

The security risks associated with electronic ballot return are severe, well-documented, and broadly acknowledged by the federal government's top security agencies and the nation's leading cybersecurity experts.

A joint analysis from the Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST), published in 2020, and again in early 2024, classifies electronic ballot return as high risk, capable of enabling attacks that could alter or disrupt election results at scale. As stated in their analysis, "Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and can occur at scale."[1]

Congress shares these concerns. The U.S. Senate Select Committee on Intelligence concluded that no system of online voting has yet established itself as secure and urged states to resist adopting internet voting.[2]

Independent cybersecurity experts mirror these findings. In 2022, a working group of cybersecurity and cryptography experts convened at the University of California, Berkeley to create standards to govern the security of internet voting systems instead concluded that "the current cybersecurity environment and state of technology makes it infeasible . . . to draft responsible standards." The group, chaired by former Department of Homeland Security secretary Janet Napolitano, determined that the technology required to secure online ballot return does not exist today, and that a single attacker could potentially alter thousands or even millions of votes.[3] The group outlined that electronic ballot return also carries multiple unique vulnerabilities, including malware, denial-of-service attacks, spoofing, identity fraud, and breaches that could expose voters' private information.[4] Any one of these could compromise an election; several could do so without detection. **Currently, no federal certification standards exist for electronic ballot return systems.**

As recently as January 16, 2026, a coalition of computer scientists and security researchers issued a statement clarifying that, even with recent technological advances, electronic ballot return technology is still not yet suitable for use in public elections. According to their statement, "it has been the scientific consensus for decades that internet voting is not securable by any known technology. Research on future technologies is certainly worth doing. However, the decades of work on [electronic ballot return] systems has yet to produce any solution, or even any hope of a solution, to the fundamental problems."[5]

For these reasons, we respectfully urge you to reject SB 970, which would ultimately authorize electronic ballot return. Implementing electronic ballot return would run counter to the unified assessment of national security experts, cybersecurity professionals, federal intelligence

---

[1] CISA, EAC, FBI, and NIST, Risk Management for Electronic Ballot Delivery, Marking, and Return, 2020/2024.

[2] SSCI, Russian Active Measures, Vol. 1., 2019

[3] UC Berkeley CSP, Working Group Statement on Internet Ballot Return, 2022.

[4] Ibid.

[5] Appel, Andrew, "Internet Voting Is Insecure and Should Not Be Used in Public Elections - CITP Blog, 2026."

agencies, and leading academic researchers. The risks—to ballot confidentiality, integrity, and public confidence—simply outweigh any potential benefits at this time.

Sincerely,

Lawrence Norden
Vice President
Elections and Government
Brennan Center for Justice

Kim Alexander
President & Founder
California Voter Foundation

Susan Greenhalgh
Senior Advisor on Election Security
Free Speech for People

Aquene Freechild
Co-Director
Democracy Campaign
Public Citizen

C.Jay Coles
Deputy Director of Legislative Affairs
Verified Voting