May 24, 2023

The Honorable Carl E. Heastie
Speaker, New York State Assembly

Assembly Member Latrice Walker, Chair
Assembly Committee on Election Law

Assembly Member Harvey Epstein

Oppose Insecure Electronic Ballot Return

Dear Speaker Heastie, Chair Assemblymember Walker, and Assemblymember Epstein,

Thank you for your work to expand and enhance voting access for New York voters. Our organizations are committed to ensuring that all voters—including those with disabilities and military and overseas voters—can exercise their right to vote.

However, we write to you with grave concerns about S5729 Hoylman-Sigal and A5280 Epstein, as drafted. If passed at this time, this legislation will put the security of New York's elections at high risk for cyber incidents, and undermine public confidence in election results.

The legislation would permit certain classes of voters to return ballots over the internet—a process known as "electronic ballot return." **We urge you, in the strongest possible terms, to oppose this legislation at this time.**

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 recommends paper ballots.[1]

[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_ElectronicBallot_05082020.pdf?mod=article_inline.

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).

This risk assessment was issued to address the fact that state policy makers like yourselves are facing pressure to allow internet voting. At a time where the integrity and veracity of election results are continuously called into question, it would not be prudent 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 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] [5]

---

[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.

[5] V.S.A. § 2538.

The accessibility issues some voters, especially voters with disabilities, face are real. New York has a long way to go in terms of improving access, and we look forward to working with the bill sponsor, advocates and the State Board of Elections to identify workable solutions.

We urge the Legislature to invest resources in examining other methods that will improve access for voters with disabilities, *without returning ballots over the internet*. Technologies are being developed and piloted that may be able to help address these challenges—and their promise is very exciting, but today these technologies are in their infancy.

There are additional steps New York should take to improve voting accessibility that do not create security risks. As noted above, NIST produced a detailed report of recommendations[6] that we urge you to consider, such as:

- ensuring that all elections websites are more accessible and provide practical information such as physical descriptions of each polling place, indicating accessible entrances, exits, public transit, and parking;
- providing election-related information in accessible formats, through a variety of channels including social media, radio, text and phone;
- providing voting education classes for voters with disabilities in collaboration with local disability support agencies;
- including tactile marks, such as punched holes, to guide visually impaired voters where to sign and date their ballot envelopes; and
- establishing a workgroup or task force made up of representatives from voting and disability rights communities to explore and recommend additional accessibility improvements that are secure.

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 accessibility improvements that do not present security risks.

At a time when election security and public confidence are under relentless attack, New York should not rely on insecure technology for voters that produces unprovable election results.

Respectfully submitted,

Susan Lerner
Executive Director
Common Cause New York

---

[6] National Institute of Standards and Technology, *supra* note 2.

John Kaehny
Executive Director
Reinvent Albany