May 13, 2020

Phil Murphy
Governor of New Jersey
225 W State Street
Trenton, JN 08625

Tahesha Way
Secretary of State of New Jersey
P.O. Box 300
Trenton, NJ 08625

Gurbir Singh Grewal
Attorney General of New Jersey
RJ Hughes Justice Complex
25 Market Street, Box 080
Trenton, NJ 08625-0080

Mr. Robert Giles
Director, New Jersey Division of Elections
NJ Division of Elections
P.O. Box 304
Trenton, NJ 08625-0304

Dear Governor Murphy, Attorney General Grewal, Secretary Way, and Director Giles:

We write concerning the use of internet voting options in recent local elections, as well as statements from state officials that this limited implementation will serve as a pilot for potential expanded use in future elections.[1] We agree with the legal conclusions expressed in Professor Penny Venetis's May 7th letter,[2] that the use of internet voting would violate the statewide court order issued in *Gusciora v. Corzine*,[3] and we are aware of new litigation brought by Mercer County Assemblyman Reed Gusciora and New Jersey citizen groups arguing the same. As Judge Feinberg recognized in *Gusciora*, "as long as computers, dedicated to handling election matters, are connected to the Internet, the safety and security of our voting systems are in jeopardy." While we recognize the challenges that the pandemic poses for our democracy and the need to expand voting options to ensure free and safe elections, these expansions should not be done in a way that jeopardizes election security. And the overwhelming consensus among security experts is that no method of internet voting can be conducted in a secure manner at this time. For this reason, we strongly urge you to refrain from any further use of internet or mobile voting systems in 2020.

[1] "New Jersey Announces Accessible Voting is Coming to May Elections," Mobile Voting Project from Tusk Philanthropies, May 4, 2020, https://mobilevoting.org/2020/05/new-jersey-announces-accessible-voting-is-coming-to-may-elections/; Eric Geller, "Coronavirus Boosts Push for Online Voting Despite Security Risks, *Politico*, May 1, 2020, https://www.politico.com/news/2020/05/01/coronavirus-online-voting-229690.
[2] Penny M. Venetis, Letter Re: Enforcing Court Order in *Gusciora et al. v. Corzine et al*., Docket No. MER-L-2691-04, May 7, 2020.
[3] Docket No. MER-L-2691-04.

Judge Feinberg's order was issued ten years ago, but the security vulnerabilities associated with internet-based voting have not disappeared. In recent guidance, 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) warned that "electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots."[4] The guidance further warned that "these risks can ultimately affect the tabulation and results and, can occur at scale."[5] And while the guidance recommends cybersecurity actions for these systems, the federal agencies make clear that "even with these technological considerations, electronic ballot return remains a high-risk activity."[6]

This guidance is wholly in line with the consensus among experts concluding that online voting is not a secure solution at this time, and will not be in the foreseeable future.[7] Scientists and security experts have repeatedly expressed concerns that any internet voting platform would be vulnerable to malware and denial of service attacks that could risk disenfranchisement, violations of voter anonymity and ballot secrecy, and the recording of incorrect voter choices. Moreover, internet voting systems fail to produce a meaningful voter-verified paper record that can be used to ensure the accuracy of election results.

In the midst of this pandemic that has so profoundly re-shaped our elections, we must remember that the election security threats revealed in 2016 persist. American elections remain vulnerable to foreign interference and cyberattacks. Federal intelligence agencies have warned that "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process."[8] And malicious actors have already sought to exploit vulnerabilities that have surfaced during the confusion caused by Covid-19.[9] The use of unproven voting technology only provides more opportunity for disruption.

We appreciate the desire to expand voting options in response to the Covid-19 pandemic However, we encourage you to make decisions based on the scientific evidence available. And that evidence is clear: the use of internet voting systems jeopardizes confidence in the accuracy of elections. We encourage you instead to use methods of voting – such as expansive mail voting and early in-person voting – which have proven to be accessible, safe, and secure. Additionally, New Jersey can provide access to voters with disabilities using options, deployed in other jurisdictions, which provide accommodation without risking the integrity of the election and the voters' ballot. For example, California, a state that has rigorous security standards, has

---

[4] "Risk Management for Electronic Ballot Delivery, Marking, and Return," Cybersecurity and Infrastructure Agency (CISA).
[5] "Risk Management for Electronic Ballot Delivery, Marking, and Return".
[6] "Risk Management for Electronic Ballot Delivery, Marking, and Return".
[7] "Letter to Governors and Secretaries of State on the Insecurity of Online Voting," American Association for the Advancement of Science, April 9, 2020, https://www.aaas.org/programs/epi-center/internet-voting-letter.
[8] "Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections," FBI National Press Office, November 5, 2019, https://www.fbi.gov/news/pressrel/press-releases/joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2020-elections.
[9] "COVID-19 Exploited by Malicious Cyber Actors," Joint Alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC), April 8, 2020, https://www.us-cert.gov/ncas/alerts/aa20-099a.

conditionally certified three systems[10] to provide a remote accessible vote by mail (RAVBM) option.[11] These systems allow voters with disabilities to receive an electronic ballot, download it, mark it offline using their own assistive technologies, print it out and mail it or drop it off. We would be happy to provide further information about how these systems work.

Please let us know if there is any way we can be a resource as you continue to prepare our democracy for the unprecedented challenges ahead.

Respectfully,

Susannah Goodman
Director, Election Security Program
Common Cause

Lawrence Norden
Director, Election Reform Program
Brennan Center for Justice at NYU School of Law

Marian K. Schneider
President
Verified Voting

[10] Democracy Live Secure Select 1.2.2, Five Cedars Group Alternate Format Ballot (AFB) v5.2.1 and Dominion ImageCast Remote 5.2

[11] "Many Voters with Disabilities Can Vote by Mail Privately and Independently," Disability Rights California, January 14, 2020, https://www.disabilityrightsca.org/publications/many-voters-with-disabilities-can-vote-by-mail-privately-and-independently.