February 24, 2023

Oppose Senate Bill 488 and House Bill 645
AN ACT concerning Election Law – Electronic Ballot Return System – Study and Request for Proposals

Dear Legislators:

Thank you for your work to expand and enhance voting access for Maryland voters. We applaud the reforms enacted recently to make voting safe and accessible, including expanding access to mail-in voting, early voting, and voting in correctional facilities throughout the state. We are committed to ensuring that all voters, including those with disabilities and military voters overseas, can exercise their right to vote.

However, we write to you with grave concerns about SB 488 and HB 645 as drafted. If passed at this time, this legislation will put the security of Maryland's election infrastructure at risk and undermine public confidence in election results.

The legislation requires the State Board of Elections to issue a request for proposals for an "electronic ballot return" voting system.

Four federal government agencies have concluded in a recent risk assessment that "electronic ballot return" is "High" risk. 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**." 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).[1]

This risk assessment was issued to address the fact that state policy makers like yourselves are facing pressure to allow internet voting for certain classes of voters.

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

[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*, May 2020, available at https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf?mod=article_inline

[2] Page 48, *Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities*, National Institute of Standards and Technology, March 2022, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1273.pdf

yet established itself as secure."[3]

- Just weeks ago, experts convened by the University of California's Berkeley Center for Security in Policy 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]

Senate Bill 488 and House Bill 645 also propose a study of electronic ballot return systems currently available. The study directions do not instruct the Department of Legislative Services to consider security or to consult the the government agencies charged with protecting our national election infrastructure, i.e. DHS' CISA, the FBI, EAC and NIST. These agencies - especially the FBI and CISA - routinely track the escalating threats to our election infrastructure - both foreign and domestic - and advise election policy makers on how to address these threats. Any study should absolutely include a review of the recommendations of these agencies and a consultation with their personnel. Moreover, a study should review the conclusions of the University of California at Berkeley Working Group, the National Academy of Sciences,[5] and other election security experts. Finally, the study should stand alone and not be linked to a request for proposal.

The accessibility issues some voters, especially voters with print disabilities, face are real. Various programs that help address these challenges are already in use in other jurisdictions, like bringing poll workers and accessible systems to voters who need them. We urge the legislature to invest resources in examining alternative accessible absentee voting methods that will improve access for voters with

---

[3] Report of the Select Committee on Intelligence, *United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1* (2019), available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

[4] R. Michael Alvarez et al., "Working Group Statement on Developing Standards for Internet Ballot Return," University of California, Berkeley Center for Security in Politics, December 14, 2022. Available at https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement-on-Internet-Ballot-Return.pdf

[5] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy*, The National Academies Press (2018), available at https://nap.nationalacademies.org/catalog/25120/securing-the-vote-protecting-american-democracy

disabilities, without returning ballots over the internet. Other 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. No standards have yet been developed that these systems could be certified to. Any new voting system deployed by the State of Maryland should undergo the rigorous testing and certification that Maryland requires for its polling place ballot marking systems.

Furthermore, at a minimum, there are additional steps Maryland should take to improve voting accessibility – which do not create security risks. As noted above, NIST produced a detailed report[6] of recommendations that we urge you to consider, such as:

- ensuring that county elections websites are accessible;
- providing election-related information in accessible formats, through a variety of channels including social media, radio, text and phone;
- providing physical descriptions of each polling place, indicating accessible entrances, exits, public transit, and parking;
- providing voting education classes for voters with disabilities in collaboration with local disability support agencies;
- implementing alternative attestation methods for voters who cannot sign their mail-in ballot oaths;
- including tactile marks, such as punched holes, to guide blind voters where to sign; 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.

Other jurisdictions are innovating solutions to ensure access to all voters. San Francisco County, the State of Arizona, and the State of Vermont offer in-person accessibility assistance in voters' homes – and we would be happy to provide you with more information about those programs.

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

[6] *Promoting Access to Voting*, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1273.pdf

with you on implementing accessibility improvements that do not present security risks.

Respectfully submitted,

Joanne Antoine
Executive Director
Common Cause Maryland

Yanet Amanuel
Public Policy Director
ACLU Maryland

Rebecca Wilson,
CoDirector, SAVE our Votes
Secure, Accessible, Verifiable Elections for Maryland

Lawrence Norden
Director, Elections and Government Program
The Brennan Center for Justice

Susan Greenhalgh
Senior Advisor on Election Security
Free Speech for People

Alexandra Chandler
Policy Advocate
Protect Democracy

Aquene Freechild
Co-Director, Democracy Campaign
Public Citizen

Pamela Smith
President
Verified Voting