Common Cause
Maryland
Holding Power Accountable

121 Cathedral Street
Annapolis, MD 21401
443.906.0442
www.commoncause.org/md

February 23, 2026

The Honorable Melissa Wells
Chair
Government, Labor, and Elections Committee
Maryland House of Delegates
145 Lowe House Office Building
Annapolis, Maryland 21401
Via email

Re: House Bill 1066 - Oppose

Dear Chair Wells and Committee Members,

On behalf of Common Cause Maryland, I am writing in opposition to House Bill 1066 which would allow ballot return via the internet for certain voters. Common Cause's mission is to uphold the core values of American democracy by creating an open, honest, and accountable government that serves the public interest, promotes equal rights, opportunity, and representation for all, and empowers people to make their voices heard in the political process. We are a nonprofit, nonpartisan membership organization with approximately 18,920 members in the state of Maryland.

Thank you for your work to expand and enhance voting access for Maryland voters and especially voters with disabilities. We share your commitment to ensuring that all voters, including those with disabilities can exercise their right to vote. However, legislation to allow electronic ballot return, via the passage of House Bill 1066 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. At present, no known technology can secure ballots returned over the internet.

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) classifies electronic ballot return as high risk, capable of enabling attacks that could alter or disrupt election results at scale. As stated in the 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]

Other agencies have been equally clear. The Department of Defense has stated that it does not advocate transmitting cast ballots electronically under any method.[2] The Department of Homeland Security has likewise advised that online voting is not recommended at any level of government at this time.[3]

[1] CISA, EAC, FBI, and NIST, Risk Management for Electronic Ballot Delivery, Marking, and Return, 2020/2024.
[2] DOD statement quoted in Greg Gordon, McClatchy, April 16, 2015.
[3] DHS statement quoted in Sarah Horwitz, Washington Post, May 17, 2016.

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.[4]

Independent cybersecurity experts mirror these findings. A working group convened by the University of California, Berkeley—including pioneers in cryptography and election security—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.[5] The group further emphasized that online voting lacks the basic safeguards present in other online transactions, because the secret ballot prevents voters from verifying that their vote was received and counted as cast. Currently, no certification standards exist for electronic ballot return systems.

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.[6] Any one of these could compromise an election; several could do so without detection.

Recently, a group of computer scientists and security researchers reaffirmed that while electronic ballot return methodologies continue to be researched, it is still not yet suitable for use in public elections. According to this group, "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."[7]

For these reasons, we respectfully urge you to reject House Bill 1066 which would allow electronic ballot return for certain voters. Implementing electronic ballot return would run counter to the unified assessment of national security experts, cybersecurity professionals, federal intelligence agencies, and leading academic researchers. The risks—to ballot confidentiality, integrity, and public confidence—simply outweigh any potential benefits at this time.

We appreciate your leadership and your commitment to ensuring both accessibility and security in our elections.

Sincerely

Susannah Goodman
Director
Election Security Program
Common Cause

[4] SSCI, Russian Active Measures, Vol. 1.

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

[6] Ibid.

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