



December 20, 2022

To the Members of the District of Columbia Council,

In February 2022, eight D.C. Councilmembers introduced a [bill](#) that would require the District of Columbia to implement, by 2024, a system enabling all D.C. voters to vote online. This change would harm voting rights in D.C., end the District's ability to have secure and verifiable elections, and undermine the perception of D.C.'s ability to self-govern.

No bill that would enable online voting — specifically, the electronic return of voted ballots — should be considered until election experts agree that such a system would be both secure and reliable for D.C. voters.

[Recent elections](#) in the Australian state of New South Wales illustrate the danger of internet voting. Their iVote system was unavailable for a substantial portion of the voting period, disenfranchising thousands of voters. The outcome of potentially dozens of races was called into question; a judge [ordered](#) three races to be rerun. In response to this disastrous failure, New South Wales [decided to discontinue](#) using iVote for now.

Multiple American jurisdictions have piloted various forms of internet voting software for small groups of voters. Upon investigation by security experts, the software used in those elections has repeatedly been found to be [riddled with vulnerabilities](#) that allow attackers to alter or delete votes. Even worse, these attacks could be undetectable to the voter or to election officials administering the election.

There is a reason that universal internet voting has not been implemented in any U.S. state: The election security community is in agreement that internet voting is woefully insecure. A [2018 consensus report](#) carried out by the National Academies of Sciences, Engineering, and Medicine concluded that the internet “should not be used for the return of marked ballots until and unless very robust guarantees of security and verifiability are developed and in place.” In May 2020, the Federal Bureau of Investigation, the Election Assistance Commission, the National Institute of Standards and Technology, and the Cybersecurity and Infrastructure Security Agency [warned](#) that electronic ballot return is “high risk,” stating that “securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time”.

D.C. has experimented with internet voting before, wisely inviting security researchers to test the systems in a mock election with online voting. [Within 48 hours](#), a University of Michigan team was able to hack the system such that they could change every recorded vote, reveal every secret ballot, access server room security cameras and login credentials, and more. Election officials did not even notice the intrusion for two business days.

If an online voting system were to be implemented and hacked, we fear that it would undermine perceptions of D.C.'s ability to self-govern.

We all believe that it should be as easy to vote as possible in the District. Many of us work to protect and expand voting rights daily. But internet voting is the wrong way to increase access.

There are other, more secure ways to improve access to voting. In fact, D.C. has already taken many laudable steps to increase access, including the Council's passage of the [Elections Modernization Amendment Act](#) and the [Local Resident Voting Rights Amendment Act](#). To boost voter access and turnout, D.C. might also consider, during the early voting period, bringing ballot marking devices to voters who are unable to handle paper.

[The Intercept](#) has published an article explaining the multiple issues internet voting would raise in D.C. In order to uphold voting rights for District residents, including the right to a secure and meaningful vote, we urge you not to enable internet voting until there is widespread agreement that the system is secure.

Sincerely,
Public Citizen
Center for Democracy & Technology

ACLU of the District of Columbia
Brennan Center for Justice
Common Cause
Free Speech For People
League of Women Voters DC
National Election Defense Coalition
NETWORK Lobby for Catholic Social Justice
OSET Institute, Inc.
Secure Elections Network
Sierra Club DC Chapter
TrustTheVote® Project
United Food and Commercial Workers Local 400
Verified Voting