CONSENSUS STUDIES EXAMINING INTERNET VOTING

Internet voting has been assessed many times and always comes up short. Below we highlight notable studies. More studies—including those of some systems currently being marketed—are available at verifiedvoting.org/internet-voting-resources/.

Securing the Vote: Protecting American Democracy (2018)

National Academies of Sciences, Engineering, and Medicine

In its 2018 consensus report, *Securing the Vote: Protecting American Democracy,* the National Academies of Sciences, Engineering, and Medicine stated bluntly:

At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.[1]

Report of the Select Committee on Intelligence on Russian Interference (2019)

U.S. Senate Select Committee on Intelligence

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."[2]

---

1 National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* 9, 106 (2018), available at https://verifiedvoting.org/wp-content/uploads/2020/07/National-Academy-Report-_Securing-the-Vote-Protecting-American-Democracy_.pdf.

2 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.

Risk Management for Electronic Ballot Delivery, Marking, and Return (2020/2024)

CISA, EAC, FBI & NIST

Four federal government agencies—the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST)—concluded in a risk assessment ahead of the 2020 election 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 recommend paper ballots.[3]

Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities (2022)

National Institute of Standards and Technology

NIST, the federal agency responsible for issuing cybersecurity standards, conducted research on ways to enhance accessibility for voters with disabilities. In its 2022 report, *Promoting Access to Voting*, NIST did not recommend electronic ballot return, instead concluding, "there remain significant security, privacy, and ballot secrecy challenges."[4]

Working Group Statement on Developing Standards for Internet Ballot Return (2022)

University of California, Berkeley Center for Security in Politics

In late 2022, a blue ribbon panel convened by the University of California, Berkeley's 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."[5]

---

3 U.S. Cybersecurity and Infrastructure Security Agency, U.S. Election Assistance Commission, Federal Bureau of Investigation & National Institute of Standards and Technology, *Risk Management for Electronic Ballot Delivery, Marking, and Return* 1 (2020), available at https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf.

4 National Institute of Standards and Technology, *Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities* 48 (2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1273.pdf.

5 Michael Alvarez et al., University of California, Berkeley Center for Security in Politics, *Working Group Statement on Developing Standards for Internet Ballot Return* 10 (2022), https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement on-Internet-Ballot-Return.pdf. The working group was funded by Tusk Philanthropies, which campaigns for every American to be able to vote on their mobile phone.