Verified Voting

February 6, 2024

New Hampshire House of Representatives
Election Law Committee
Concord, NH 03301

RE: Verified Voting Urges Rejection of House Bill 1133

Dear Chairman Berry and Committee Members,

On behalf of Verified Voting, I write in opposition to House Bill 1133, which would allow electronic return of voted ballots. Verified Voting is a nonpartisan nonprofit organization whose mission is to strengthen democracy for all voters by promoting the responsible use of technology in elections. Since our founding in 2004 by computer scientists, we have acted on the belief that the integrity and strength of our democracy rely on citizens' trust that each vote is counted as cast. With this in mind we oppose allowing voted ballots to be returned electronically through insecure means.

Four federal government agencies have concluded in a recent risk assessment 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 recommends paper ballots.[1] 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). **This guidance is still in effect as it has not been rescinded.**

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.

To illustrate just how dangerous electronic ballot return can be, **Microsoft discovered a Chinese cyber-espionage campaign that enabled the attackers to gain access to customer email accounts in 2023. This included employees in the US State and Commerce Departments and other US government agencies.**[2] The proposed legislation would specifically allow email return as the option to return the voted ballots. Clearly, email is not a secure option (no electronic ballot return option is secure). Just last week FBI Director Christopher Wray warned a Congressional Committee that Chinese hackers are preparing to, "*wreak havoc and cause real-world harm*" in the United States.

[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 1 (2020), available at https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf?mod=article_inline.

[2] See https://www.infosecurity-magazine.com/news/chinese-threat-group-us-government/

While this policy of electronic ballot return has been studied for the last 20+ years and the results are always the same, that electronic ballot return in any form is high risk, here are two highlights from recent studies:

- The University of California Berkeley's Center for Security in Politics hosted a Working Group in 2022 to determine the feasibility of technical and implementation standards that would enable safe and secure digital remote ballot marking and return of these ballots. Among the group's conclusions: "The Working Group concludes that the current cybersecurity environment and state of technology make it infeasible for the Working Group to draft responsible standards to support the use of internet ballot return in U.S. public elections at this time."[3]
- In our recent report, *Casting Votes Safely: Examining Internet Voting's Dangers and Highlighting Safer Alternatives*, Verified Voting highlights safer, more secure alternatives to electronic ballot return. From the report: "Missing the ballot return deadline has been the most common reason for ballot rejection among military and overseas voters in every presidential election since at least 2008. Although overseas military voters can use free expedited mail return and many states accept late-arriving ballots from military voters as long as they are postmarked by Election Day, some states still require ballots to be received on or before Election Day. States not currently doing so should consider counting military ballots postmarked by Election Day and received up to seven days after, which would give election officials in most states enough time to count our troops' ballots before certification."[4]

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.

At a time when election security and public confidence are under relentless attack, New Hampshire should not rely on insecure technology for voters that produces unprovable election results. Again, we urge you to vote "no" on HB 1133 and reject any other proposal that includes electronic return of voted ballots.

Respectfully submitted,

C.Jay Coles
Senior Government Relations Associate

[3] University of California, Berkeley study from the Center for Security in Politics (December 2022), available at https://csp.berkeley.edu/wp-content/uploads/2022/12/Working-Group-Statement-on-Internet-Ballot-Return.pdf

[4] Verified Voting: Casting Votes Safely: Examining Internet Voting's Dangers and Highlighting Safer Alternatives (October 2023), available at https://verifiedvoting.org/publication/casting-votes-safely-oct-2023/