

November 22, 2021

National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899
Via electronic submission

RE: NIST-2021-0005 Draft Report on Promoting Access to Voting

On behalf of Verified Voting, I submit these comments in response to the request for comments on the Draft NIST Special Publication 1273 regarding promoting access to voting. Verified Voting is a nonpartisan nonprofit organization with a mission 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. Election technology and practices must support equitable participation and justified public confidence.

Draft NIST Special Publication 1273 identifies barriers experienced by voters with disabilities to vote independently and privately and proposes recommendations to address these barriers. This work is important for voters, and Verified Voting appreciated the opportunity to reply to the June 2021 Request for Information. The draft publication is aligned with many suggestions that Verified Voting made in its earlier comments,¹ notably on ensuring compliance with federal law on polling place access, providing remote accessible vote-by-mail and go-to-voter services, and protecting voter rights when implementing signature match technology and procedures. We strongly support methods of voting that are accessible in practice, not only in principle.

We support a number of the draft publication's recommendations, including that further efforts should be made to research and integrate existing technology into voting processes (p. 19). We also agree with the recommendation that ballots produced by ballot marking devices should be readable by tabulators, which would protect voters and reduce burdens on election officials (p. 40).

Our main focus in these comments is to promote clarity about the dangers of electronic ballot return. Verified Voting believes that voters with disabilities have the

¹ Available at: <https://verifiedvoting.org/comments-nist-2021-0003/>

same right as all voters to a secret ballot and should have the same assurance that their votes are counted as cast. Accessible solutions that transmit votes over the internet compromise the secrecy of the ballot. Currently available systems that allow for electronic ballot return are unable to provide the security that voters with disabilities, like all voters, deserve. Analysis of electronic ballot return should squarely face these threats. Our additional comments and proposed changes are included below.

Ballot secrecy

Maintaining secrecy of the cast ballot is one of the challenges for voters with disabilities. All voters—including voters with disabilities—deserve ballot secrecy, as defined in VVSG 2.0. The VVSG 2.0 defines ballot secrecy in Principle 10.2: "The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices or selections."²

The draft publication should acknowledge the risk to ballot secrecy from electronic ballot return. States that include electronic return of voted ballots (e.g., by email, fax or mobile phone app) compromise ballot secrecy. As explained in *The Secret Ballot at Risk*, "because of current technological limitations, and the unique challenges of running public elections, it is impossible to maintain separation of voters' identities from their votes when Internet voting is used."³ It is not only the election official who may have access to information on the voter and associated ballot, but the electronic systems themselves, representing a more serious breach of ballot secrecy.

The purpose of ballot secrecy is to allow voters to freely participate without coercion or undue influence over how they vote. The risk of allowing voters to waive the right to a secret ballot—a waiver often required for voters to access systems employing electronic return—is that it not only compromises an individual right to a secret ballot but undermines the integrity of the election as a whole. Remote Accessible Vote By Mail (RAVBM) implementations that use server-side ballot marking also threaten ballot secrecy.

² U.S. Election Assistance Commission (2021) Voluntary Voting System Guidelines 2.0, EAC (Washington, D.C.)

³ Fitzgerald, Caitriona, Pamela Smith, and Susannah Goodman. "The Secret Ballot At Risk: Recommendations for Protecting Democracy," August 18, 2016. <https://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf>.

As of 2016, 44 states had a constitutional obligation to protect the secrecy of the ballot.⁴ Of the five major US territories, three mention ballot secrecy in their constitutions.⁵

Proposed changes:

- **p. 7, Lines 277-281:** Add text: **“Online and electronic alternatives often are inadequate. Not all voters with disabilities have access to broadband, internet, or computers. For example, only 72% of adults with disabilities have a smartphone compared to 88% of those without disabilities. Some states have attempted to provide accessibility through email or fax return of voted ballots, but these methods compromise the secrecy of the ballot. Election officials may lack resources to provide additional accessible alternatives to voters with disabilities who cannot use online or electronic options even when they are accessible and secure.”**
- **p. 32, Lines 1054-55:** Revise text: **“Even when voters with disabilities can privately and independently read and mark their ballot, they may face challenges in returning that could prevent their vote from being counted or compromise ballot secrecy.”**
- **p. 33, Line 1099:** Add text: **“RAVBM implementations that transmit votes over the internet (server-side ballot marking) endanger ballot secrecy.”**
- **p. 46, Lines 1480-2:** Add text: **“This may include procedures for poll worker staffing, set-up and signage, and protecting voters’ independence and privacy while casting their ballot curbside, as well as protecting the secrecy of the cast ballot.”**
- **p. 46, Line 1485:** Add text: **“This technology should also include privacy for the voter to cast their vote and secrecy of the ballot after casting.”**

Electronic ballot return

According to the National Academies of Science, Engineering and Medicine, “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

⁴ “The Secret Ballot At Risk,” p. 2. <https://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf>.

⁵ American Samoa: <https://new.asbar.org/revised-constitution-of-american-samoa/#sec016>, Northern Mariana Islands: <https://cnmilaw.org/cons.php#gsc.tab=0>, Puerto Rico: <https://welcome.topuertorico.org/constitu.shtml>.

developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.”⁶

Currently practiced methods of electronic ballot return can guarantee neither the accuracy nor the secrecy of the ballot. In case of disputed outcomes, ballots returned over the internet cannot serve as reliable evidence of voter intent, as voters cannot verify the information that reaches the election agency via email, fax, smartphone, internet or any other exposed network.⁷ In particular, none of the methods currently in use provides the necessary software independence (see Section 5.2 of the report).

Proposed changes:

- **p. 22, Lines 754-8:**
Replace "Developing accessible and secure methods for future voting. Future research should explore how to continue to securely integrate next generation technology into the voting process. For example, electronic ballot return would overcome many barriers faced by voters with disabilities. However, it is vital that research on security continue as electronic ballot return systems are being implemented."

With: "Developing security standards for innovations in accessible voting systems. For example, electronic ballot return would overcome many barriers faced by voters with disabilities, but currently proposed and deployed systems have not been shown to provide the security that voters with disabilities—like all voters—deserve; nor can these systems be guaranteed to protect ballot secrecy."

- **p. 33, Lines 1105-7:** Revise as follows: "Although electronic return methods currently exist, **they present severe security risks and cannot guarantee ballot secrecy. Voters who are invited to waive ballot secrecy to use electronic return may be unaware of the dangers to their own ballots and the integrity of the election.**"
- **p. 34, Line 1110:** The second bullet in the summary box should be revised as follows to match the text of the recommendations on p. 35, lines 1142-3: "Expand electronic options for requesting[~~[,]~~] and marking[~~[, and returning]~~] blank ballots when facilitating voting by mail."

⁶ National Academies of Sciences, Engineering, and Medicine. "Securing the Vote: Protecting American Democracy." Washington, D.C.: National Academies Press, 2018. <https://doi.org/10.17226/25120>

⁷ "Securing the Vote: Protecting American Democracy," especially Recommendation 5.11. <https://doi.org/10.17226/25120>

- **p. 35, Line 1154:** We recommend omitting the entire line regarding research on electronic ballot return, as the point is made elsewhere and is irrelevant to a recommendation related to requesting and marking blank ballots.

Security and accessibility

Voting systems need both security and accessibility. Failure on either score disenfranchises voters. The fourth of the five Systemic Barriers is framed differently than the rest and provides an incomplete view of the problem.

Proposed changes:

- **p. 5, Line 218, bullet 4 and p. 9, Line 331:** Replace "Design of security solutions may not consider accessibility" with "Limitations of current technology in providing usable, secure options for voters with disabilities."
- **p. 9, Lines 332-5:** Replace paragraph as follows: "Current election technology generally falls short in either usability or security for voters with disabilities—and often in both. For example, the use of hand-marked paper ballots and electronic ballot markers to address security needs often creates barriers to voting, especially for voters with print disabilities[footnote] (see Sec. 2.1.3). Contrariwise, voting systems that eschew voter-verified paper ballots for usability reasons create untenable security risks because the results cannot be meaningfully recounted. Efforts to design voting systems that excel in both usability and accessibility are still nascent and require greater priority."

Other comments and suggested changes:

- **p. 8, Lines 314-6:** Many paper-based systems are made accessible to varying degrees, although improvements to such systems must continue to be developed. The statement "the use of paper ... excludes some voters" from voting privately and independently is overly strong. Proposed changes: "The use of paper in many aspects of voting **can create challenges** for some voters with disabilities—especially those with manual dexterity or who are blind or low vision—to privately and independently **participate** in the voting process."
- **p. 9, Lines 327-329:** Again, to say that "the use of paper is the barrier"—implying that the paper itself must be removed regardless of the dangers of doing so—is too broad. Replace this short paragraph with the following: "For many aspects of elections—including registration and blank ballot transmission—paper is unnecessary and accessible alternatives should be provided. Where paper is necessary, it is up to the states to ensure there are accessible methods for handling the paper so that equal opportunity to voters with disabilities is provided, consistent with the law."

- **p. 14, Lines 500-1:** This passage conflates marking and casting ballots, and confusingly poses an apparent choice between using “paper” or “an accessible voting machine.” Revise text: “Voters should have the option to **hand-mark their ballot or to use an accessible ballot marking device.**”
- **p. 40, Lines 1300-1:** All voters—including voters with disabilities—need to have an opportunity to verify the document to be used for tabulation and counting. Add bolded text: “Ensure that the paper output of an accessible voting machine can be **directly verified by the voter**, tabulated, and counted.”
- **p. 40, Lines 1303-5:** According to the NIST Terminology Election Glossary, a “ballot” is a “presentation of the contest options for a particular voter.”⁸ Such a “ballot” is *not* what is counted. The point here is that the voter should be able to verify the document that will be counted. Revise text: “Develop accessible and secure methods for voters with disabilities to mark and verify their **contest option votes**. Technology should continue to be developed and used to support voters with disabilities in independently marking and verifying the **votes** they cast....”
- **p. 41, Lines 1307-9:** Methods that are accessible in theory but are not used in practice are not truly accessible. Revise text: “Research and development of secure and accessible **vote verification methods**[[~~of ballots~~]], **as well as usability and adoption rates**, should be done for paper-based (e.g., BMDs) and paperless (e.g., end-to-end verifiable voting systems) systems.”
- **p. 41, Lines 1318-9:** Effective election verification in this context depends not only on the availability of verification procedures but on their rate of uptake.⁹ Revise text: “ensuring these processes work for, are clear to, **and are sufficiently widely used by voters with disabilities.**”

Respectfully submitted,

Mark Lindeman, Ph.D.
Director

⁸ NIST SP 1500-10x NIST Election Glossary Draft Version 1.0,
<https://pages.nist.gov/ElectionGlossary/#ballot>

⁹ Bernhard, Matthew, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, J. Alex Halderman. “Can Voters Detect Malicious Manipulation of Ballot Marking Devices?” 2020 IEEE Symposium on Security and Privacy (SP), 2020 May 18 (pp. 679-694). IEEE.