



November 22, 2021

Submitted Electronically

Dr. James Olthoff, Director
U.S. Department of Commerce
National Institute of Standards and Technology
Washington, DC

Re: Comments of the ACM U.S. Technology Policy Committee
on NIST Special Publication 1273 (NIST-2021-0005-0001)

Dear Under Secretary Olthoff:

The U.S. Technology Policy Committee (USTPC) of the Association for Computing Machinery (ACM) appreciates this opportunity to respond to NIST's October 21 call for comments on Draft Special Publication 1273: *Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities* (86 FR 58255). USTPC's specific suggestions for changes to broaden, clarify, and strengthen the Report are detailed in the attached Appendix* and address three sets of issues: internet return of voted ballots; other election security issues; and general accessibility matters.

While we trust that the Appendix's granular analysis will be clear, USTPC wishes to again underscore prominently here a key observation last shared with NIST in our July 16, 2021 comments on its RFI Regarding Promoting Access to Voting. Specifically:

[A]t this writing all internet-connected voting technologies and systems which return an electronic or digital ballot remain insecure. Because all voters, no matter what physical or geographical challenges they face, are legally and morally owed a highly secure and private way to cast their ballots, internet-facilitated voting cannot fairly be said to provide meaningful access to the ballot at all. [S]uch technologies thus must not be relied upon to assure the voting rights of disabled and distant voters unless and until they are transparently, independently, and conclusively proven safe.

(See: <https://www.acm.org/binaries/content/assets/public-policy/ustpc-nist-comments-voting-access.pdf>).**

* USTPC's detailed comments were prepared by a working group co-chaired by Andrew Appel and Douglas Jones. It also included USTPC Chair Jeremy Epstein, Vice Chair Alec Yasinsac, and Committee members Thomas Chen, Juan Gilbert, Lorraine Kisselburgh and Barbara Simons.

** NIST also may find helpful [USTPC's Statement on Accessibility, Usability, and Digital Inclusiveness](https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_accessibility.pdf), ACM U.S. Public Policy Council (2017) [https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_accessibility.pdf]

We reiterate this point so recently made because Draft Report 1273 appears in a number of instances addressed in the Appendix (see comments on lines 757, 764, 1105, and 1110) to not fully appreciate that when voting systems that return electronic ballots are network-connected they become subject to attack from any malicious party, anywhere in the world. Accordingly, we strongly recommend changes to the document particularly at those points.

ACM's U.S. Technology Policy Committee continues to believe that robust accessibility at every stage of the voting process is in no way in tension with maximizing voting security. We commend NIST for Draft Report 1273, which contains many positive and useful recommendations that will help enable and empower all those eligible to vote to do so with security, privacy, and dignity.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Alec Yasinsac".

Alec Yasinsac, Vice Chair

Appendix

**“PROMOTING ACCESS TO VOTING” -- DRAFT NIST SPECIAL PUBLICATION 1273
 COMMENTS OF THE U.S. TECHNOLOGY POLICY COMMITTEE OF
 THE ASSOCIATION FOR COMPUTING MACHINERY**

REPORT SEC/PAGE	REPORT LINE	COMMENT (Draft Report text shown in <i>italics</i>)	PROPOSED CHANGE
ISSUE: RETURN OF VOTED BALLOTS BY INTERNET			
2.2.5 / 22	757	<p><i>However, it is vital that research on security continue as electronic ballot return systems are being implemented.</i></p> <p>This puts the cart before the horse. It is well established that no known technology can adequately secure electronic ballot return systems. It is thus inappropriate to <i>implement</i> any electronic ballot return systems before there is a scientific way of reliably securing them.</p>	<p>EDIT the cited sentence to read:</p> <p>"However, as there is no known technology that can adequately secure electronic ballot return, no such system should be implemented unless or before research can demonstrate a means of securing this process."</p>
764		<p><i>"ElectionGuard is an example of a voting technology... [that uses] E2E verifiability. E2E verifiable voting systems are a type of voting system that is software independent and could potentially perform as a paper-based or paperless system."</i></p> <p>Combining these sentences gives the misleading impression that ElectionGuard can be used as a paperless voting system. The cited reference for ElectionGuard (www.electionguard.vote), however, makes no such claim. The lead scientist behind ElectionGuard, Dr. Josh Benaloh, a proponent of research in E2E verifiable voting systems, is also a co-author of the National Academies 2018 report, which concludes that no known technology (including E2E) can adequately secure internet ballot return.</p>	<p>DELETE the two sentences that begin at line 766 with "E2E verifiable voting systems..."</p>

<p>4.1 / 33</p>	<p>1105</p>	<p><i>"Although electronic return methods currently exist, several security challenges and concerns should be addressed when expanding the use of electronic returns to ensure these methods are secure enough to confidently use to vote."</i></p> <p>It is a well-established scientific consensus that "the Internet (or any network connected to the internet) should not be used for the return of marked ballots. . . . [as] no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the internet." [National Academies of Science, Engineering, and Medicine, <i>Securing the Vote: Protecting American Democracy</i>, 2018.] In the three years since that peer-reviewed assessment was published, no technological revolution has changed the fact that "no known technology" can make it safe or secure to return voted ballots electronically. In fact, during that time, one after another after another, deployed e-ballot-return systems have been shown to be insecure. This is unsurprising in light of the National Academies' scientific assessment of the technology's infeasibility.</p> <p>This scientific consensus is the basis for USTPC's 2015 statement in its comments in Docket 210608-0123 that "all internet-connected voting technologies and systems which return an electronic or digital ballot remain insecure.... [I]nternet-facilitated voting cannot fairly be said to provide meaningful access to the ballot at all.... [S]uch technologies thus must not be relied upon to assure the voting rights of disabled and distant voters unless and until they are transparently, independently, and conclusively proven safe."</p>	<p>REVISE this text to read, "No known technology can assure the secrecy, security, and verifiability of electronic ballot return. Although electronic return methods currently exist, all of them are inherently unsecurable. Accordingly, they should not be used in public elections."</p>

	1110	<p><i>"Expand electronic options for requesting, marking, and returning ballots when facilitating voting by mail."</i></p> <p>This sentence misstates the recommendation spelled out in lines 1142-43: "Expand electronic options for requesting and marking blank ballots when facilitating voting by mail," by adding the words "returning ballots" to the actions to be facilitated electronically. USTPC is concerned that a reader simply skimming the Report could miss this subtlety and quote the Report as written to actively recommend electronic ballot return.</p>	<p>CHANGE "requesting, marking, and returning ballots" to "requesting, marking, and returning a printed paper ballot."</p>
4.2 / 34	1145	<p><i>"Provide fully accessible RAVBM."</i></p> <p>According to the scientific consensus, it is possible to electronically download unvoted ballots and mark them on a home computer or other assistive device with adequate security/auditability. Indeed, that's what RAVBM is. However, election administrators would have great difficulty coping with <i>large numbers</i> of RAVBM ballots because they tend to be printed on nonstandard paper (with nonstandard scaling and nonstandard alignment) and they cannot be reliably scanned by conventional optical-scan voting machines. Accordingly, they must be "remade" by local election officials.</p>	<p>EDIT to add the capitalized text as follows: "Provide fully accessible RAVBM FOR VOTERS WITH DISABILITIES."</p>
ISSUE: ADDITIONAL ELECTION SECURITY MATTERS			
4.2 / 36	1185	<p><i>"... using technology to facilitate scanning or automate remaking the ballot."</i></p>	<p>ADD a new bullet point to read: "All voters have the right in a hand recount or audit to have their original ballot mark reviewed. Subjecting the ballots of only certain voters with disabilities to an automated ballot "remaking" process would expose only those voters to the risk that a computer may accidentally or (if manipulated) even "deliberately "misconstrue the voter's mark in the ballot "remaking" process. Therefore, in any hand recount or hand audit of an election, the voter's original ballot paper should be the one counted, not the remade ballot."</p>

5.2 / 40	1292	<p><i>"Encourage the use of all-in-one voting stations."</i></p> <p>Unfortunately, all-in-one voting stations have <i>severe</i> inherent security risks. The computer in such voting stations if hacked, for example, may print votes onto paper different from those cast by the voter, and then deposit the ballot without the voter having had a chance to detect the switch. See <i>Ballot-Marking Devices Cannot Assure the Will of the Voters</i>, by Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark. <i>Election Law Journal</i>, vol. 19 no. 3, pp. 432-450, September 2020.</p>	<p>DELETE lines 1292-1297 entirely.</p>
ISSUE: ACCESSIBILITY CONCERNS AND REMEDIES			
2.1.2 / 8	286	<p><i>"Asking for information in-person. When poll workers and election officials do not have the knowledge or resources to communicate with a voter with a disability (e.g., American Sign Language (ASL)), the voter may be unable to complete parts of the voting process."</i></p> <p>Persons with communication disabilities are not limited to those using ASL. In fact, while 15% of U.S. adults have some trouble hearing, only 0.4% are functionally deaf and likely to be sign language users. The remaining 14+% might require assistance in the form of a text-alternative to voting instructions, a transcription option (real-time transcriber or transcribing tool, or post-session captions), or simply need to converse in a non-noisy location.</p>	<p>ADD the capitalized text as follows: "When poll workers and election officials do not have the knowledge or resources to communicate with a voter with a disability (e.g., American Sign Language (ASL), TRANSCRIBERS, OR TEXT ALTERNATIVES), the voter may be unable to complete parts of the voting process."</p>
2.1.2 /	289	<p><i>Receiving election information and registering to vote. Information is often not provided through accessible communication channels such as ASL interpretation or closed captioning.</i></p>	<p>ADD the capitalized text as follows: "Information is often not provided through accessible communication channels such as ASL interpretation OR closed captioning, OR MAY REQUIRE USE OF A TELEPHONE."</p>

2.1.2 / 8	297	“Information for voters can be inaccessible in several ways . . .”	ADD a new bullet to read: “Voter registration offices often use websites to provide information about voter registration, locations, and assistance, but require phone conversations for non-mainstream information, such as requests for accommodations or questions about registration forms.”
2.1.5 / 10	357	“Extra obstacles encountered by voters with disabilities...” Voters with chronic illnesses and disability may face difficulty walking long distances, standing for long periods of time, or being away from medications and assistive support for more than a short time.	ADD the capitalized text to this bullet as follows: “Long wait times during in-person voting can be particularly burdensome to voters with disabilities who have difficulty standing OR BEING AWAY FROM ASSISTIVE EQUIPMENT for an extended period. IN ADDITION, VOTERS WITH IMMUNODEFICIENCIES FACE SERIOUS HEALTH RISKS WHEN FORCED TO WAIT LONG PERIODS IN CROWDED SETTINGS.”
2.1.5 / 10	363	Districts that provide early or mail-in voting options have varying requirements for eligibility that may provide an option to accommodate some disabilities, but not others, or none at all.	ADD a new bullet to read: “SOME STATES AND DISTRICTS MAY NOT PROVIDE OPTIONS FOR EARLY, ABSENTEE, OR MAIL-IN BALLOTS FOR VOTERS WITH DISABLING CONDITIONS.”
2.2.3 / 14	494-99	See comment regarding Line 363, above.	---
2.2.3 / 15	519-20	“ . . . including nonvisual accessibility for the blind and visually impaired.” This qualifying phrase may erroneously suggest to voters and system designers that it is most important to make voting systems <i>visually</i> accessible. There are additional accessibility needs addressed by the ADA that should or must be considered including dexterity restrictions for marking ballots (with styli or fingers) and auditory restrictions for any audible signals or instructions of systems, etc.	EXPAND this description to broaden the definition beyond accessibility for the visually impaired (as is done in the section following).
2.2.4 / 18	623-24	Vision and mobility disabilities are frequently referenced in the Report, yet 15% of adults have a hearing impairment and face communication challenges during the voting process. Their needs also should be	ADD the capitalized text as follows: “including those with HEARING, intellectual, ...”

		included in the first list of less common (or not as well-known) disabilities to assure that systems designers are aware of and fully address them.	
2.2.5 / 18	654	Research and development... Voter privacy issues often arise when designing and implementing accessible voting solutions. Adding a call for R&D in the area of voter privacy thus would be advisable and important, as well.	ADD the capitalized text to this bullet as follows: "cybersecurity, VOTER PRIVACY, and elections."
2.2.5 / 19	668	See comment regarding Lines 623-24, above.	ADD the capitalized text to the parenthetical list in this bullet as follows: "(e.g., manual dexterity, blind or low vision, OR COMMUNICATION DISABILITIES, etc.)"
2.2.5 / 19	684	<i>"Investigating new communication technology."</i> As noted earlier, ASL interpretation is important but doesn't alone capture the broader interaction technologies used by larger populations.	ADD the capitalized text to this bullet as follows: "Technology that supports alternative interaction styles may include live or remote ASL interpreters OR SPEECH-TO-TEXT TRANSCRIBERS."
4.1 / 31	1023-1025	Excuses for absentee voting . . . NOTE: This is not true in all states. Some specify that only certain types of disabilities (e.g., mobility) are eligible.	---
4.1 / 33	1087	Re: correcting signature issues: If states implement a process to contact a voter <i>by phone</i> to cure missing or mismatched signatures, voters with hearing impairments will be faced with challenges and are likely to be missed and marked as unreachable.	---
6.1 / 43	1361	See comments for Line 357, re: challenges for those with chronic illnesses or weak immune systems.	---

<p>7.1 / 48</p>	<p>1544</p>	<p><i>“Communicating with voters with disabilities who utilize AT or ASL. Some closed-captioning services do not translate well to these communications channels.”</i></p> <p>The language in this recommendation is incomplete and outdated. It does not, for example, address non-ASL voters with hearing disabilities.</p>	<p>REPLACE the current bullet in its entirety with: “Communicating with voters with disabilities who utilize Assistive Technologies or ASL. Some speech-to-text transcribers, for example, require internet access and connectivity, and low-noise environments, leaving voters with weak support.”</p>
------------------------	--------------------	---	---