CENTER FOR
DEMOCRACY
& TECHNOLOGY

June 7, 2023

To: Attn: Testing & Certification
        Election Assistance Commission
        633 3rd Street NW
        Suite 200
        Washington, DC 20001

Re: Request for public comment on Voluntary Voting System Guidelines, EAC-2023-0001

On behalf of the Center for Democracy & Technology (CDT), I submit the following comments in response to the U.S. Election Assistance Commission's (EAC) request for comments as part of its annual review of the Voluntary Voting System Guidelines (VVSG).[1]

CDT is a nonprofit 501(c)(3) organization focused on advancing civil rights and civil liberties in the digital age, including the right to free, fair, secure, and accessible elections. CDT has long supported the EAC's important work,[2] including the much-needed VVSG 2.0 update in 2021.[3] We appreciate the opportunity to participate in the EAC's ongoing work to maintain the VVSG and ensure that voting systems used across the country are accessible and secure.

While the VVSG 2.0 represents a major improvement over VVSG 1.0 and 1.1, there is still room for further progress.

Our comments focus primarily on parts of the VVSG that relate to ballot-marking devices (BMDs), a topic that we have studied in recent years, including in a 2022 report.[4] BMDs are used by millions of Americans in every election; about a quarter of all registered voters live in jurisdictions using BMDs for all voters.[5] BMDs are a crucial technology for ensuring that voters with disabilities are able to vote privately and independently. The EAC must update the VVSG to ensure that votes cast via BMD are not second-class votes. We propose the following edits to the VVSG that will better ensure that VVSG-certified BMDs are usable and accessible, ensure the privacy of voters who use them, and increase the likelihood that voters can and will verify their BMD-printed ballots before casting them.

We propose additional changes to ensure the security, accessibility, and privacy of U.S. election infrastructure.

---

[1] U.S. Election Assistance Commission. (2023, March 9). Voluntary Voting System Guidelines Request for Public Comment. [perma.cc/M7YV-RBK3]
[2] Turner, M. (2019, May 20). Written Testimony for Public Hearing on Voluntary Voting System Guidelines 2.0 Principles and Guidelines. *Center for Democracy & Technology.* [perma.cc/K5SR-9RH2]
[3] U.S. Election Assistance Commission. (2021, February 10). Voluntary Voting System Guidelines 2.0. [perma.cc/4XDE-RGP9]
[4] Adler, W.T. (2022, July 12). No Simple Answers: A Primer on Ballot Marking Device Security. [perma.cc/Q7WF-QYLK]
[5] Verified Voting. (n.d.). The Verifier. [perma.cc/BCS9-AQM5]

1401 K Street NW, Suite 200 Washington, DC 20005

CENTER FOR DEMOCRACY & TECHNOLOGY

Suggested additions to the VVSG's enumerated requirements and associated discussion sections are <mark>highlighted in yellow</mark>, and suggested deletions are ~~struck through~~. We also provide *italicized* commentary alongside these edits. Some suggestions are identical or similar to suggestions made by the State Audit Working Group[6] or the National Disability Rights Network.[7]

William T. Adler, PhD
Senior Technologist, Elections & Democracy
Center for Democracy & Technology
wadler@cdt.org

BMDs frequently encode voter choice in barcodes or QR codes.[8] Voters and auditors should be able to easily decode and understand how their choices are encoded. We suggest the following revision.

3.3-C – Bar and other codes
Manufacturers must provide publicly available documentation that fully specifies the barcode, how barcoded data is formatted, and any other encoding standards or methods used on ballots or audit material. <mark>The barcode must be decodable by commercial-off-the-shelf devices. (See *4.2-A – Standard Formats*.)</mark>

Discussion
The voting system documentation needs to include the name and version of the standard used for barcodes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to ~~develop applications that~~ examine <mark>and fully understand</mark> the barcoded contents <mark>with minimal need for application development</mark>.

---

[6] State Audit Working Group. (2023, May 22). Comment from State Audit Working Group.
[7] National Disability Rights Network. (2020, June 19). Comment from Michelle Bishop.
[8] Adler, W.T. (2022, July 12). No Simple Answers: A Primer on Ballot Marking Device Security. *Center for Democracy & Technology.* [perma.cc/Q7WF-QYLK]

CENTER FOR DEMOCRACY & TECHNOLOGY

Voter verification of BMD-printed ballots is a critical component of election security. However, these printed ballots are often difficult to comprehend. We suggest the following revision to ensure that ballots are more easily understood and verified.[9] Moreover, we suggest that manufacturers consider the future use of optical character recognition for interpreting voter selections, which would provide a security benefit by ensuring that the machine-readable portion of the ballot is the same as the human-readable portion.[10]

7.1-I – Text size (paper)
The voting system must be capable of printing paper ballots, including blank ballots for hand marking and ballots printed by BMDs, that are easily understandable by the voter. Ballots and other paper records should have a font size of at least 3.5 mm (10 points). Font and layout on paper should support potential use of optical character recognition on ballot images as a means of verification, tabulation, or supplemental audit review.

The key security benefit of a voting machine with a paper trail (i.e., a BMD) over one with no paper trail is to enable voters to verify their printed ballots. However, there is no requirement in VVSG 2.0 that the BMD inform the voter to verify their printed ballot. We therefore suggest that the following section be added. (The later requirements in 7.3 would have to be re-lettered.)

7.3-H – Voter verification of BMD-printed ballots
A BMD must inform the voter that the printed paper ballot is the official record of their vote and that the voter should verify the BMD-printed ballot before casting it.

Discussion
This requirement is intended to increase the likelihood that a voter will verify that their printed ballot reflects their intended choices, before they cast it.

We suggest the following changes to streamline the section on usability testing and make it more comprehensible. More substantially, it requires that manufacturers report the rates at which voters

---

[9] Baumeister, L. & Quesenbery, W. (2021, August 30). Legibility of paper ballots: What makes a printed summary-style ballot easy to verify? *Center for Civic Design.* [perma.cc/95EP-UZXF]

[10] Adler, W.T. (2022, July 12). No Simple Answers: A Primer on Ballot Marking Device Security. *Center for Democracy & Technology.* [perma.cc/Q7WF-QYLK]

verify their BMD-printed ballots. We recognize that the associated Test Assertions document[11] contains more detail on usability testing. Our suggested changes will require corresponding changes to the Test Assertions document; that may be an appropriate place to provide more detail on how to determine whether voters are thoroughly reviewing their BMD-printed ballots. Alternatively, the EAC could consider including more detail on usability testing requirements in the VVSG Requirements document.

8.3-A – Usability tests with voters

The manufacturer must conduct usability tests with voters using the voting system.~~, including all voter activities in a voter session from ballot activation to verification and casting.~~

~~The test participants must include voters who represent the following:~~

~~1. General population, using the visual interface (without audio), including:~~

1. The test participants must include:
   a. voters using the visual interface without the audio format;
   b. voters who are native speakers of the language being tested for each language defined as supported in the technical data package (TDP);
   c. blind voters, using the audio format plus tactile controls;
   d. voters with low vision, using the enhanced visual features with and without audio; and
   e. voters with limited dexterity, using the visual interface with low and no dexterity controls
2. Usability tests must include all voter activities in a voter session from ballot activation to verification and casting.
3. Usability tests for ballot marking devices (BMDs) must evaluate the percentage of voters who review their ballots and the frequency with which they detect discrepancies between their intended selections and the human-readable information printed on the ballot.
4. The manufacturer must submit a report of the results of their usability tests, including effectiveness, efficiency, and satisfaction measures, as part of the TDP using *ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b].*

---

[11] U.S. Election Assistance Commission. (2021, February 10). Voluntary Voting System Guidelines 2.0: Test Assertions Version 1.1. [perma.cc/U9MF-SQ7E]

Software independence means that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results.[12] Systems in which the ballot selection area of a voted ballot passes under a printhead after verification are arguably not software independent; an undetected change to the software could enable the system to alter the selections on the ballot. The current version of the VVSG arguably accommodates systems in which the ballot passes under a printhead that is disabled from printing on the ballot selection area only via software. We suggest clarifying that the system should be not merely disabled from printing on the ballot selection area via software, but physically unable to print over the ballot selection area.

9.1.5-G – Preserving software independence

After a voter verifies their selections on a voted ballot and submits the ballot for casting, a paper-based voting system must not be capable of making an undetectable change to the paper record.

Discussion

After a voter verifies and submits their ballot, a voting system may print on paper ballot to apply a unique identifier that is later used for auditing purposes. To preserve software independence the voting system should not be <mark>physically</mark> able to print over or within the ballot selection area because that would cause an undetectable change to the election outcome. Instead the voting system should only be <mark>physically</mark> able to print outside of the bounds of the ballot selection area and may also create further distinction by printing in a different font style or color.

This printing process should be preserved regardless of software or hardware updates.

Some voting systems produce voted ballots that can appear very different, depending on whether they are filled in by hand or printed out by a BMD. If, in this case, for example, only a single voter in a precinct uses a BMD to vote, then it may be easy for someone with access to the ballots cast in that precinct to identify that voter's selections. We suggest the addition of the following section to protect

---

[12] Rivest, R.L. (2008, August 6). On the notion of "software independence" in voting systems. *Philosophical Transactions of the Royal Society A.* [perma.cc/B97S-PUTX]

the privacy of (e.g., disabled) voters who may be part of a BMD-using minority of voters in a polling place.

10.2.2-F – All voted ballots produced are similar

All methods of voting supported by a voting system must produce voted ballots of similar size, shape, and layout; or the manufacturer must provide procedures to be used to ensure that sufficient numbers of ballots of each type are cast to ensure ballots cannot be easily associated with individual voters on the basis of ballot type.

The VVSG already requires that systems be capable of multi-factor authentication to verify the identity of users before performing critical operations like updating system software or tabulating ballots. We suggest this additional section so that election officials can choose to require authentication from multiple people in order to carry out operations deemed particularly critical.

11.3.1-D – Multi-person authentication for critical operations

The voting system must be capable of using multi-person authentication for performing critical operations. (See *11.3.1-B – Multi-factor authentication for critical operations* for examples of critical operations). Multi-person authentication capabilities enable election officials to choose to require (multi-factor) authentication from two or more users, presumably bipartisan, before executing actions.

Compliance audits are referred to in the requirements but not defined. We suggest the following addition to the glossary.

compliance audit

A compliance audit is a comprehensive review of an organization's adherence to governing documents or processes. For instance, a compliance audit of a paper ballot system assesses the trustworthiness of the paper trail. It includes but is not limited to ballot accounting, eligibility compliance, physical chain-of-custody, and evaluation of compliance with election processes.