VerifiedVoting

Verified Voting public comments on VVSG 2.0 for 2023 annual review
June 7, 2023

We appreciate the opportunity to offer public comments as part of the U.S. Election Assistance Commission's annual review of version 2.0 of the Voluntary Voting System Guidelines (VVSG). VVSG 2.0 offers valuable improvement over previous standards, especially in its standards for auditability (foregrounding software independence), interoperability, accessibility, ballot secrecy and voter privacy. The accreditations of two Voting System Test Labs to test to VVSG 2.0, last November, constitutes crucial progress in the implementation of these enhanced standards. This annual review offers a valuable means for all interested parties to help ensure that the standards are clear and comprehensive.

The following comments focus on relatively few aspects of VVSG 2.0, generally pertaining to voter verification and other key elements of auditability.

1.1.5-G – Record audit information: We support essentially the current scope of this requirement. In particular, including both "identification of the specific creating device" (often referred to as "tabulator ID") and batch identifiers can be crucial in many tabulation audits and ballot reconciliation processes. Tabulator IDs also can be important in investigating anomalous results.

See also our third point under *9.4.A – Risk-Limiting Audits*.

7.3-G – Full ballot selections review: This section appropriately requires a voting system with an electronic voting interface to provide a function for reviewing all selections "before printing or casting their ballot." However, for *paper-based* systems with an electronic voting interface—i.e., ballot marking devices—voters also must verify their printed ballots before casting them. This voter verification confers software independence. Accordingly, for such systems, the VVSG should explicitly require the voting system to prompt the voter to check their printed ballot before casting it. (Additional voting system support for voter verification may be warranted.) This requirement could be added to 7.3-G or included separately, as follows:

"[the electronic voting interface] prompts the voter to review their printed ballot for correctness before casting it."

8.3-A – Usability tests with voters: This requirement implies that paper records produced by paper-based voting systems must be included in the usability testing (as part of "all voter activities in a voter session from ballot activation to verification and casting"). However, neither the requirement and discussion nor the test assertions specifically address testing voters' ability to verify the voter verified paper records. This is a serious omission. It is crucial to ensure that voters with all the various characteristics mentioned in 8.3-A can, in realistic conditions, verify their VVPRs before casting. Nominally voter-verifiable paper records that many voters cannot verify in practice, due to design flaws in the equipment or the records themselves, do not provide substantive software independence. Paper record usability testing should be explicitly mandated under this requirement and the associated test assertions, for instance, adding the following the introductory text in 8.3-A:

"Usability tests must include testing of the voter verified paper records produced by the voting system."

There appears to be a formatting error involving the definition of test participants. (One effect is that numbered point 2 has nothing in common with point 1.)

9.1.3-A – Records for voter verification: The requirement that voters be able to verify that the voting system correctly "interpreted" their ballot selections is inscrutable. We believe the intention is that voters be able to verify that their ballot selections are correctly "recorded," either on a voter verified paper record or in an end-to-end verifiable digital record.

9.4-A – Risk-Limiting Audits: This discussion is welcome but would benefit from further refinement. 9.4-A states, "A paper-based voting system must produce paper records that allow election officials to conduct a risk-limiting audit." It is unclear what paper records are intended here beyond the voter-verifiable paper records discussed under 9.1.5, *Paper records*. As the discussion of 9.4-A makes clear, some *digital* records—at bare minimum, ballot manifests—typically are integral to risk-limiting audits. The language of 9.1.4-A, *Auditor verification*, appropriately is more general: "Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated." We suggest removing the word "paper" from 9.4-A in parallel: "A paper-based voting system must produce records that allow election officials to conduct a risk-limiting audit." Additional changes may be helpful.

The discussion of 9.4-A at times seems to conflate risk-limiting audits (RLAs) generally with ballot-level comparison RLAs. Ballot-level comparison RLAs are most efficient, but not the only kind of tabulation audit that a paper-based voting system should support. Most tabulation audits conducted in the United States, including many RLAs, are *batch-level* comparison audits that rely upon batch subtotals (i.e., tabulation reports subtotaled by batch). (A batch represents a set of ballots that are tabulated and stored together, such as all the ballots tallied on a voter-facing scanner, or a set of ballots fed through a batch-fed scanner.) Batch-level comparison audits may well remain common even after requirements that support ballot-level comparison audits are widely adopted. With these points in mind, we offer the following comments:

1. The ability to export batch subtotals in a machine-readable format should at least be listed among the "example features/paper records" in the discussion. We recommend that it be formally required and tested for. 1.1.5-G, *Record audit*

information, already requires CVRs to include “identification of the batch containing the corresponding voted ballot, when applicable”—information that supports voting system export of ballot manifests (although any such manifests should be checked in compliance audits) and also can support batch subtotals. For instance, the following could be added as 9.4-E –Batch reporting:

“The voting system must be able to export batch subtotals [compliant with CDF specifications].”

2. The text states, “For example, batch subtotal reporting by the voting system, may make the process of ballot sampling more efficient.” Batch subtotals (in the sense we describe) are integral to batch-level comparison audits, but they are not used to sample individual ballots. We suggest clarifying the statement as follows [new text italicized]: “For example, batch subtotal reporting by the voting system *is essential for batch-level comparison audits*.” Other examples could be offered, but they seem unnecessary here.

3. Relatedly, it is highly desirable for voter-facing scanners used in early voting to be capable of assigning ballot sheets to batches—for instance, one batch per day of early voting—crucially provided that vote totals remain unavailable until the closing procedures are completed at the end of early voting. (Also, jurisdictions that handle early voting ballots before the end of early voting must implement strict procedures to protect ballot secrecy.) This capacity allows jurisdictions to divide large numbers of ballot sheets tabulated during early voting into smaller batches, facilitating ballot reconciliation and tabulation audits including risk-limiting audits (RLAs).

   It is unclear how best to facilitate support for batching early voting ballots. One approach would be to add to 1.1.5-G: “8. identification of the date when an early voting ballot is cast, when applicable.” In many cases, this information could allow jurisdictions to batch early voting ballots by date cast without compromising ballot secrecy. However, this approach runs afoul of the discussion of 10.2.2-B (see comments below), and does pose some possibility of deanonymizing ballots or votes if an early voting scanner is barely used during a day of early voting. That problem could be addressed by automatically combining consecutive dates when necessary to avoid deanonymization, or by providing some procedure for election workers to designate new batches. We believe this issue deserves further consideration.

9.4-C – Unique ballot identifiers: This important requirement should be clarified. For paper-based voting systems, auditability typically entails that election auditors must be able to address individual voter verified paper records, or ballot sheets. The ballot sheets of multi-page ballots (referenced without discussion in 9.4-D) often cannot be reliably associated after ballots are cast, and may even be deliberately separated to protect ballot secrecy. Adding the phrase "or ballot sheets" as follows may suffice to generalize the requirement to both paper-based and end-to-end verifiable systems:

"The voting system must enable election auditors to uniquely address individual ballots *or ballot sheets*."

The discussion of 9.4-C notes that "The unique ballot identifier must not tie a ballot to an individual voter." However, the corresponding test assertion does not address this requirement. This omission is significant because unique ballot identifiers assigned by voter-facing scanners—unlike identifiers assigned by batch-fed scanners—must be randomized to obfuscate the order in which ballots were cast. Unfortunately, not all implementations of pseudo-random numbers obfuscate the order. We recommend adding a test assertion to ensure that voter-facing scanners that imprint non-serialized unique ballot identifiers do so in a manner that satisfies the requirement and also meets the standard specified under 10.2.2-E – Randomly generated identifiers.

Also, the discussion of 9.4-C should clarify that this requirement is needed to support *ballot-level comparison* RLAs, not all RLAs as follows [new text italicized]:

"This capability is needed to support *ballot-level comparison* RLAs."

10.1-A – System use of voter information: The discussion notes, in the context of ballot secrecy, that "the voting system cannot prevent a voter from self-identifying within write-in fields or other areas of the ballots." We suggest noting that this concern extends to unredacted ballot images and, potentially, CVRs. These digital artifacts can pose additional threats to ballot secrecy. (The requirements for guideline 10.2 grapple with this conundrum.) We do not believe VVSG 2.0 can be expected to resolve the policy questions pertaining to ballot images and CVRs. Nevertheless, some reference to the underlying ballot secrecy concerns would provide helpful context.

10.2.2-B – No voter record order information: The discussion states: "No data or metadata is allowed whether in CVRs and ballot images or elsewhere if that metadata can be used to associate a voter with a record of voter intent…. For instance, date of creation of record in the voter-facing device might reveal the order of voting." It is unclear whether the discussion intends to forbid including creation date in CVRs and other artifacts, or only to take whatever precautions are needed to avoid revealing voter record order. (See our discussion above under point 3 of 9.4-A.) We would prefer the latter approach, which could be supported by adding to the current language: "...might reveal the order of voting unless steps are taken to prevent this." Including creation dates in most early voting CVRs, combining dates if necessary to protect ballot privacy, appears to be the simplest and best way of allowing early voting ballots to be audited in smaller batches.