# Comments on draft VVSG 2.0

## P.B. Stark

## Prepared for the EAC Public Hearing on VVSG 2.0

## Salt Lake City, Utah

## 23 April 2019 (Last edited 29 April 2019)

This document is a slightly extended version of comments presented in oral testimony at the 23 April 2019 hearing on draft VVSG 2.0.

- I am limiting my comments to the principles, not the guidelines.
- Overall, the principles in VVSG 2.0 are terrific and I strongly endorse them.
- I strongly support separating principles from detailed technical requirements.
- However, the devil is often in the details—in this case, the detailed requirements that will flow from the principles and guidelines.
- As far as I know, there is as yet no process to ensure that the detailed requirements embody the VVSG and do not contradict it.
- My primary concerns with the VVSG Principles themselves regard language that is ambiguous and wording that suggests that future voting systems will not use hand-marked paper ballots—the most secure, trustworthy, and resilient mode of voting currently available.
- I also recommend that the VVSG include a precise glossary to define important terms including "ballot," "cast," "cast vote record," "audit," and "physical port." While the definitions in the VVSG might conflict with the use of those terms in state laws, it is necessary for the VVSG to be completely clear; the use of that language of course is not binding on states. Language concerning the "secrecy" of ballots and votes versus the "anonymity" of ballots could also be improved: voters should vote privately and there should be no way to link votes to individual voters, but votes should be anonymous rather than secret.

I now comment on specific principles.

## Principle 4: INTEROPERABLE The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

- This is critical for establishing a truly competitive market for voting systems, to facilitate innovation, and to facilitate meaningful audits of election results.
- Software to support efficient tabulation audits, such as risk-limiting audits, will need to parse exported results and exported cast vote records, for instance.
- Interoperability is also critical to enable more modular certification decisions, so that eventually, individual components rather than monolithic systems can be certified. That can facilitate the deployment of technology improvements and security improvements and make maintenance and upgrades cheaper and easier.

### 5.1 Voters have a consistent experience throughout the voting process in all modes of voting.

- This could be read to imply that all voters should use the same technology to mark and cast ballots, which could reduce usability for some groups of voters.
- Each voter should be provided a means of marking, verifying, and casting a ballot that is as usable by that voter as possible.

### 5.2 Voters receive equivalent information and options in all modes of voting.

- This implies that the system should provide voters with disabilities a means to verify independently that what is printed on the paper record matches their selections. It would be good to spell that out explicitly.

### 6.2 Voters can mark, verify and cast their ballot or other associated cast vote record, without assistance from others.

- Voters do not “cast” or “mark” cast vote records; voters cannot see, touch, or verify cast vote records.
- Voting equipment creates a cast vote record from voter input. CVRs are the system’s internal electronic representation of the voter’s selections.

- There is no guarantee that the cast vote record matches the voter's input, what the voter saw on the screen, or what was printed on the ballot. Indeed, one way of conducting a risk-limiting audit involves checking whether CVRs accurately reflect what is printed on the corresponding ballot.
- This is another example of language that needs to be tightened.

## Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

- Again, this should include a provision to ensure that voters with disabilities are provided a means to verify independently that what is printed on the paper record accurately reflects their selections.
- On-screen (or audio) verification before the paper record has been printed is not sufficient, because the system could print something different on the paper record, as a result of bugs, misconfiguration, or hacking.
- Again, the language in this principle lacks precision: "vote selections" are not cast. Ballots are cast.

## 7.1 The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

- This implies that all voters will vote using an electronic interface, which would be detrimental to election integrity and security.
- I suggest revising the wording to include requirements for usability of hand-marked paper ballots.

## 7.2 Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

- This implies that ballots, rather than ballot presentation formats, are controlled by the voter.
- The voter should have control over some aspects of the format of the presentation of information for the purpose of making selections.
- This is another example where the draft language is not consistent. The "ballot" is a piece of paper that records the voters' selections, not a screen that presents the voter options.

## 8.3 The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

- "Effectiveness" and "efficiency" need workable definitions.
- How does one trade off between speed and accuracy?
- Measuring things is great—if they are well defined—but what action does this lead to? How do these measurements affect whether a voting system can be certified?
- The system should be tested for accuracy in capturing voter intent and for ease of use, both for recording votes and for verifying selections on the paper ballot, for representative voters, including voters with and without disabilities.
- Satisfaction is desirable, but accuracy and ease of use are essential.
- Analogously, good bedside manner increases patient satisfaction with doctors, but first and foremost, we need doctors to be competent.

## 8.4 The voting system is evaluated for usability by election workers.

- This should include usability for auditing election outcomes, not just for conducting the election.
- Is "evaluation" enough? Presumably there is a minimum level of usability that should be required for certification.

## 9.4 The voting system supports efficient audits.

- This is rather vague. What constitutes an audit? What is to be audited? What does it mean for an audit to be "efficient"—what is it to be compared to?
- The definition of "audit" varies widely across jurisdictions. Some jurisdictions consider examining a transaction log to be an audit. While that is valuable, it is not sufficient to establish that contest outcomes are correct. The same is true for logic and accuracy testing (LAT), and for "audits" based on inspecting digital images of ballots, rather than the original voter-verified paper records.
- The system should support efficient audits of the integrity of the paper trail and the accuracy of the tabulation and the reported results, at a minimum.

- We need systems to support audits that can detect whether the evidence trail has been compromised and that can correct wrong reported outcomes, for instance, so-called "compliance" audits of the integrity of the paper trail. combined with rigorous risk-limiting audits of the tabulation. Here is some terminology, for reference:
  - A *compliance audit* establishes whether the paper trail is trustworthy.
  - A *risk-limiting audit* (RLA) ensures that if tabulation errors caused the wrong candidate or position to appear to win, there is a large chance of correcting the outcome before it is certified. RLAs involves manually inspecting a random sample of paper records. If a compliance audit has demonstrated that the paper trail is trustworthy, a RLA has a known probability of correcting the outcome if the outcome is wrong, no matter why it is wrong.
- RLAs are most efficient when the voting system can export a cast vote record (CV) for each physical ballot, in a way that the ballot that corresponds to a given CVR is uniquely identified, and vice versa. That makes it possible to check the voting system's interpretation of individual ballots. It would be facilitate efficient audits if the VVSG required voting systems to create and export a CVR for every physical ballot, in such a way that the corresponding physical ballot is uniquely identified and can be retrieved for manual inspection.

## 10.1 Ballot secrecy is maintained throughout the voting process.

- Ballots are public records of a sort.
- Votes should be anonymous, not secret.
- The contents of at least some ballots need to be seen by election officials and auditors, but there should be no way to know who cast which ballot.
- This is another example where the language should be tightened.

### Principle 13 and Principle 14.2

- Together, these *should* imply that voting systems shall not have wireless connections such as bluetooth, WiFi, or cellular communication ports.
- Is a wireless interface considered a "physical port"? There is no definition of "physical port."
- Will the requirements reflect that?

- I recommend that the VVSG prohibit radios of any kind in equipment used to mark ballots, record votes, or tabulate votes. Such wireless communication hardware should not be present in those devices: disabling it in software is not an adequate precaution.

### 15.4 A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

- No system for capturing or tabulating votes should ever be connected to the Internet, nor to a private network that is connected to the Internet, nor to any other public communications infrastructure.
- No system for marking ballots or capturing or tabulating votes should have "remote desktop software" installed.