VerifiedVoting

Verified Voting.org

Public Comments on VVSG 2.0 Principles and Guidelines

Submitted May 29, 2019

Verified Voting is pleased to see the VVSG 2.0 principles and guidelines finally moving forward. We are enthusiastic about the VVSG 2.0 structure and, with some reservations, about the content of the principles and guidelines. Full implementation of the VVSG 2.0 will, in time, help bring about voting systems that set new standards for universal usability, security, and verifiability. All these properties – backed by sound procedures – are essential to enable officials to run resilient elections, and to reassure voters that their votes have been cast as intended and counted as cast.

We urge the EAC to allow the technical requirements and test assertions to be approved and revised without a vote of the commissioners. We agree with the TGDC, the NASED executive council, and others that for several reasons, these documents are best managed by technical staff, adhering to a well-defined process with broad consultation and opportunity for public comment.

Verification and the VVSG

Verified Voting especially welcomes Principle 9, which stipulates that a voting system "is auditable and enables evidence-based elections," and the associated guidelines. No matter how otherwise usable and reliable a voting system may be, it is unacceptably dangerous if it cannot provide trustworthy, software-independent evidence that people's votes have been accurately recorded and counted.

A voting system alone can "enable" evidence-based elections but cannot provide them. As Philip Stark and David Wagner wrote in their seminal paper, the basic equation is that "evidence = auditability + auditing." A voting system with a voter-verifiable audit trail, such as a voter-marked paper ballot, provides auditability. Compliance audits to ensure that the audit trail is substantially complete and accurate, and risk-limiting tabulation audits of the audit trail, provide actual evidence that outcomes are correct.

These considerations point to two ongoing challenges for the EAC and everyone else who works with the VVSG. One challenge is to communicate

that, in practice, voting system security largely depends on election procedures and especially on post-election audit procedures. Compliance and risk-limiting tabulation audits happen after elections but cannot be afterthoughts: evidence-based elections depend on them.

The other challenge is to frame requirements and test assertions that help to move auditability from an abstract possibility to a standard of excellence. One lesson of the Help America Vote Act era has been that a voting system may be formally "accessible" without being very usable by the voters who need it most. Similarly, a voting system may be "verifiable in name only" if its audit trail is difficult for voters to verify and/or for authorities to audit.

Voting systems should be rigorously tested to see if voters consistently and effectively verify their paper ballots or other auditable records in a variety of election conditions. (See the discussion of "ballots" below.) The systems also should be assessed for ease of auditability. The most auditable paper-based systems not only provide paper records that are easy for audit officials (as well as voters) to handle and to verify, but allow each paper record to be matched with the corresponding digital cast vote record(s) without compromising ballot anonymity.

Ballots and cast vote records: definitions and implications for auditability

In common parlance, ballots are paper records of voters' votes, and cast vote records are digital representations of the votes on the ballots. To accommodate alternative models, the glossary that accompanies the VVSG defines "ballot" as a "presentation of the contest options for a particular voter," and "cast vote record" as an "archival tabulatable record of all votes produced by a single voter from a given ballot." In this framework, a ballot could be physical or digital, as could a cast vote record.

These expansive definitions seem to account for several confusing points in the principles and guidelines, such as 6.2's reference to casting a cast vote record. They also complicate discussions of auditability. In a system based on paper ballots, the paper ballots can be verified and cast by voters and then audited. In systems that do not use paper ballots – even if they produce an auditable paper record – verifying and casting the ballot does not assure that the voter has verified the auditable record. If we could make just one change to the principles and guidelines, it would be to clarify in principle 7 and the associated guidelines that voters must be able to readily verify the records that will be retained and used to check whether the election outcome is correct (guideline 9.2).

Moreover, we believe that for the foreseeable future, only voter-verifiable paper records should be used for this purpose. Given the inherent vulnerabilities of today's internet, no voting system that relies on digital records alone can provide truly secure and verifiable elections.

Specific comments

Principles 1 and 2: High Quality Design and Implementation

These principles are well framed, and we generally support the associated guidelines, particularly guideline 2.2 on user-centered design methods. Because most Americans vote no more than once or twice per year, user-centered design is essential to provide systems that voters can use accurately and verifiably.

We believe that the guidelines should explicitly reference security as a crucial aspect of high-quality design. This can be accomplished by adding a new guideline 1.4, "Voting system design incorporates security best practices," and by adding "best practices, including security best practices, in software development" in guideline 2.1.

Principle 3: Transparent

Guideline 3.1 refers to "security measures," which ordinarily would refer to procedures rather than elements of voting system design. We suggest changing "security measures" to "security features."

Principle 5: Equivalent and Consistent Voter Access

We support this principle. We recommend making explicit that guideline 5.1 extends to verification, for instance as follows: "Voters have a consistent experience throughout the voting process, including verification of the auditable records of their votes, in all modes of voting." All voters deserve voting systems that facilitate verification.

Principle 6: Voter Privacy

We support this principle. We recommend revising guideline 6.2 to clarify, again, that the need for independent verification extends to whatever records will be used to audit tabulation accuracy. The phrase "ballot or other associated cast vote record" is too vague given the ambiguous definitions of both those terms. One possibility: "Voters can mark, verify and cast their ballot and other auditable records of their votes without assistance from others.

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." We doubt that vote selections (contest selections?) can be cast. We believe the intended meaning is something like "Ballots, including contest options and contest selections, are presented in a perceivable, operable, and understandable way; ballots can be marked, verified, and cast by all voters."

We recommend adding a guideline to the effect that "The voting system allows voters to consistently and accurately verify their ballots and the auditable records of their votes." Such a guideline lends itself to requirements and test assertions that support high levels of voter verification. Here is another place where voting system security will largely depend on election procedures, such as polling place layout and the instructions given to voters.

Guideline 7.2 enigmatically specifies that “voters have direct control of all ballot changes.” The intended meaning may be “voters have direct control of all ~~ballot~~ changes in their contest selections.”

Principle 8: Robust, Safe, Usable, and Accessible

In guideline 8.3, “measuring… for effectiveness, efficiency, and satisfaction” seems vaguely defined. We recommend language that evokes a rigorous performance standard, such as “for ~~effectiveness, efficiency, and satisfaction~~ accuracy, efficiency, and satisfaction in marking, verifying, and casting their ballots.”

Principle 9: Auditable

We recommend revising guideline 9.2 to underscore that vote records used to verify outcomes should also be voter-verified. Moreover, for the foreseeable future, we would require these records to be physical. Also, a “correct” election outcome is undefined. We suggest: “The voting system produces readily available physical records that voters could verify. These records provide the ability to check whether the election outcome corresponds with voters’ contest selections and, to the extent possible, identify the root cause of any irregularities.”

In guideline 9.4, audit efficiency is desirable, but audit validity is paramount. We recommend expanding the guideline: “The voting system supports efficient, valid audits carried out with best practices.”

Principle 10: Ballot Secrecy

We agree with the comments of the Electronic Privacy Information Center (EPIC) in support of this principle. The term “ballot secrecy” is not included in the glossary, and its exact meaning is not self-evident: voted ballots themselves are not secret, and typically become public records once the election is complete. Verified Voting fully endorses the principle of ballot secrecy or ballot anonymity, as expressed in guideline 10.2: roughly, it should be impossible to tell how a particular person voted. We recommend defining this term in the glossary.

Principle 13: Data Protection

This principle, and guideline 13.4, appear to use “sensitive data” to refer both to data that should not be revealed due to privacy or confidentiality concerns, and data that is critical to the integrity of the election but not “sensitive” from a privacy standpoint. We suggest deleting “sensitive” from the principle (no data should be subject to “unauthorized access, modification, or deletion”), and drawing the distinction in guideline 13.4: for instance, “The voting system protects the integrity and authenticity of all data, and the confidentiality of sensitive data, transmitted over all networks.”

Principle 14: System Integrity

Guideline 14.2 appears to be missing a word: "…by reducing unnecessary code, data paths, and physical ports, and by using other technical controls." We further recommend replacing "reducing" with "avoiding" or "eschewing."

We concur with the recommendation of EPIC, the State Audit Working Group (SAWG), and others to add a new guideline (or add to 14.2): "The voting system does not use wireless technology or connect to any public telecommunications infrastructure." These risks are best eliminated.

In guideline 14.3, we concur with the SAWG proposal to insert: "The voting system maintains and verifies, and facilitates independent human verification of, the integrity of software, firmware, and other critical components." Systems should not be relied upon to verify themselves.

Principle 15: Detection and Monitoring

Guidelines 15.3 and 15.4 seem to go beyond the scope of the associated principle. It may be appropriate to add "prevention" to the principle or to narrow these guidelines, perhaps broadening guidelines associated with other principles accordingly.

About Verified Voting

Verified Voting (www.verifiedvoting.org), founded by computer scientists in 2004, is a leading national not-for-profit, non-partisan organization focused exclusively on the critical role technology plays in election administration. Through education and advocacy, our mission is to strengthen democracy by promoting the responsible use of technology in elections. Since our founding in 2004, we have acted on the belief that the integrity and strength of our democracy relies on citizens' trust that each vote is counted as cast. We bring together policymakers and officials who are designing and implementing voting-related legislation and regulations with technology and election administration experts who comprehend the risks associated with the emerging digital landscape, particularly the online and electronic elements in voting. Additionally, we connect advocates and researchers, the media and the public to provide greater understanding of these complex issues.