TruVote
International

Basic Concepts

The basic concepts include the use of a voter verified paper record of the vote which becomes the legal record of the vote; independent verification processes where two independent records of the voter's selections are recorded, linked and audited; cryptographic signature of all data; and all data and los are signatured..

Audits are critical to the success and must be completed in an efficient and accurate manner.

Electronic financial transactions are a tested and accepted model for transparent, accurate and audited voting systems. Financial systems use paper receipts, independent verification cryptographic protection where required, and audits to insure accuracy. Hundreds of millions of electronic transactions are successfully completed without the problems experienced with voting systems.

Although voting machine security has received a considerable amount of interest in the public press where votes have been changed through hacking or modification of software, to date the voting process has not experienced these attacks. However other attacks and problems have been demonstrated, in particular, poor ballot design; inability of the voter to accurately record their race selections; and not counting of ballots and errors introduced by polling place workers. Examples of these issues are the famous "butterfly ballot" and the Sarasota Florida undervote.

1. What do you think will be the dominant business model for voting system vendors in the coming decade? Will vendors be technology innovators or service providers? Both or neither?

The economic model for voting equipment and services is unique in that the number of potential customers is well defined and limited. The market is not large and somewhat static and the voting industry has changed with the introduction of HAVA. The typical revenue model is one where an initial revenue bubble results from hardware purchase which is followed by a smaller the recurring revenue stream from election services. As an example, little additional voting equipment has been purchased in the past few years with the exception of PCOS systems. However, significant revenue has been generated through election services. This model is expected to repeat as new legislation is introduced and funding is available to support the objectives of the 2007 Guidelines.

The 2007 Guidelines are significantly more complete and complex than prior Guideline versions. The complexity of the 2007 Guidelines will significantly increase the barrier of entry for companies to comply and be certified. In the same manner that few companies certified their systems to the 2005 Guidelines even fewer will certify to the 2007 Guidelines. The 2007 Guidelines will have the effect of requiring increased pricing for voting equipment due to the costs of certification. Alternatively, jurisdiction officials will be faced with the problems of accepting voting systems which are certified to an older set of guidelines.

The 2007 Guidelines will have a significant impact on the future of the voting industry. The requirement of openness removes the trade secret and proprietary cloak from election programming where a new generation of "election programming" consultants and services will emerge. These new participants in the industry introduce an additional problem with the lack of their experience. A certification process for election programmers needs to be established similar to that used in the computer and networking industry.

2. Is the proposed Innovation Class section of the 2007 VVSG Draft a viable approach to certification testing? As written, how would it impact your firm's strategy for developing and marketing systems?

Innovation classes as defined in the standard are principally focused upon new voting machines and ballot recording processes. Innovation classes should be expanded to include classes that address the other aspects of a transparent, accurate and audited system such as electronic poll books and merged equipment types such as optical scanners and touch screens.

Many of the proposals introduced for additional classes tend to focus on only a portion of the total set of requirements for a transparent, accurate and audited voting system. A complete check list of system requirements which must be completed for each new innovation proposed. Proposers of innovation classes should measure their proposals against this check list.

3. What is the value of the open-ended vulnerability testing model? What are the risks? Do you conduct a form of this testing as part of your development process?

Open-ended vulnerability testing is a necessary but not complete solution for transparent elections. As mentioned above, the entire voting process should be considered. The end-to-end audit and accountability is of more value than an open-ended vulnerability test against a system. Vendors should not be held accountable for various attacks on their system as no system is immune to attacks. Independent Verificaiton should be the primary focus for security.

4. How could the processes of the VVSG be modified to incorporate minor revisions without incurring the costs (time and money) of a total system test, and still maintain the integrity of the standard?

Vendors are exposed with conflicts between the need to make minor bug fixes and changes at a time schedules that does not permit a complete ITA sequence. As a vendor passes through the ITA schedule for the first time and the test plan is developed, the vendor should be allowed to perform their own testing and certification of changes against that test plan. This should be sufficient for a small changes to be released. However, the vendor must accept accountability for these changes and are liable for problems which may ensue. Only after the changes pass through the ITA process is this accountability mitigated.

5. Does the current draft of the VVSG create functional standards which permit vendors appropriate design freedom to innovate and implement, or

is it a design standards that specifies how to build and implement voting, limiting design options

The draft of the VVSG limits the design and functional capabilities of the next generation of voting system. However, it does leave considerable latitude for innovations in screen designs and human factors which provide system differentiation. Various hardware designs are also possible.

The draft should provide an emphasis on the use of COTS for hardware and software to minimize design, support, implantation costs and security risks. The use of commercial components with extended usage will increase the reliability of both hardware and software. The amount of unique application and border logic should be minimized as well as the design of customized hardware.

The flexibility of user interface available in the VVSG also causes problems as these user interfaces appear to be responsible for many voter errors and other inaccuracies in the vote. Standards and practices for user interface design should be expanded. .

6. Are there any changes to the VVSG, in either scope or depth, which would significantly reduce the cost (time and/or expense) of compliance without adversely affecting the integrity of the VVSG or the systems that are derived from its implementation

The guidelines should be expanded to assist election officials in their responsibilities. A transparent and accurate election requires more than just having hardware and software. Suggestions and guidelines created by EAC for the major responsibilities of election officials should be added and incorporated into the voting system design. This provides support for election officials and minimizes problems with election accuracy that result from inexperience.

The depth of the VVSG is good. However, the scope needs to be expanded in particular in the areas of process and operation.

The requirements for PCOS systems which meet the intent of independent verification should be expanded.

The EAC provides guidelines for suggested practices in election management. These practices need to be codified and introduced into the standard. Jurisdictions may accept of reject these practices, but they should be supported by application logic in the voting system and easily modified by the jurisdictions to meet their needs. The use of such standards will minimize the probability of defective processes that can cause errors in the election.

The Guidelines need to be expanded to incorporate suggestions for ballot and screen layouts. Recent studies have shown screen and ballot layout have a major effect on the ability of the voter to accurately record their race selections. Examples of ballot and screen design have resulted in election confusion such as the “butterfly ballot” and the Sarasota Ballot. Election officials do not have the time nor often the experience to perform usability testing on their ballot designs and as a result confusion can exist at the polling place as voters with a wide range of experience and capabilities use the system. A national standard for ballot layouts might be considered which is well tested and effective that jurisdiction officials can use for their ballots. Ballot and screen layout is not an area of random invention.

The recent release of Voting Technology The No-So-Simple Act of Casting a Ballot has documented the need for a measure that includes the accuracy of the voter in recording their intentions on the ballot or voting machine. Ballot and screen design suggestions should be added to the Guidelines.

The 2007 Guidelines have accepted PCOS as a viable system which meets the IV standard while this is not correct. Studies have shown optically scanned ballots are no more secure than punched card systems; the ballots are easily modified; modification or confusion of ballots require jurisdiction officials to "determine the intent of the voter". The guidelines should be modified to define independent verification requirements for PCOS systems to eliminate these issues.

Accuracy should be expanded to include not only the accuracy of the system in counting the votes, but also the accuracy of the system in accurately recording the intention of the voter. This accuracy should be significantly less than 0.5%.

The guidelines need to identify the process whereby a vendor can be certified to provide ongoing election programming and support. There needs to be a national certification for individuals who provide these services.

Requirements in the guidelines are based upon "shall" and "may" levels of differentiation. These definitions should be expanded to include a relative importance of each requirements. For example, the requirements concerning under and over votes are probably more important than the need to operating the voting equipment for two hours on battery power. After all, it is difficult to vote in the dark

Certification should follow the same process. The current "pass/fail" process should be expanded to a range of conformance. A vendor may choose to not implement fully a requirement due to possible expense and schedule impact. The system should not "fail" due to these tradeoffs. Jurisdiction officials must have a clear ability to understand where these trade offs have been made. A table of requirement, relative importance and conformance scale should be provided.

7. How would the proposed VVSG impact the time-to-market of a new voting system? Can you identify specific requirements and associated processes within the standard that would significantly impede timely development and deployment of a voting system? What recommendations would you suggest for modifying the standard to address these impediments

The standards must enable vendors to implement and deploy for the 2010 and 2012 federal elections. Twelve months must be provided in the schedule for jurisdictions to accept, train polling place workers and prepare operation procedures.

Voting system vendors must accept the responsibility for quality systems. After test plans have been generated, the vendors can certify they have testing their system and/or changes to their system to these standards. However, the vendor retains legal accountability for their in-house tested systems. As the vendors has completed ITA testing, these legal accountability requirements are no longer applicable.

The ITA process should be a two stage process. The first stage will be for the ITA to assist the vendor in completing a test plan. Vendors who intent to minimize the cost and time associated with certification should validate their system against this test plan before the system is submitted for certification. Vendors should be able to offer their systems for use by the jurisdictions after they have completed internal testing against the test plan. However, vendors are accountable (legally and financially) for their systems meeting the test plan. As the vendor completes the full ITA certification of their system, the vendor is relieved of this accountability.

A focus on voting systems to use COTS hardware and software will minimize the costs and time required to meet the guidelines.

TruVote Disclosure

TruVote has been issued a patent relating to voter verified paper ballots and audit processes. The claims of this patent are encapsulated in the 2005 and 2007 Guidelines. TruVote however, has not participated in the definition of these requirements and the claims of the patent were identified prior to the discussion and issuances of these guidelines.

TruVote provides a software product which implements voter verified paper ballots and audit processes.