www.votehere.com

155 108th Ave NE
Suite 425
Bellevue, WA 98004

425 450.2770 T
425 453.4350 F

VOTEHERE

20 December 2004

From Jim Adler <jim.adler@votehere.com>

To EAC Technical Guidelines Development Committee (TGDC)

Subject Security and Transparency in Electronic Voting

Thank you for giving me the opportunity to provide input to your voting standards project. As you know, elections are deceptively difficult with many believing they are experts (at least initially) but all being humbled (eventually). It is with this humility that I submit some brief observations on the current FEC voting system standard, the IEEE P1583 voting standards effort, and some recommendations on how to proceed toward an effective security and transparency standard.

The current standards dilemma – fuzzy goals

The current FEC standards for voting systems have been widely criticized for being insecure, insufficient, and ineffective. The standards could be greatly improved by promoting confidence in *election results* instead of merely specifying the security of *election equipment*.

Election confidence can be proven through a combination of technology, procedure, and people. By building security and transparency into the entire election process, not just through adding more layers of security to the voting device, confidence can be measured and incrementally improved in each election.[1]

The IEEE P1583 standards effort has focused on the creation of improved standards for some time. However, the resulting standard is flawed in several key areas:

- The standard puts the cart before the horse. It focuses on prescriptive functional design requirements, while largely skipping meaningful performance requirements. Instead of describing what results are desired from a voting device, it describes existing designs. This stifles the innovation, since there is only one basic design that can get qualified.
- By limiting the scope of this standard to just poll-site voting machines in isolation of the rest of the ballot chain-of-custody, the door is left wide open for larger, system level vulnerabilities. Without a reasonably complete "usage framework" to evaluate voting machines end-to-end, only the most superficial and ineffectual analysis can be performed.
- Outside of the "voter verification" sections (Annex I and J), the standard tries to achieve security entirely through protective measures and, in so doing, ignores the use of detective technology and/or procedures for the discovery of system failures and fraud.
- Many of the more complete sections of the current draft appear to be cribbed from other sources without due consideration as to how they might apply to voting. For example, the "Usability" section is taken quite liberally from military standards. This is probably a fine source for mandating a design for use by young soldiers, but fails when applied to the six-sigma voting population.

[1] For more detail on how to quantify and measure election confidence, see Annex I (Voter Verifiable Audit Trail, Sections 1-3) and Annex J (Fraud Detection Probability), *IEEE P1583™/D5.3.2 Draft Standard for the Evaluation of Voting Equipment.*

A clear goal – confidence in election results

The IEEE P1583 standard attempts to improve upon previous standards such as the 2002 FEC Voting System Standards – an admirable goal. However, P1538 restricts its scope to "voting equipment used directly by the voter" and, therefore, largely ignores standards surrounding tabulation equipment, election procedures, and personnel that clearly have a direct impact on confidence in election results.

Election confidence would require that, in every election, (1) voters have the ability to verify that their vote is counted properly and (2) that anyone has the ability to audit the election results.

Reliability, accuracy and security standards

No system can be "perfectly" reliable, accurate, and secure. It is possible to specify such a standard, but building such a machine would take exorbitant resources. Yet P1583 ignores precedents in other types of transactions made daily by millions of people. Online banking, ATM's, e-commerce, credit card, and many other types of transactions are trusted not because the machines that enable these transactions are perfectly secure (to say Common Criteria EAL7), but because of a balance of preventive security combined with customer verifiability and end-to-end auditability.

The election industry should take a lesson from these best practices. A better solution would identify reasonable levels of reliability, accuracy, and security, and require minimum levels of robust audit and transparency. By adding transparency to the election process, levels of detection are added to layers of protection. With detection, election confidence can be definitively proven. And if election confidence cannot be proven for a given election, rational policy can specify appropriate remedies.

Without detection capabilities, it is guesswork to determine where and how to place protective measures. Such detection mechanisms could be used to devise more effective protective mechanisms; to locate and track down equipment failure or software defects; to identify or respond to procedural problems; or to identify election fraud. Voting machine vendors should be required to prove, through testing and analysis, that their designs meet or exceed allowable error rates.

Operating environment, procedures, and personnel

Voting machines do not operate in isolation. In fact, many of the security measures that protect them today are based on procedural steps related to their deployment. To specify a design for voting devices and then completely ignore how they will be used in a larger end-to-end system and process is irresponsible.

An adequate standard must set requirements for the effectiveness of a voting machine within its operating environment of procedures and personnel.

Recommendations

With respect to transparency and security, I would recommend the following minimum guidelines:

1. Establish minimum standards for election confidence through (1) voter verification that their vote is counted properly and (2) results verification by any auditing organization.
2. Require that any election system support, by technology and/or procedure, the measurement of election confidence.
3. Require that jurisdictions measure and publish election confidence for each election.

Again, thank you for this opportunity. Please don't hesitate to contact me if you have any questions or require any clarification.

Best Regards,

/s/

Jim Adler
Founder, VoteHere, Inc.
Co-Chair, IEEE P1583 Voter-Verifiable Special Task Group 3