Votermarch

David Aragon
1563 Solano Ave. #434
Berkeley, CA 94707
voterregistration@votermarch.org

December 18, 2004

Members of the Technical Guidelines Development Committee
for the Election Assistance Commission

c/o Allan Eustis
Project Leader, Voting System Standards, NIST
via email: voting@nist.gov

Dr. Eustis, TGDC Members, and Honorable Commissioners:

When you receive the current draft of the IEEE P1583 Standard, it will be accompanied by an Excel spreadsheet of comments from working group members. That format is good for corrections at the line or paragraph level, but not for addressing overall problems in the organization or assumptions behind the Standard. I am therefore addressing these comments to the TGDC directly.

Three sections of the current draft contain material that can assist TGDC's work:

- Section 5.3 (Usability and Accessibility). This section – alone of all the main sections – properly derives requirements from the needs of the *voter* as opposed to the properties of the technology.
- Section 5.4 (Environmental) is essentially non-controversial within P1583. The TGDC may wish to examine the temperature limits in 5.4.5 as to whether the upper limit of 104° F adequately protects the rights of voters in Gulf Coast states.
- In Annex I, Section I.4.1 is derived from the California standards and can be the basis for a Federal (EAC) version of those standards – but only for the specific architecture to which they refer.

The remaining normative sections of the document are not yet in condition to use.

Although improved from earlier drafts, the Standard still proceeds not forward from the rights of the voter, but backward from an assumed technical solution. Further, in much of the draft, a particular technical solution is assumed – a DRE. The Standard extends only with difficulty even as far as optical scanners, a very common current system; we can anticipate even greater difficulty in applying it to future innovations. (By "difficulty" I mean "confusion", which is quite a serious problem if certification is at stake.)

My concern is not merely over philosophy or emphasis. The inappropriate or inconsistent context makes it dangerous for TGDC even to lift specific technical requirements that may appear reasonable and conservative in themselves. It does voters no good to specify an $800 hammer where the system may or may not depend on nails.

You will receive many letters from P1583 members concerned with Security (5.1). I will therefore use Reliability (5.2) to illustrate my point.

First, mean time between failures (MTBF) is not a measure that should be applied to software components. MTBF is appropriate for hardware that may wear out or have manufacturing variations or defects, etc., which are well modeled by a random statistical process. Software is quite insensitive to its age, but very sensitive to its input data; if a program fails in a particular case, all copies of it will always fail in that case. While MTBF describes random failures of hardware operating within its design limits, software failures are usually the deterministic result of conditions unanticipated in the design. These conditions may depend on something about the voter. Thus, there can be civil rights implications that are not captured in a figure like MTBF.

Reliability requirements on any component (hardware or software) should be motivated by the question, "what would happen if it were to fail?" Failures can be distinguished according to how they are detected and corrected. Among the detectable failures, the more serious are those for which recovery is difficult or uncertain. Failures which may go undetected are, of course, the most serious. The Standard generally makes no such distinction, however.

Error detection is obviously an issue in security and reliability, but it is also a usability issue. Errors are noticed and acted upon *by someone*. Consider Carteret County, NC where the equipment worked as designed, but the majority of votes were lost. Officials noticed the error after the close of polls, too late for recovery. Had the error been noticed by pollworkers earlier, damage might have been reduced. But if it had been detectable by the *voter*, perhaps no votes at all would have been lost.

When we in P1583 consider a component (hardware or software), we ought to be asking ourselves "if this malfunctions, how can the voter notice and take action to protect their vote?" (Or failing that, how can election officials do so?) Extending the "voter first" approach of Section 5.3 to the other sections would make for a more robust, technology-neutral Standard, better aligned with EAC's mission.

Presently, however, that unifying context is lacking, and the Standard specifies components either out of context, or in the context of assumptions about DRE machines.

As one example, subsection 5.2.1.2 requires redundant memories for storing Cast Vote Records[†]. No motivation is given for requiring vendors to choose redundant storage over other known methods for reducing memory errors. The types of errors to be reduced are not identified, nor is there any model or even conjecture as to the amount of error reduction afforded by this design choice. It is possible to comply with this section without reducing *any* errors. Because 5.2.1.2 calls for discrepancies to be resolved by a "predefined hierarchy" of memories, a common understanding of "hierarchy" suggests accepting the result of the highest-ranking memory. In that case, the other memories cannot affect the output at all and are truly redundant! The Standard thus requires a specific implementation choice that adds to cost but need not deliver any benefit at all to the voter (though it sounds great in sales pitches). Conversely, if it were beneficial, why is this section labeled as being only for DRE, rather than for all machines that store votes in memories? It might be said (and was, in FEC 1990) that optical scanners do not require it because the paper ballot itself is an additional copy of the vote. But 5.2.1.2 explicitly excludes paper from the allowable media for the redundant storage function, with no reason given.

The confused requirement results partly from adversarial processes in the working group amending line-by-line. Unfortunately, those same processes apply across much of the Standard. The material often began as a description of a current DRE, then was amended based on concerns also specific to DRE designs, then counter-amended, and so forth.

TGDC has an opportunity to organize its guidelines differently, with a voter-centered notion of functionality against which the specific technologies can be measured. Values of voter empowerment and transparency, which P1583 avoids as "policy" questions, are perfectly within EAC's mission – and would also result in a more technically coherent and sound Standard.

Thank you,

David B. Aragon
Co-Chair, IEEE P1583 Special Task Group 3
Chair, Voter Registration Committee, Voter March Ltd.
1563 Solano Ave. #434
Berkeley, CA 94707
voterregistration@votermarch.org

cc: Lou Posner, Esq. (Executive Director, Voter March Ltd.)

[†] I use this example because redundant storage is often cited as a reason for confidence in voting equipment.