Memorandum

To: Election Assistance Commission (EAC)
EAC Technical Guidelines Development Committee (TGDC)

From: Stanley A. Klein
sklein@cpcug.org
301-881-4087

Date: December 17, 2004

Subject Voting machine reliability and synopsis of comments to IEEE P1583 Draft 5.3.2

This memorandum discusses my comments on voting machine reliability made to IEEE P1583 draft 5.3.2, and provides a summary of my other comments to the draft. Sections 5.2 and 6.2 of the draft contain a statement that they are being revised. With little time remaining for review, the revisions have not appeared. These comments are based on the original text of the draft.

The reliability requirements of P1583 are substantially the same as those in the 1990 and 2002 Federal Election Commission (FEC) standards. In the 2004 general election, several citizen groups sent volunteer observers to polling places to record problems with voting machines and election administration. The problems with P1583 are well correlated with the observed results.

Reliability testing requires sufficient test time to obtain statistically valid results. The P1583 draft explicitly states (in 6.2.2) that reliability testing will be performed in conjunction with other testing. It appears that rather than determine a proper reliability standard for voting machines, the P1583 draft and the FEC standards are based on capping the reliability testing at the duration of the other testing and setting the reliability standard at what can be accommodated under the cap. The result is a requirement for Mean Time Between Failures (MTBF) of 163 hours .

The P1583 draft correctly states that the reliability model is “constant hazard rate” with time between failures distributed according to the Exponential Distribution, and that multiple machines can be operated simultaneously to obtain the required test time. For this model, and the 163 hour specified MTBF, the resulting failure probability is 1/163 per hour of machine operation. For a 15 hour election day, the probability of a machine failing is 9.2% (reliability of 90.8%) . To illustrate, if fewer than 1472 of Maryland's 16000 voting machines fail on election day, observably or unobservably, the system satisfies the reliability requirement.

The standard specifies that a failure is any loss of function or any performance degradation lasting more than 10 seconds. Thus, a touch screen misalignment (“calibration”) failure, that causes the machine to appear to switch a voter's entered choice among candidates, is a machine failure. Although the standard states a more appropriate standard for availability than for reliability, it uses a continuous service model for calculating availability. Such a model does not apply well to a situation in which there are dispersed sites, limited repair personnel, and a short duration during which the devices at the sites must operate correctly. In addition, polling place repair of voting machines raises a concern about possible tampering by machine technicians. My proposed change would set the MTBF at 15000 hours (for 99.9% election day reliability) and assess availability assuming voting machines are non-maintainable during election day.

Election day provides a very extensive test of voting machine reliability. TrueVote Maryland had observers in 108 of Maryland's 1787 precincts during the 2004 general election. The observers reported 201 "machine-related" problems in a number of categories. I reallocated the categories to identify specific voting machine failures on election day. For example, failures of the smart card encoder, while they are overall system failures, were not allocated to voting machine failure. Also, candidates and other contests/issues missing from the ballot were reallocated as a machine failure during election setup, not election day.

After reallocation, the total election day machine failures were 111. Providing 16000 machines for 1787 precincts gives an average of 8.95 machines per precinct. Multiplying by the number of precincts covered gives 967 machines observed. Having 111 election day failures in 967 machines is a failure probability of 11.4%. Considering statistical variability and the uncertainty in categorization, this is reasonably close to the FEC/P1583-allowed failure probability of 9.2%. Note that allowing 1472 failures in 1787 precincts means that, within the standards, over 80% of precincts can experience an observable or unobservable voting machine failure.

The reallocation of candidates and other contests/issues missing from the ballot as setup failures provided an opportunity to clarify a usage scenario stated in the FEC standards and the P1583 draft. There were 16 such failures reported, giving a failure rate of 1.65%. The standard states a scenario that has pre-election activity requiring 30 hours. The calculated failure rate implies a time of 2.7 hours, consistent with an overall pre-election setup time of about 3 or 4 hours. It appears that the 30 hours may be for a machine used in Logic and Accuracy testing, and that a setup time of 3 or 4 hours more reasonably applies to other machines. This was confirmed in a discussion with an election administration office prior to preparing the relevant comment.

The reliability test cap issue is repeated more explicitly in the area of voting system accuracy. The accuracy requirement is a maximum of one error in 10 million ballot positions, which seems appropriate. However, this is stated as a meaningless "target" rather than a firm requirement. The test specification, which is firm, is for one error in 500,000 ballot positions, an error rate 20 times worse than the "target". Also, the standard is ambiguous regarding whether the accuracy must be maintained even if the machine fails, i.e., fail-safe retention of previously cast ballots. My comment would make the "target" the firm requirement, and require fail-safe accuracy.

Some of my other important comments would:

- Require a systematic search for security vulnerabilities, and penetration testing that assumes a technically-sophisticated, highly-motivated, well-financed attacker per 5.1.2.3.
- Prohibit systems from using short-range optical communications within the polling place unless optical access to machines by other optical-capable devices is physically blocked.
- Require that randomization of ballot storage be based on random events and not just on pseudo-random number sequences that can facilitate matching of voters and their votes.
- Require that machines that encounter limits, such as storage or maximum counts, stop accepting voting sessions and produce alarms, and requiring that limit behavior be tested.
- Require that any device used to validate voting machine software integrity pass all tests, other than voting machine functionality, required of voting machines.
- Define a default logic for straight ticket voting that allows the voter to select the straight ticket choice and then make changes. This corrects an issue that caused problems in 2004.