Written Testimony of Howard Stanislevic

Nov. 21, 2006

Dear Commissioners, Mr. Ravitz and Mr. Gonzalez,

We have heard quite a lot about how New York's attempt to adhere to the latest (2005) version of the EAC's Voluntary Voting System Guidelines (VVSG) will safeguard electronic vote counting systems that may be certified by the State Board of Elections. However, most experts agree that the federal standards should never be relied upon exclusively. For one thing, in those very standards, the EAC and its predecessor NASED have granted themselves the right to certify non-compliant voting systems. Volume II, Appendix B.5, Qualification Test Results and Recommendation clearly states:

"Of note, any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection."[1]

Since there is no way to know in advance if a particular deficiency will "involve the loss or corruption of voting data", almost none of the requirements in the VVSG actually have to be met for systems to be federally qualified. Therefore, it's really up to the states to do their own due diligence.

One might reasonably ask if any non-compliant voting systems have actually been certified and the answer is a resounding "Yes.":

1. For example, design flaws in the federally certified Diebold AccuVote TS and TSx DREs' software upgrade feature allow the boot loader, the operating system and the application software to be completely replaced simply by booting these machines from a corrupted memory card or network server, completely altering the machines' programming without detection. According to Michael Shamos, a computer scientist and voting system examiner for the State of Pennsylvania, "It's the most severe security flaw ever discovered in a voting system." But these systems were certified anyway.[2]

2. In Maryland, the recently published Freeman, Craft and McGregor report has confirmed that Diebold's code cannot be independently verified once it's been loaded onto the DRE. This may be due to the boot loader vulnerability noted above, but could also be due to the presence of self-modifying code, which would be another standards violation. But these systems were certified anyway.[3]

3. ES&S's application software appears to be unverifiable as well once an election definition file is loaded onto their voting systems because that file makes changes to the application software when loaded. To comply with the VVSG, every ES&S system would have to be recertified

---

[1] H. Stanislevic, VoteTrustUSA, "Gaping Hole in HAVA Voting System Standards Widened in 2005",
http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1299&Itemid=26
[2] D. Dill, D. Jones and B. Simons, "The Diebold Bombshell",
http://www.opednews.com/articles/opedne_david_di_060723_the_diebold_bombshel.htm
[3] Freeman, Craft, McGregor, "Report from a Review of the Voting System in The State of Maryland",
http://www.elections.state.md.us/pdf/maryland_report.pdf

before every election. But these systems remain certified anyway.[4]

4. The Diebold AccuVote OS optical scanner has been found to have interpreted (human readable) code on its memory cards which allowed a team from the University of Connecticut to hack into the scanner with a laptop PC, neutralize candidates so that their votes are not counted, swap the votes of two candidates, or bias the results by shifting some votes from one candidate to another -- all without even removing the memory card from the scanner. This, along with the huge insider risks inherent in any electronic vote counting system, have prompted the State of CT to conduct a 20% hand count of their optical scan systems this year, among other safeguards.[5, 6]

If the federal standards meant anything at all, none of the above systems would have been certified. And these are only some of the standards violations we know about.

There is also the issue of the absurdly lax hardware Reliability spec of only 163 hours Mean Time Between Failures in the federal standards.[7] This allows 1 in every 11 DREs or scanners to fail either partially or completely in any 15-hour election day. This is one standard that should not be hard to comply with because it allows almost 10% of all DREs and scanners in the nation to fail on Election Day and is tantamount to a denial of service attack on our entire election system. Nevertheless, some DREs have been shown to exhibit even higher failure rates in actual elections and volume tests conducted by the State of California. Imagine the chaos, queuing and disenfranchisement that would ensue if this were to occur in New York City on your watch -- especially with DREs (without which voters would not even have access to the ballot).[8]

By contrast, we know from the 2004 election that our 40+ year-old lever machines have much higher reliability than mandated by the VVSG, and they are much easier to repair in a timely manner by your own trained lever machine technicians.[9] This is one reason why the State of New York had only a 0.77% undervote rate for President in the 2004 general election, which rivals that of any electronic vote counting system in service today.[10]

In light of the above deficiencies, the best answer for New York is to do as little as possible to comply with HAVA. This means providing one accessible ballot marking device per polling place as ordered by the judge in the DoJ's lawsuit while retaining all our lever machines. This will result in a fully HAVA-compliant voting system, as defined by HAVA Sect. 301, ERMA 2005 Sect. 11, New York Election Law Sect. 7-202 and Sect. 7-200 which allows any Board of Elections to have up to two voting machines or systems in operation concurrently in any election.

---

[4] J. Washburn, "ES&S Programming is Unverifiable", http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1475&Itemid=51

[5] A. Kiayias, L. Michel, A. Russell, A. A. Shvartsman, Univ. of Connecticut, "Security Assessment of the Diebold Optical Scan Voting Terminal", http://voter.engr.uconn.edu/voter/Reports.html

[6] G. Barnett, TrueVoteCT, "Audits in Connecticut", http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2054&Itemid=113

[7] R. Mercuri, "DREs – Designed for Failure", http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1851&Itemid=26

[8] W. Edlestein, New Yorkers for Verified Voting, "New Voting Systems for New York - Long Lines and High Cost", http://www.nyvv.org/doc/voterlines.pdf

[9] Stanislevic, "DRE Reliability: Failure by Design?" http://www.votetrustusa.org/pdfs/DRE_Reliability.pdf

[10] Election Assistance Commission, "2004 Election Day Survey", Chapter 8, "Overvotes and Undervotes", http://www.eac.gov/election_survey_2004/toc.htm

To achieve this, the City should return the $4,000 per Election District of HAVA Title I funds, retain all lever machines, and purchase the additional ballot markers with Title II funds, which are the lion's share of the HAVA money anyway. This is exactly what is being proposed in our neighboring counties of Nassau, Suffolk and Westchester and they are willing to go to court to do it. By rushing into electronic vote counting, we will be bucking the downstate trend and taking a huge, unnecessary and expensive risk.

The only reasonable alternative to retaining the levers is to follow the lead of Connecticut and use PB/OS with rigorous hand counts of enough paper ballots to confirm the outcome of every race on the ballot.[11] Regulations to govern such audits are currently being drafted by our State Board and will likely result in much higher percentages of hand counts than the 3% minimum required by law. If you replace lever machines, you must be prepared to abide by such rules, as they will be the only way to ensure that the outcome of our elections are correctly decided by electronic vote counting systems.

---

[11] Stanislevic, "Random Auditing of E-Voting Systems: How Much is Enough?", http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf