Voting System Certification: Who’s Minding the Store?

(January 09, 2007) - Contributed by Howard Stanislevic, VoteTrustUSA E-Voter Education Project

Iin Jan. 2005 at a meeting of the EAC’s Technical Guidelines Development Committee (TGDC), Resolution # 27-05 was passed in an attempt to close a giant loophole in the federal voting system qualification standards. These standards are known as the Voluntary Voting System Guidelines (VVSG), although they are voluntary only in the sense that the States are free to disregard them and develop their own standards if they so choose.

The loophole, which appears in Volume II, Appendix B.5 of the 2002 version of the guidelines states that any uncorrected deficiency observed in the qualification test results that does not involve the loss or corruption of voting data is not necessarily cause for rejection of a voting system. This loophole means that the EAC and the nongovernmental agency that qualified voting systems to these standards through July, 2006, the National Association of State Election Directors (NASED), were free to disregard any part of these standards, except for the accuracy (error rate) spec which is also a statutory requirement of Section 301 of the Help America Vote Act (HAVA).

The TGDC’s resolution recommended either the deletion of any requirements frequently not met by voting systems, or the closure of the loophole that allowed certification of non-compliant systems in the first place. Curiously nearly two years later, in the new version of the standards (which HAVA required the EAC to develop), the loophole still exists. This raises the question of which voting systems, theoretically qualified to the standards, might in fact not comply with the standards, and to what extent. Since the certification process is largely a clandestine one, this remains an open research question.

Meanwhile, certain high profile “hacks” of the Diebold Accuvote touch screen and optical scan systems, as well as hardware and software problems which caused the former machines to crash frequently, have indicated that at least one vendor is not in compliance. Michael Shamos, a professor of computer science at Carnegie Mellon University and adviser to the Commonwealth of Pennsylvania on electronic voting, said of the AccuVoteTS DRE’s security flaw reported last year by Finnish computer scientist Harri Hursti was so bad that, "Any losing candidate could challenge the election by saying, 'How do I know that the software on the machine is the software certified by the state?'"

Revelations about other vendors’ noncompliance may follow, but the question also arises as to whether NASED has been giving voting systems that do not comply with the standards a pass by using the loophole that the EAC has preserved for itself and whether the so-called “Independent Testing Authority” (ITA) laboratories have been failing to adequately test systems in accordance with those standards. The experience of one state (New York) with one ITA (Ciber, Inc.) may shed some light on these questions.

Despite copious evidence of electronic voting problems across the country, New York has been roundly criticized even by some of its own legislators, for being the last state in the nation to fully comply with HAVA. A remedial order by the judge in the Dept. of Justice’s lawsuit against the state required New York to produce a plan to replace its lever machine voting systems with HAVA-compliant voting systems at each polling place by Sept. 2007. The state complied by producing a detailed schedule for certification of both direct recording electronic voting systems and optical scan electronic vote counting systems in addition to some previously state certified electronic paper ballot marking devices for voters with disabilities.

The state had chosen Ciber, Inc. to conduct certification testing on its behalf including the production of two project plans known as the Master Test Plan and the Security Master Test Plan. New York requires voting systems to comply with State Election Laws, the EAC’s 2005 VVSG and Voting System Standards issued by the State Board of Elections.

The state also hired NYSTEC, a nonprofit spin-off from the US Air Force's Research Laboratory at Rome, NY, to conduct an independent review of Ciber’s Security Master Test Plan.

On Sep. 27, 2006, NYSTEC issued its first report, which was highly critical of Ciber, stating that the ITA's test plan for the state's new voting systems lacked numerous security and functional testing requirements of the 2006 NY State Election Law, the EAC's 2005 Voluntary Voting System Guidelines Vols. 1 & 2, and NY State's Voting System Standards. In fact, in addition to the security test plan, NYSTEC also found it necessary to comment on Ciber’s functional test plan due to numerous omitted requirements.

According to NYSTEC, some of the items omitted from the plans were: - a requirement for voting systems to not include

any device or functionality potentially capable of externally transmitting or receiving data via the Internet, radio waves or other wireless means;

- a requirement for the voting system software not to contain any ‘viruses’, ‘worms’, ‘time bombs’, and ‘drop dead’ devices that may cause the voting system to cease functioning properly at a future time;

- a requirement for voting systems to provide a means by which ballot definition code may be positively verified to ensure that it corresponds to the format of the ballot face and the election configuration. Furthermore, Ciber’s Security Master Test Plan did not specify any test methods or procedures for the majority of requirements. Ciber stated that these would be provided in another phase of the project.

On Nov. 2, 2006, amidst continuing delays in the certification process, NYSTEC issued a second report entitled “Analysis of Changes to the Electronic Voting Machine Implementation Timeline”. Here are selected excerpts from that report:

During late August and September 2006, SBOE worked with the selected Security Testing Vendor (CIBER) to firm up a schedule for creating security testing plans and security certification testing….SBOE continued to hold weekly status meetings to monitor the timeline and continually followed up with each voting machine vendor to request the necessary equipment, software, documentation, and funding for testing. Despite repeated phone calls, emails, and letters, not one voting machine vendor was able to send in a complete submission during August and September.

Unanticipated delays in completing security test plans. In spite of the delay in deciding what machines would be tested, the prime security vendor, CIBER, began creating a draft security master test plan, which was scheduled to be completed by 9/14/06. The timeline assumption was that CIBER would include all required security regulations in its first draft so the independent review would not need to recommend substantial changes. This did not turn out to be the case. NYSTEC recommended a substantial number of security requirement additions to both the security master test plan and the overall master test plan (which covered both non-security and security test plans). The timeline assumption was three days for CIBER to make final revisions. CIBER actually completed the next security test plan revision on 10/9/06, taking 9 days.

NYSTEC did a second independent review of what was thought to be the final version of the security master test plan and noted that a large number of security requirements were still missing. During a conference call with SBOE, CIBER, and NYSTEC to discuss the situation on 10/11/06, it was decided that CIBER would travel to Albany the following week to work with NYSTEC for two solid days to resolve the document deficiencies. During these meetings, on 10/18 and 10/19, NYSTEC documented and discussed more than 200 security requirements that still needed to be added to the latest documents. CIBER estimated the changes would be completed by 10/24. The latest revision was received on 10/25 and is currently being reviewed by NYSTEC. The initial estimate for making final revisions to the master security test plan was three days. So far, it has taken 18 days (9/28 to 10/24), and NYSTEC is still checking to be sure that the latest revision includes all necessary security regulations. Also during the two-day meeting and subsequent discussions between CIBER and NYSTEC, a new timeline for security planning and testing was created.

Because of the delay in identifying what machines to test and the amount of time it actually took to finalize a master test plan, the ending date for security certification has now moved from the 12/12/06 estimate in the revised timeline (in September 2006) to February 2007. All of the above took place before New York learned of the EAC’s recent denial of interim certification to Ciber.

Unlike NASED and the EAC, the New York State Board of Elections has actually been requiring compliance with the voting system standards and not invoking the giant loophole noted above. This experience shows that when voting system laws and regulations are actually taken seriously, the certification process is a lot more rigorous than what the ITAs have become accustomed to while working only for the vendors with only election integrity advocates minding the store.