Written Testimony by Rebecca Mercuri
mercuri@acm.org 609/587-1886
Representing: The BRAD BLOG
Voting Advocates Roundtable Discussion
EAC Offices, Washington, DC, April 24, 2008

The 2007 draft Voluntary Voting System Guidelines (VVSG) represents a significant departure from earlier Federal voting system guidelines (2005 EAC, 2002 and 1990 FEC), while still retaining much of the certification framework that has been increasingly demonstrated to be problematic. Within the guise of certification, the past few years have seen billions of Federal and State tax dollars squandered on the purchase of voting systems that were subsequently revealed as inappropriate for use, and then discarded. We now know that the VVSG, and its ITA testing program, provide no assurance of process or equipment correctness, either to those who are making procurement decisions, or to the citizens who must entrust their votes to these systems. Tragically, the net result of this false validation has led to further erosion of voter confidence in elections.

This draft VVSG continues to perpetrate this scam. Among other changes, it recognizes earlier shortcomings of the certification process (especially in the areas of voter verification, transparency, auditability and security) by introducing an innovation class that allows for the submission of novel voting system paradigms for certification, and provides for the (somewhat related) adoption of a software independence requirement. Unfortunately, both of these concepts are oxymorons in the context of voting system specifications. Here's why. If a construct is truly innovative, the existing guidelines will not be able to appropriately address it, hence the resulting certification may be flawed or the implementation of the new design may necessarily be impeded by a lack of understanding as to how to properly perform certification. A system that contains software can never be software independent, even within the TGDC/NIST's constrained definition that ties undetected changes or errors in software to election outcomes. Any software in the system necessarily affects a whole host of voting attributes that can affect election results, irrespective of undetected changes or errors.

Furthermore, neither the innovation class nor the software independence requirement are satisfiable due to legacy constraints imposed by the certification process. This is, at least in part, because the 2007 draft VVSG (like its predecessors) masquerades as a functional standard, while actually continuing to be predisposed to existing designs. Even the TGDC's description of the innovation class makes design assumptions, such as its limiting "expect[ation that] most technologies in this class [will] be based on multiple mutually auditing components." But even as a design specification, the draft VVSG falls short of achieving its goals of specifying "how voting systems should perform or be used in certain types of elections and voting environments." This is because the guidelines repeatedly make the erroneous assumption that insiders (i.e. vendors, repair personnel, election officials, etc.) are trusted agents in the highly partisan process of US elections. In reality, insiders have both motive and opportunity to make changes and cover up the fact that they have done so. Where errors have been blatantly obvious, vendors go to great lengths (including lawsuit threats) to prevent independent examinations of equipment architecture and computer code. Some election officials have improperly conducted audits in order to avoid revelation that problems have occurred "on their watch." In sum,

virtually all of the checks and balances that are specified by the VVSG fail to take insider attacks into sufficient consideration. Voters believe that elections are inherently corrupt, and the VVSG does nothing to allay these fears.

Nor are the VVSG's specified controls transparent enough to allow verification by the voter that the election system they are using has been configured properly. Production of a voter-verified paper ballot is utterly moot if vote totals are generated electronically and never checked against the original paper. Recent literature has suggested random audits (or spot-checks), but since these percentages are based on the computer-generated results, they grossly underestimate the amount of independent tallies that must be performed to sufficiently validate the election. These checks are not prescriptive as to what to do when anomalies are revealed. Courts have been reluctant to dismiss election results, even in the extreme, such as when over 80% of the precinct ballot counts differ from the number of signatures in the polling books and the vendor has admitted to deploying an uncertified configuration of voting system components in violation of State requirements (ref. the 2006 Franklin County, Ohio recount case of Carole R. Squire vs. Christopher J. Geer).

In these matters, it generally falls to the contestor to prove that anomalies affected the results in such extent that, had they not occurred, the outcome would have been different. And the contestor must make this proof in the absence of access to the voting equipment or test results, since vendors and ITAs are allowed to claim trade secrecy protection for their materials. The 2007 draft VVSG further perpetuates this trade secrecy loophole (as had prior versions of the guidelines) by continuing to exempt COTS (commercial-off-the-shelf) products (including those with critical underpinnings such as device drivers and operating systems) from source code inspection and other standard reviews. This lax and dangerous view of COTS products is most evident in the fact that these are never required to be updated, even when new versions are issued to remedy known security risks.

One might think that, at least, if a voting system (or any of its components or modules) was found to be defective, or if the testing was discovered to have been improperly performed or deemed inadequate, there would be some process whereby the EAC would be required to withdraw certification. But the 2007 draft VVSG (like its predecessors) omits mention of any methodology whereby certification can be rescinded because of later-discovered flaws. The VVSG thus provides no protection to either the purchasers or the voters, since perversely, there is a disincentive for vendors to issue corrections to deployed systems, because any changes (even necessary ones) require costly recertification. The Catch-22 scenario is that you can continue to use defective voting machines, but you may not be able to obtain versions that have had the defect corrected. This situation must stop.

Most of the above issues are well-known and have been reported to the EAC in its various incarnations, by many people (including myself and Brad Friedman), numerous times. The 2007 draft VVSG continues the tradition of providing a set of straw hurdles that must be jumped over (or skirted around) in order to attain certification, while resulting in no true assurances. Another VVSG rewrite, novel designs, or more extensive testing cannot begin to solve these problems until the voters' demands for transparency, reliability, security, accuracy and auditability requirements have first been appropriately defined and addressed. So long as the goal of certification trumps the need to ensure election integrity, the resulting systems, no matter whose imprimatur they bear, will be invalid and must be rejected.