To: The U.S. Election Assistance Commission
From: Rebecca Mercuri, Ph.D. 609/587-1886 mercuri@acm.org
Subject: Comment on the 2009 Draft VVSG
Date: September 28, 2009

This document is provided in response to the public call for comment for the draft revisions to the 2005 Voluntary Voting System Guidelines.

By means of introduction, I am a computer scientist/engineer who has researched, written, and testified on the subject of electronic voting since 1989. My testimony on this topic includes appearances before the U.S. House Science Committee, the U.S. Election Assistance Commission, the U.S. Commission on Civil Rights, the U.K. Cabinet, various State Legislative Committees (in CT, MD, PA, VA, NY and NC), and court proceedings (in NJ, FL, OH, CA and MI). I have directly influenced the wording of Federal, State and international election legislation, especially as it pertains to voter verified ballots and independent auditing of election results, and have provided comment to the EAC and FEC on the earlier 2002, 2005 (draft) and 2007 (draft) VVSGs, as well as participated in the IEEE voting standards work that was consulted during the construction of the 2005 and 2007 (draft) VVSG.

The 2007 (draft) Voluntary Voting System Guidelines (VVSG) represented a significant departure from earlier Federal voting system guidelines (2005 EAC, 2002 and 1990 FEC), while still retaining much of the certification framework that had been increasingly demonstrated to be problematic. Among other changes, that version attempted to recognize earlier shortcomings of the certification process (especially in the areas of voter verification, transparency, auditability and security) by introducing an innovation class that allowed for the submission of novel voting system paradigms for certification, and provided for the (somewhat related) adoption of a software independence requirement. Unfortunately, these concepts fell short of their intended purpose and instead provided a fast-track backdoor whereby a new generation of experimental, unproven, electronic voting systems could be foisted on the voting public, without thorough examination.

Although this 2009 (draft) VVSG appears to have eliminated the use of the earlier Orwellian phrase “software independence,” which was an impossibility, since there is no way to assure that a system that uses software can somehow be, in part, independent of it. Yet this “independence” concept still persists in the 2009 draft, this time under the name “Independent Verification” (IV). Unfortunately, the description of an IV system given in Volume 1, Section 7.8 is incorrect in many respects, far too numerous to detail here (I would offer to visit to elucidate further, please contact me at your earliest convenience to arrange a meeting). Briefly, there is nothing secure about duplicate cast vote records, not even if one set is copied to unalterable storage media. That “both records are not under the control of the same system processes” does NOT make them independently verifiable BY THE VOTER (since the voter cannot directly read the electronic records).

There is also a very dismaying corruption of the phrase and concept of "Voter Verifiable Paper Audit Trail" (VVPAT), which alters its application and intention. The ballots that voters cast are just that, ballots, NOT an audit trail. For there to be an audit trail, there would have to be an end-to-end record of all transactions on the voting system throughout the election, and the need for privacy precludes this implementation. The phrase should be "Voter Verified Paper Ballot" (VVPB), which would recognize the legal status of any paper artifact that the voter VERIFIED as the actual BALLOT OF RECORD. There must be a casting action that is performed by the voter that is used to signify that they have indeed VERIFIED the ballot as correct. Without a true verification requirement, it is insufficient to have an audit trail that may or may not have been verified, since then, in a duplicate recording system, the audit trail will always necessarily be deemed unreliable.

Along this vein in this draft, cryptographic voting now appears to be increasingly relied upon to ensure "independence." Yet the status of cryptographic voting is completely dubious at this time, as it is a concept in its infancy, being promoted well beyond the capabilities that have been proven thus far by certain over-zealous scientists. Among its many flaws is the fact that none of the extensive literature on this subject has properly addressed the provability of IMPLEMENTATIONS of cryptographic voting algorithms, which is a daunting task, as yet unsolved. Nor does waving of the cryptographic wand over certain aspects of the system provide any assurance to the voter that the implementation in place on the system is actually the version that was certified for correctness (this is actually true, as I have commented before, of all software in voting systems). In fact, the necessity for the concept of "trustees" in many of the cryptographic voting systems proposed to date, provides an area of unresolvable uncertainty. Here again, special interests appear to have prevailed to create a climate favorable to a method that has not yet been demonstrated to be viable in voting systems. In short, touchscreen voting again, just in the new cryptographic version thereof. The public will not deem this acceptable.

Another of the troubling perpetuations in this draft is the exemption for unmodified COTS components from certain portions of system certification testing. It is universally agreed in the computer science community that there is nothing about a COTS product (including card readers, printers, personal computers, operating systems, programming language compilers, and database management systems) that inherently makes it secure or even ensures that it is functioning properly or appropriately. As I (along with Vince Lipsio and Beth Feehan) wrote in "COTS and Other Electronic Voting Backdoors" (Communications of the Association for Computing Machinery, November 2006):

> In other critical computer-based devices (e.g., medical electronics or aviation) COTS components may be unit tested a single time for use in multiple products, with COTS software typically integration tested and its source code required for review. In contrast, for voting equipment, this blanket inspection exemption persists, despite having strenuously been protested by numerous scientists, especially in the construction of guidelines authorized by the Help America Vote Act (HAVA). Nevertheless, special interests have prevailed in perpetuating this

> serious backdoor in the advisory documents used for the nation's voting system testing and certification programs.
>
> That uninspected COTS has caused other serious voting equipment problems to go undetected, even without tampering, was reported in 2001 to the U.S. House Science Committee by Douglas Jones, when he related a 1998 example of "an interesting and obscure failing [with the Fidlar and Chambers EV 2000] that was directly due to a combination of this exemption and a recent upgrade to the version of Windows being used by the vendor ... the machine always subtly but reliably revealed the previous voter's vote to the next voter."

Although the 2009 draft appears to clear up a number of prior vagaries pertaining to what is or isn't COTS, unfortunately the EAC, TGDC, and NIST have continued, in this draft, to fail to recognize the strong vulnerabilities that exist through the blanket exemption for unmodified COTS. Without end-to-end examination, voting systems will remain at risk.

I was heartened to see that, finally, a more appropriate definition of reliability has finally been proposed (Vol. 1, Section 4.3.3). But the stated failure rates in the table on page 119 seem to me to be rather peculiar, since the numbers given are unexplained, and have different orders of magnitude (hence imposing different levels of accuracy). The effects of these collective failure rates, independently and in combination, needs to be more appropriately addressed. I suspect that the given numbers still fall short of the desired intention, that voters shall not have their ballots lost or be electronically disenfranchised.

My overall comment is that this 2009 draft VVSG continues to perpetuate seriously erroneous concepts that do not actually improve or assure the reliability, accuracy, and integrity of the voting system, while the draft also continues to shun the necessity of end-to-end security, entirely independent verification by the voter of the ballot of record, and true transparency of the ballot creation, casting and counting process. With the consolidation of the two largest US voting system vendors into one single entity, now serving over 80% of the country, the need for these goals to be properly instantiated in the VVSG has dramatically increased. The fact that these guidelines remain inappropriate is unacceptable to the American public. I hope that this will someday change, but the time has apparently not yet come. Again, I offer my willingness to assist in elucidating these issues further. Please feel free to contact me for further information.