To: The U.S. Election Assistance Commission
From: Rebecca Mercuri, Ph.D. 609/587-1886 mercuri@acm.org
Subject: Comment on the 2007 Draft VVSG
Date: May 5, 2008

This comment is intended to augment the formal remarks I submitted pertinent to the 2007 Draft VVSG at the April 24, 2008 Voting Advocate Roundtable discussion (see <http://www.eac.gov/News/docs/mercuritestimonyapr08/attachment_download/file>).

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 and 2005 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) 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. Among other changes, it appears 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 allows for the submission of novel voting system paradigms for certification, and provides for the (somewhat related) adoption of a software independence requirement. Unfortunately, these concepts fall short of their intended purpose and instead provide a fast-track backdoor whereby a new generation of experimental, unproven, electronic voting systems can be foisted on the voting public, without thorough examination.

In particular, the definition of software independence proposed by MIT's Ron Rivest and NIST's John Wack allows computational cryptographic systems that do not necessarily include voter verified paper ballots to be certified for use in elections. This provision for the introduction of cryptographic solutions is also evident in the use of the incorrect phrase "voter verifiable" rather than the appropriate term "voter verified" throughout the draft. A "verifiable" ballot can never actually represent the true intention of a voter. Only when a ballot has been "verified" via independent examination and a deliberate casting action, can it contain a legitimate record of the voter's choices. Cryptographic ballots cannot satisfy these constraints. Nor can a voting system that includes software in any stage, ever be considered "software independent" since it is always vulnerable to a whole host of unresolvable software-related issues, including malware and denial of service attacks, as well as unintentional misprogramming, all of which can alter the outcome of an election (although not necessarily within the Rivest/Wack constraints).

Following the revelation of serious equipment shortcomings via independent state-authorized testing of previously federally certified equipment, election integrity advocates and citizens have increasingly and adamantly insisted on transparency, independent auditability, and voter verification in the election process. But the 2007 draft VVSG, through its perpetuation of the legacy COTS exemption from source code examination, continues to allow voting systems to be shrouded in secrecy while also circumventing salient portions of the testing process via the innovation class. There is no need for the COTS exemption, since operating systems, language compilers and application software (such as databases and spreadsheets) have all existed in the open source libraries for over two decades. As well, vendors have always had the option of protecting their proprietary interests by copyrighting and patenting their intellectual property, rather than insisting on trade secrecy.

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) continues to leave the methodology whereby certification can be rescinded because of later-discovered flaws to the EAC. Safety is not assured via the open-ended testing, since the VVSG provides no method whereby later-detected flaws initiate reexamination. Perversely, there is even a disincentive for vendors to issue corrections to deployed systems, because any changes (even necessary ones) require costly recertification. Nor does the draft address the matter of subsequently identified vulnerabilities in the uninspected COTS components, by requiring ongoing updates and integration testing.

The limitations and flaws of the 2007 draft VVSG (like its predecessors) are primarily due to the fact that it masquerades as a functional standard, while actually continuing to be predisposed to existing designs. 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.

Nor are the VVSG's specified controls transparent enough to allow verification by the voter or the election officials that the election system 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 records. 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. As well, these checks are not prescriptive as to what to do when anomalies are revealed.

In sum, the 2007 draft VVSG is flawed end-to-end, and is even more dangerous than its inadequate predecessors. It should be scrapped and a complete rewrite performed.