To: U.S. Election Assistance Commission
From: Rebecca Mercuri, Ph.D.
Subject: Voting System Guidelines Comments
Date: September 30, 2005

The draft version of the Voluntary Voting System Guidelines (VVSG) under consideration for adoption by the U.S. Election Assistance Commission (EAC) fails to achieve the necessary goals of insuring reliability, auditability, and transparency for election equipment. These were the salient aspects of the Florida 2000 Presidential election, and the subsequent Florida 2002 Gubernatorial primary, that led to the formation of the EAC and the construction of the VVSG under the auspices of the Federal Help America Vote Act (HAVA). Voters wanted then, and still want to know now, whether their ballots are being cast as intended, counted as cast, and available for an indisputable and independent recount. This VVSG does not provide the citizenry, the election officials, nor the courts, with the capability of determining that such assurances are now in place. Rather, the authors of this new set of guidelines, by their own admission, chose to instead "address the critical topics of accessibility, usability, and security" but have failed to accomplish these goals as well.

In light of the fact that there is no time for the EAC and its sub-committees to provide the massive overhaul that this document would require, my recommendation is that it be issued only as a draft, along with a detailed list of the areas that must be further addressed, and an admonishment to its potential adopters that the proposed "National Certification" process does not provide sufficient assurances of accuracy, integrity, reliability, usability, accessibility, security and transparency for the equipment and systems used to conduct democratic elections.

My discussion below itemizes some of the most egregious issues with the VVSG and sheds light on the problematic construction of the document itself.

VVSG's flaws as a legacy standard

The VVSG was constructed within the legacy of the Federal Election Commission's 1990 and 2002 Voting System Standards, along with input from other election equipment guidelines (such as the IEEE P1583 draft standard), many of which were also based upon the FEC work. As such, the VVSG repeats many earlier mistakes of these standards in both content and structure. Foremost among its problems is that the VVSG, like its predecessors, sits somewhere between being a design standard and a performance standard, and by failing to determine which direction it intends, provides only mediocrity for either purpose. Although the VVSG purports to "define functional requirements and performance characteristics that can be assessed by a series of defined tests," in actuality, it relies heavily on pre-existing balloting metaphors, and thus is implicitly predisposed to the assessment of only a limited set of designs. For such designs, it attempts to cover a multitude of bases, offering guidance for disparate sets of equipment that must satisfy mutually incompatible constraints. For example, the usability requirements for ballot casting are necessarily different, in many regards, for paper-based, electronic, and electro-mechanical systems, but the VVSG chooses to convolve the human factors

aspects of all of these products into a confusing mish-mash of criteria. As a performance (or functional) standard, the VVSG is overly prescriptive in terms of acceptable manifestations, hence it harbors the potential of discouraging or even thwarting the development and deployment of viable designs that have not heretofore been considered. Thus, the VVSG perpetuates vagaries over acceptability for use of unaddressed configurations. This omission has knowingly been exploited by certain lobbying groups through attempts to defeat the adoption of competitive innovations (like voter verified paper ballots intended to increase auditability and transparency, and overlay templates to improve accessibility) or alternatively, has served vendor interests with allowances for the uncertified introduction of new components with dubious security (such as telecommunications products).

Failure to adequately mitigate insider risks

Elections exist in an inherently adversarial environment where insiders have both opportunity and motive. One need only look to the history of the United States to find considerable and ongoing evidence of election-related corruption, as illustrated just this week with the indictment of the House Majority Leader under suspicion of campaign finance violations. Yet the VVSG takes the approach of focusing its entire set of risks assessment and mitigation controls (as described in Volume 1, Section 6) on processes that primarily fall under the auspices of potentially partisan vendors and election officials, without providing sufficient outside assurances that these processes are free from corruption. Take, for example, the distribution requirements, whose goal "is to ensure that the correct voting system software has been distributed without modification." Within the dozens of these requirements in Section 6.6.4 are none that allow a voter to confirm that the software deployed at the polling place is equivalent to that which was certified, nor any that enable a court to independently determine whether a voting system used during the time of the election had been configured inappropriately (since the configuration management requirements of Section 8 are similarly flawed). The certification process continues to be conducted at an insider level, with no requirements for open review of program code and system architectures, and no abolishment of the trade secrecy practices that allow vendors to shroud their products from scrutiny if litigation over election results ensues.

Massive exposure to outsider risks

The introduction of the use of telecommunications (as per Volume 1, Section 5) further compounds the nature of voting system risks far beyond that which has ever been seen or experienced in U.S. elections. The VVSG permits the use of telecommunications devices to provide access to critical data for voter authentication, ballot definition, vote transmission, vote count, and voter lists. The systems are allowed to be connected "across a broad range of technologies, including, but not limited to:" wireless, microwave, public telecommunications lines, and communications routers. Unfortunately, all such channels are not only highly vulnerable but provide avenues for insider as well as extensive outsider exposure to the election data and also potential access to the object code versions of the software running within the balloting and vote tabulation equipment. There is absolutely nothing in the standard that provides any real confidence or confirmation that

accuracy, durability, reliability, maintainability, availability, and integrity can be maintained for voting systems interfaced to telecommunications environments. The misguided encouragement for the use of such devices while simultaneously failing to mandate independent auditability features (such as voter verified paper ballots) can only be construed as either blatant naiveté or an astonishing roadmap for corruption of the election process on the part of the VVSG authors. The implication that all of these problems may somehow be mitigated through the use of cryptographic techniques is folly at best. It therefore is difficult to take any of this set of guidelines seriously, in light of this preposterous design flaw.

Miscellaneous topics

Voting system security continues to fail to be addressed in terms of the more stringent controls that are applied in a broad range of critical technology applications (such as military uses, banking, aviation, and health care). One would think that with NISTs role in the development of the VVSG, the use of their Common Criteria program would have been mandated at a level appropriate to the devices under consideration, but this was not imposed.

The reliability of voting systems can impact election results as well as ballot availability and enfranchisement. The legacy low Mean Time Between Failures, that allows for nearly a 10% equipment malfunction rate during election day, has been deemed unacceptable by members of the engineering community, such as Stan Kline (as per his comments submitted to the EAC). The MTBF level is currently set well below that which should be achievable by the vendors using present-day technology.

Certainly there is a need for a range of abilities and disabilities to be addressed by balloting systems, but to expect that all voters will satisfactorily address their individual needs using the same equipment poses a design constraint that has never been achieved by any application at this level of complexity. The amount of time required to use such devices in actual polling place environments has not been appropriately addressed by the VVSG. Nor does the VVSG provide any solution to accessibility for the millions of disabled voters who are unable to get to the polls but who would like to vote privately via absentee ballots. Universality may be more readily (and perhaps also more effectively) accomplished through disparate but equivalently effective assistive voting devices, which are not accommodated by the current structure of the accessibility and usability aspects of the VVSG.

Finally, I feel compelled to note that the composition of the Technical Guidelines Development Committee as well as the numerous panel sessions in hearings leading up to the issuance of the VVSG failed to adequately allow representation of various key individuals, both technical and non-technical, who had repeatedly articulated deep concerns over the methodologies and approaches of both the FEC 2002 and IEEE P1583 standards. The omission of these positions certainly contributed to the failure of the VVSG to accomplish the intentions promised by the HAVA legislation, and this is most unfortunate.