December 1, 2006

Dr. William Jeffery
Director, National Institute of Standards and Technology
Chair, Technical Guidelines Development Committee
100 Bureau Drive
Stop 1000
Gaithersburg, MD 20899

Dear Dr. Jeffery,

As Chair of the U.S. Public Policy Committee for the Association for Computing Machinery, I commend the TDGC's security subcommittee for its recommendation that require voting systems to be software independent as a condition for federal certification. Ensuring that voting systems are secure, useable, and reliable is critical for ensuring the integrity of our election process. The recommendations by the Security and Transparency Subcommittee (STS) of the TDGC are much-needed steps toward achieving these goals. We urge the TDGC, and ultimately the Election Assistance Commission, to embrace the recommendations as they develop the 2007 standards for voting systems.

As the use of electronic voting systems has become more widespread, the computing community has voiced its concerns about their security. This concern is rooted in years of experience in trying to build secure information technology systems. It is not possible to guarantee that any complex system is entirely secure. Testing can be done to evaluate a system's security; however, this testing is very different than standard conformance testing. In conformance testing, a system can be tested under normal conditions to evaluate whether it performs according to specific specifications. Security testing is more open-ended and while it may reveal some of the known vulnerabilities, it cannot predict how an attacker may misuse or insert a possible exploit of the system. In fact, massive human and financial resources are dedicated to making information systems more secure, but new vulnerabilities are revealed almost daily. We cannot expect voting systems to be any different.

Security and reliability vulnerabilities are not limited to those created by parties seeking to exploit a system. The known problems with voting systems in the most recent election resulted from unintentional errors or unforeseen complications of operating these complex systems. Utilizing software independent systems for voting machines helps to ensure not only that voting systems are more secure, but also that the election results from these systems are more reliable and trustworthy.

While a strategy of continually addressing security vulnerabilities may work for desktop computers at home, it cannot be adopted for e-voting machines. The integrity of our elections depends on these systems accurately collecting and counting votes. Clearly we must continue to make e-voting systems more secure, but given the shortfalls of security testing, it is our long-standing belief that voting systems should also enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and stored by the system. We are pleased that the subcommittee's paper clearly articulates this problem and recommends that voting systems must have an independent way of verifying a voter's intent. Further, that paper records represent the current best practice for creating these audit trails.

The recommendations of the STS are also carefully balanced as they address other key concerns about usability of paper ballots and continued research and development in this field. The computing community has consistently raised concerns about the usability of voting systems. DREs have many features that make voting more accessible and usable, but many have expressed concerns that adding paper trails undermines these gains. A recent study[1] found significant problems with the current implementation of paper trails on DREs. However, current paper trails leave much to be desired and represent more of ad hoc, add-on approach than a carefully engineered audit system. Usability and security are not mutually exclusive goals, and we strongly agree with the findings of the STS that much more can be done to improve the implementation of paper trail systems on DREs.

Concerns have also been raised that federal standards requiring voter-verified paper trails may bring a halt to innovation in e-voting systems. While there was never any clear evidence that this problem would arise, we are pleased that the STS recognizes these concerns and recommends an additional "innovation class" as a pathway for non-paper based system to meet certification. E-voting faces numerous challenges and is a field ripe for further research. Federal and private investments should continue to be made and new, innovative approaches should continue to be developed. However, until the fundamental constraints of security testing can be adequately addressed, these systems should have to meet a high bar for independent voter-verification before they are certified.

[1] Election Science Institute (August 2006) "Analysis of May 2006 Primary Cuyahoga County, Ohio," available at http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf

Thank you for considering our views. The recommendations of the STS represent an important step toward federal voting system standards that are more secure, usable and reliable. We urge the TDGC to adopt these recommendations.

Sincerely,

Eugene Spafford, Ph.D.
Chair
U.S. Public Policy Committee of the Association for Computing Machinery

cc: Members of the TDGC

About ACM and USACM

With over 80,000 members worldwide, The Association for Computing Machinery is an educational and scientific society focused on advancing computing as a science and a profession. USACM serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.