November 16, 2005

The Honorable Tim Hugo
Chair of the Joint Subcommittee Studying the Certification, Performance, and Deployment of Voting Equipment
General Assembly Building
P.O. Box 406
Richmond, Virginia 23218

[Delivered via email to Mary Spain, mspain@leg.state.va.us]

Dear Chairman Hugo:

The Association for Computing Machinery (ACM) is the premier scientific and technical society for computing professionals, worldwide. We have nearly 80,000 members who are scientists, engineers, educators, lawyers, students, and practicing professionals, including many who are citizens of Virginia. The USACM is the U.S. Public Policy Committee of the ACM. We write to offer our technical and non-partisan policy input as your committee considers voter-verified paper records for electronic voting equipment.

In a poll conducted last year, ACM members overwhelmingly indicated that they have serious concerns about electronic voting machines—concerns that should be addressed with specific safeguards. ACM then adopted an official policy statement (enclosed) in support of voter-verified audit trails. As you will see from that enclosed statement, ACM recommends that all voting systems—particularly computer-based electronic voting systems—embody careful engineering, strong safeguards, and rigorous testing in both their design and operation. Many of our members believe that an appropriate way of supporting these goals is by requiring direct-recording electronic (DRE) voting systems to produce a physical (e.g., paper) record. That record would provide each voter the option of verifying that his or her vote has been accurately cast. When properly implemented, these physical records can also serve as an independent check on the results produced and stored by the DRE systems. Such records are vital to preserve the option of performing a meaningful recount in the cases of possible errors or suspected fraud. These records should also be audited on a random basis to ensure the accuracy of electronic counts provided by the DRE machines.

Unfortunately, many electronic voting machines do not provide a voter-verifiable audit trail. Using such machines is risky, for when problems or unusual results leave an election in doubt, having a transparent and credible recount becomes extremely difficult, and officials may have no choice but conduct a revote or accept the existing results. Audit trails (if they exist) that are not physical and voter-verified may not accurately reflect the votes cast when undetected errors or tampering alter the outcomes of elections. The resulting lack of certainty in the results, especially in close races, not only undermines the accuracy of the vote, but may serve to diminish citizen confidence in the fairness of the process.

Other equally important provisions that should be part of any electronic voting system implementation include establishment of best practices or other means to ensure regular and random inspections, audits, and experimental testing of software and hardware by independent, qualified individuals and observers before, during, and after voting occurs. The design and management of e-voting systems should be held to the highest possible standards, for ensuring the reliability, security, and verifiability of public elections is fundamental to a stable democracy.

Please do not hesitate to contact us if we can be of further assistance as you address this important topic.

Sincerely,

Eugene H. Spafford, Ph.D
USACM Chair

Barbara Simons, Ph.D.
USACM E-voting Subcommittee Chair

Enclosure: ACM Statement on E-Voting

ACM RECOMMENDS INTEGRITY, SECURITY, USABILITY IN E-VOTING

Cites Risks of Computer-based Systems

New York, September 27, 2004 – Seeking to bolster the security, accessibility, and public confidence in the voting process, ACM's elected leadership has approved a public statement on the deployment and use of computer-based electronic voting (e-voting) systems for public elections.

ACM Statement on E-voting

Virtually all voting systems in use today (punch-cards, lever machines, hand counted paper ballots, etc.) are subject to fraud and error, including electronic voting systems, which are not without their own risks and vulnerabilities. In particular, many electronic voting systems have been evaluated by independent, generally recognized experts and have been found to be poorly designed; developed using inferior software engineering processes; designed without (or with very limited) external audit capabilities; intended for operation without obvious protective measures; and deployed without rigorous, scientifically-designed testing.

To protect the accuracy and impartiality of the electoral process, ACM recommends that all voting systems—particularly computer-based electronic voting systems—embody careful engineering, strong safeguards, and rigorous testing in both their design and operation. In addition, voting systems should 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. Making those records permanent (i.e., not based solely in computer memory) provides a means by which an accurate recount may be conducted. Ensuring the reliability, security, and verifiability of public elections is fundamental to a stable democracy. Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by the electorate.

For more information, see <http ://www.acm.org/usacm/weblog/index.php? p=73>.