

BY JEFF GROVE

---

# ACM STATEMENT ON VOTING SYSTEMS

*The Association recommends more attention to integrity, security, and usability in the design and use of all voting systems.*

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 computer-based electronic voting (e-voting) systems for public elections. ACM's statement recognizes that while computer-based e-voting systems have the potential to improve the electoral process, such systems must embody careful engineering, strong safeguards, and rigorous testing in both their design and operation.

Experts from the computing community (see the special section in this issue) have identified a variety of risks and vulnerabilities in many e-voting systems stemming from poor design, inferior software engi-

neering processes, mediocre protective measures, and insufficient comprehensive testing. As a result of these risks, ACM has recommended that e-voting systems enable each voter to inspect a physical (for example, 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. Those records should be made permanent, not based solely in computer memory, to provide a means to conduct an accurate recount.

The ACM statement on e-voting reflects the values in its long-held Code of Ethics and Professional Responsibility ([www.acm.org/constitution/code.html](http://www.acm.org/constitution/code.html)). The Code states that computing professionals have a responsibility to share technical knowledge and expertise with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. USACM—ACM's public policy committee on U.S. IT issues—has actively engaged in dialogue with policymakers, election officials, and voting rights advocates to promote improved accuracy, integrity, security, and usability of e-voting systems. While the ACM statement is primarily based on recommenda-

tions from USACM and focused on current events in the U.S., it is of global importance, particularly in Europe where the Council of Europe's Committee of Ministers is formulating recommendations to member states on legal, operational, and technical standards for e-voting.

Prior to approving the statement, ACM engaged its membership by bringing the issue to their attention and soliciting their feedback. Members were encouraged to participate in an online poll to gauge their support for the statement. Of the nearly 4,600 members from around the world who expressed their opinions, 95% indicated their agreement with

the statement. ACM plans to engage its membership more frequently as it continues to strengthen its position, visibility, and participation in government policy formulation by educating and informing policymakers on key issues in computing and IT.

For more information, contact the ACM Office of Public Policy in Washington, D.C.; [usacm\\_dc@acm.org](mailto:usacm_dc@acm.org) or +1-202-659-9711. **C**

---

**JEFF GROVE** ([jeff\\_grove@acm.org](mailto:jeff_grove@acm.org)) is director of the ACM Office of Public Policy, Washington, D.C.

## ACM Statement on Voting Systems

*Approved by ACM Council on Aug. 25, 2004*

**V**irtually all voting systems in use today (punch-cards, lever machines, hand-counted paper ballots, among others) 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 (for example, 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 (that is, 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. **C**