

# ACM Statement on Voting Systems

Approved by ACM Council on Aug. 25, 2004

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.