Notes for a Hearing of the California Assembly Committee on Elections Reapportionment and Constitutional Amendments

Peter G. Neumann
Principal Scientist, Computer Science Lab
SRI International, Menlo Park, California
333 Ravenswood Ave, Menlo Park CA 94025-3493
Tel 1-650/859-2375; Fax 1-650/859-2844
Neumann@CSL.sri.com; http://www.csl.sri.com/neumann

Tuesday, June 15, 2004

Among my many other roles as a computer professional since 1953, I have been involved with integrity, reliability, security, and privacy as directly related to election systems for almost 20 years, specifying requirements, evaluating systems, and analyzing system failures, alleged fraud, and human errors. These efforts included participation in New York City's eventually aborted attempt over a decade ago to upgrade from lever machines to electronic voting systems.

My testimony to your committee on January 17, 2001 (see reference below) stated that *"The election process is inherently subject to errors, manipulation, and fraud. It is a process that demands extraordinary integrity of any computerized systems involved, as well as honesty and experience of the people involved in administering elections. Evidently, it may require considerable sophistication on the part of voters as well."* This statement is increasingly relevant today.

Elections require an end-to-end concern for a wide variety of system integrity requirements, from registration through vote tabulation and reporting. During the voting process in particular, errors and malicious alterations of software and results can easily go completely undetected.

Subsequent to my previous testimony, the system integrity problems have intensified rather than abated. This is largely a result of the post-2000 feeding frenzy to acquire unauditable all-electronic direct-recording voting machines (DREs) that, in the absence of voter-verified audit trails (VVATs), provide *no meaningful assurances* that votes are correctly processed. (Ideally, a VVAT is human-readable medium such as paper that is also machine-readable, and forms the vote of record especially in cases of any disputes.) From the perspective point of system security experts, vendor claims that VVATs are unnecessary are seriously disingenuous and contraindicated by past experience, for a variety of reasons – such as the extremely weak criteria that are used for evaluation, the vendor insistence on proprietary code, an evaluation process that is proprietary and paid for by the vendors, pre- and post-election testing of equipment that generally fails to detect certain serious problems such as Trojan horses and unauthorized dynamic changes, and other clear evidence in recent elections that the claims are not justified. The presence of convicted felons among company personnel is also distressing. Worse yet, vendors claim there is no need for the VVAT because there is no evidence of tampering. However, that completely avoids the main point: these machines allow no evidence of tampering precisely because there is no VVAT! What goes on inside the computer memories is completely inscrutible.

The lead editorial in *The New York Times* on Sunday, June 13, 2004 ("Gambling on Voting"), points out that the bar is set much higher on gambling machines than on voting machines. "But the truth is, gamblers are getting the best technology, and voters are being given systems that are cheap and untrustworthy by comparison. There are many questions yet to be resolved about electronic voting, but one thing is clear: a vote for president should be at least as secure as a 25-cent bet in Las Vegas."

Some recent anomalies were obviously detectable, such as the MicroVote software used in Boone County, Indiana, where 144,000 votes were recorded when only about 5,000 people had voted, or an earlier electronic voting machine case in which only one vote was recorded when several thousand people had voted. In other cases, detection of something having gone wrong has been very difficult or even impossible, especially in close elections – where it counts the most. For example, one machine (WinVote) was discovered *after the election* to have been shifting about 1% of the votes from one candidate to another (Fairfax County, Virginia), despite supposedly conclusive certification and pretesting. In many other cases, the inability to do a meaningful recount (there is nothing to recount other than the bits that may already be incorrect) hinders post-election remediation. Furthermore, as you probably know, in all 17 counties in which Diebold software was used in the 2002 general election, the software that was in use was not the certified software. This is a very important concern, because undocumented software or configuration changes can result in essentially arbitrary subversion of the election results, either accidentally or intentionally.

Of course, all voting systems are subject to varying degrees of errors and manipulation; however, the unauditable all-electronic systems without voter-verified audit trails create a situation in which very small flaws or illicit software changes can result in widespread systematic alterations of the intended results. Computer scientists with extensive backgrounds in computer security know how to provide much better security, integrity, and reliability with suitable checks and balances. Apparently the developers of all-electronic voting machines either do not know how, or perhaps do not want to do so. Thus, the opportunities for accidents, fraud, and subversion can go largely undetected.

An enormous educational process is needed; government officials, election commissioners, and voters are just beginning to comprehend the depth of the risks involved in having election systems without meaningful integrity. I note that the League of Women Voters, which previously was supportive of the paperless all-electronic voting systems, yesterday changed its position after reaching a more accurate understanding of the risks involved. Their position is now this: "In order to ensure integrity and voter confidence in elections, the LWVUS supports the implementation of voting systems and procedures that are secure, accurate, recountable, and accessible." There is also similar controversy within the sight-impaired communities, where some people simply believe that the unauditable all-electronic voting machines must be inherently good (of course we can trust computers, can't we?), whereas others in that community understand that the ability to vote is meaningless if the votes are not correctly recorded and correctly counted. (One of the most outspoken critics of voter-verified audit trails is evidently receiving funding from at least one of the system vendors, according to the lead editorial in *The New York Times* on June 11, 2004.)

California's Secretary of State Kevin Shelley has recognized many of the risks of all-electronic systems that are not augmented with some sort of voter-verified audit trail that can permit definitive recounts. Unlike most other transactions in which customer receipts, extensive audit trails, and even surveillance cameras on ATMs are commonplace, election system recounts and adjudication of suspected irregularities are not meaningful in the absence of a VVAT. Vendors seem to have traded off system integrity for privacy. This is an unnecessary tradeoff.

My conclusion is simple: for the foreseeable future, all-electronic voting systems should not be used without voter-verified audit trails. In the near future, the only sensible alternative for those machines is the addition of a voter-verified paper audit trail, although for counties that have not already acquired all-electronic voting machines without VVATs, they would be better off staying with optical-scan technology or whatever else is used for absentee ballots. It is little consolation to other California counties that, after several of us spoke to the Santa Clara County Board of Supervisors during January and February 2003, the supervisors insisted that if the VVATs were mandated by the state and properly certified, the vendor would have to deliver them as part of the contract. However, for the forthcoming November 2004 election, this is still too little too late. Nevertheless, there are various short-term measures that could be invoked in the coming months. For example, the Leadership Conference on Civil Rights is preparing such a set of recommendations, which will include a set of guidelines being prepared by the National Committee for Voting Integrity (NCVI, of which I am the chairman) for the use of the various all-electronic voting machines (as well as optical-scan systems) for use by election officials, poll judges and supervisors, and voters; it is expected to be available in the next few weeks. Other organizations are also preparing similar guidelines. These guidelines should be taken seriously, even though they cannot overcome the most serious integrity problems that can result from inherently unauditable all-electronic voting systems. For example, these measures cannot ensure that no votes will be lost or corrupted, but only that it will be more likely that certain irregularities can be detected, corrected, or avoided. However, unless the fundamental lack of integrity and auditability is corrected before future elections, the integrity of the results will always remain in doubt. No state, county, or local government should have to deal with legal and other problems that can otherwise be avoided.

A Few References:
My Web site: http://www.csl.sri.com/neumann
Illustrative Risks document: http://www.csl.sri.com/neumann/illustrative.html and click on Election Problems
My 2001 testimony: http://www.csl.sri.com/neumann/calvot01.pdf
My 2004 testimony: http://www.csl.sri.com/neumann/calvot04.pdf
Peter G. Neumann, *Computer-Related Risks,* Addison-Wesley 1995
National Committee for Voting Integrity: http://www.epic.org/privacy/voting/
Rebecca Mercuri's Web site: http://www.notablesoftware.com/evote.html
David Dill's VerifiedVoting.org: http://www.verifiedvoting.org
Kim Alexander's California Voter Foundation: http://www.calvoter.org