Howard Stanislevic
Founder, E-Voter Education Project
Website: http://e-voter.blogspot.com/

Testimony Before the NYS Senate Standing Committee on Elections
Joseph P. Addabbo, Jr., Chair
NYC, NY, October 9, 2009

Thank you for the opportunity to testify. My name is Howard Stanislevic and I am the founder of the E-Voter Education Project -- a group dedicated to the demystification of electronic voting. Today I want to speak to you about the need to audit elections counted by computerized electronic ballot scanners, known as precinct-count optical scanners (PCOS), and how the State Board of Elections and our election laws have failed to meet that need.

First of all, we can't trust computers to count votes because it's not possible to conduct tests that would be adequate to merit our trust. In 2006, the same computer scientists at the National Institute of Standards and Technology (NIST) who wrote the 2005 federal voting system standards that New York has adopted to certify its new ballot scanners, advised the US Election Assistance Commission (EAC) that testing of software-based voting systems "to high degrees of security and reliability is from a practical perspective *not possible*." (emphasis added)

These scientists, and many others, advocate *software-independent* (SI) voting systems.[1] A voting system is software-independent only if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome. This means we must randomly audit the election results, independently of software, by hand-counting enough votes to see who won each contest. *Nothing in our election law or regulations requires this*.

Some have incorrectly asserted that dependence on software is only a problem with direct recording electronic (DRE, usually touchscreen) voting machines -- not optical scanners. So I asked Dr. Ron Rivest of MIT and the EAC's Technical Guidelines Development Committee (TGDC) -- one of the co-authors of NIST's Software Independence paper -- to clarify whether SI principles must be applied to precinct-count op scans (PCOS) as well as DREs. Dr. Rivest's thoughtful response is attached and I ask that it be included in the record. To summarize, he said that indeed op scan elections are at risk; thorough testing is not sufficient to provide strong confidence in election outcomes; and "Testing is no more a guarantee of good behavior during an election than is good behavior before marriage a guarantee of fidelity afterwards!"

Ballot scanners are no more secure than touchscreens. They are both computers, and they are both programmed by yet another computer -- each county's Election Management System – a PC with election management software that costs about $75,000.

If these computers were people, and their memory cards were organs, we'd be talking about a highly efficient way to spread a sexually transmittable disease. No Internet or wireless connection is necessary to spread a computer virus. Malicious code could infect every scanner in a jurisdiction via the same memory cards necessary to program the scanners before each election, and to upload their tallies afterwards. We see no evidence of procedures to mitigate this risk in New York. For example, doing so would require not one, but three of those $75,000-PCs in each county -- completely isolated from each

[1] An excellent primer on software independence (SI) with links to the original papers by Rivest and Wack and the SI resolution passed by the EAC's Technical Guidelines Development Committee can be found at: http://en.wikipedia.org/wiki/Software_independence

other.[2] The University of Connecticut "hacks" each scanner's memory card, on behalf of their Secretary of State, to examine its contents.[3]

Computer scientists agree that the best answer is to rely on paper ballots. But New York will *not* be doing so, despite the claims of some of our election officials. Our Election Law provides no right to a post-election-night recount of *all the paper ballots* cast at the polls. The Election Law § 9-208 recanvass is *not* a recount, but merely a comparison of the reported scanner tallies, to paper copies of the same tallies -- up to two weeks after the election. Obviously, such a recanvass can neither detect nor correct erroneous or fraudulent tallies produced by scanner software within the Election District *on election day*. Correcting such errors requires a hand count of all the paper ballots originally counted by the machine. This recount is known as a *post-election audit.*

An unverified outcome of a contest is one in which the wrong winner may be certified, despite the fact that no miscounted votes were found in the post-election audit. The 3% audits required by Election Law § 9-211 may not find a single miscounted vote, even if the winners of many elections are incorrect. For example, we estimated that a 3% audit of Election Districts (EDs) in recent general elections, which is a more effective audit than that required by our election law, would result in the following numbers of unverified outcomes of recent State and Federal contests: [4]

Unverified Outcomes of NY General Election Contests with a 3% Audit of Election Districts	
2002-2006	14 out of 87 US House races
2006	32 out of 150 Assembly races
2006	7 out of 62 NYS Senate races

In light of recent events, imagine the effect that ***seven unverified outcomes*** could have on the composition of the NYS Senate!

The number of unverified outcomes would be even greater if, as required by the Election Law, we audited 3% of *ballot scanners* instead of 3% of EDs. Since there are fewer total scanners than EDs, fewer scanners will be audited. But the chance of finding problems depends crucially on the *number* of units audited – not the fraction (percentage) thereof. If we use scanners to count votes, the audit required by our Election Law is a *worst practice.*

Not only does our Election Law lack a provision for larger random audits of closer races, it also has no provision for targeted investigations of anomalous results in particular Election Districts. And although the law says that a "complete audit" can be used to determine the winner of an election, it has no definition of "complete audit." The law is being read by the State Board of Elections as if a "complete audit" means an audit of only a *single county!* Thus a statewide or other multi-county contest may be decided by a hand count of only a ***single county!***

The SBoE has also said that candidates who lose computer-counted elections must go to court to obtain more than a 3% hand count. But as we have seen, the 3% audit may not provide *any* evidence of miscounted votes to bring to court – even if the wrong winner were reported by the voting system.

At least one courageous Election Commissioner has said she will *not* certify a computer-counted election. Do we really want computers and courts to decide who wins and who loses our elections on a

[2] See: "You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems" http://citp.princeton.edu/pub/hrsw-evt08.pdf

[3] Details of scanner vulnerabilities and mitigations implemented by Connecticut, can be found at U. Conn's Voting Technology Research Center website: http://voter.engr.uconn.edu/voter/Reports.html

[4] "NY Election Audits: Is Three Percent Enough?" http://sites.google.com/site/evoterproject/files/NYAuditGraphs.pdf

routine basis? Or should it be the will of the voters and the votes they actually cast? I vote for the voters. So please, *either fix the audit law, or keep the lever voting machines*. Experts are available who would be more than happy to help draft the appropriate legislation, *pro bono.*

Finally, I ask that the names of the thousands of New Yorkers who signed petitions to keep the lever voting machines, and the many county and non-governmental resolutions to do so, be included to the record. Thank you.

Personal Communication From Dr. Ronald L. Rivest [5]
On Precinct-Count Optical Scanner (PCOS) Security Threats
And the Need for Software-Independent Audits
Dec. 8, 2008 (Submitted for the record with his permission)

It may be the case that PCOS software tends to be simpler than DRE software, since it doesn't need code to support complex interaction with the voter.

However, while thorough testing is a good idea, it is not sufficient by itself to provide strong confidence in the election outcome.

If the testing is only done for certification, you have the problem that the software running on election day may not be the software that was certified. Also, such testing wouldn't catch "ballot programming" errors.

So-called "logic and accuracy" testing may catch some of these problems. (Although I have been amazed that some jurisdictions run test decks that have the **same number** of votes for each candidate -- this fails to catch the common error when the ballot positions for two candidates are switched in the ballot programming!)

But both certification testing and L&A testing are inadequate to catch malicious software. Such malicious software may, for example, be triggered to enter "malicious mode" when a ballot of a certain configuration is entered early in the day by a confederate. So-called "parallel testing" would not catch this error either, since the trigger ballot would never be entered for the test machines. Once malicious mode is entered, a small percentage of the ballots may have their votes switched to the opposing candidate.

Testing is no more a guarantee of good behavior during an election than is good behavior before marriage a guarantee of fidelity afterwards!

The recent experience in Humboldt county shows the vital importance of statistical audits; you can't always trust the machines, even if (you believe that) they've behaved well in the past...

Cheers,
Ron Rivest

[5] Dr. Rivest is the Viterbi Professor of Electrical Engineering and Computer Science in MIT's Department of Electrical Engineering and Computer Science, a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and a founder of its Cryptography and Information Security Group. Dr. Rivest serves on the EAC's Technical Guidelines Development Committee, chaired by the National Institute of Standards and Technology (NIST). NIST and the TGDC write the federal voting systems standards adopted by the New York State Board of Elections.