Assemblymember Joan Millman, Chair,
Committee On Election Law

Assemblymember Catherine Nolan, Chair,
Committee On Education

Assemblymember Barbara Lifton, Chair,
Committee On Libraries And Education Technology

Assemblymember Brian Kavanagh, Chair,
Subcommittee on Election Day Operations and Voter Disenfranchisement

Statement by Teresa Hommel, Chairwoman,
Task Force on Election Integrity, Community Church of New York

<u>The Election Commissioners' Association of the State of New York shows ignorance of computers on the eve of computerizing our vote.</u>

It is better to continue using our well-understood, affordable lever voting machines than to computerize our vote-counting at this time when our counties cannot afford – and our election commissioners do not understand the need for – proper audits.

Thank you for the opportunity to testify here today.

The first points I wish to make, very firmly, have to do with *context*. New York State has had enormous achievements in our preparation to replace lever voting machines by computerized equipment. We have led the nation in several ways.

- Audits -- At a time when activists nationwide were haggling to get *1/2 percent* audit of electronic voting systems, New York passed the Election Reform and Modernization Act requiring 3% audit.

- Communications -- At a time when electronic voting systems nationwide had communication capability that would enable malicious persons worldwide to easily modify our election results, we banned communications capability in electronic equipment to be used in New York State.

- Testing prior to Purchase -- At a time when other states were buying equipment without testing it, and without any attempt to evaluate the so-called federal testing for certification that was being done, New York required testing to federal standards and hired an independent technical company to evaluate the work of our federal laboratory. And as a result it became known that the federal laboratories either were not actually doing any testing, or were doing very little.

- Paper trail – New York law requires a paper record of every vote cast on electronic voting or vote-counting equipment. In 2005 when our law passed, this was a major achievement.

I want to repeat, New York's achievements are great when evaluated within the context of how computerized voting and vote-counting equipment is used in our nation. However, there is a larger context, which is the use of computers in the professional world. I have worked with computers professionally since 1967. Many of the election integrity activists nationwide are computer professionals. We compare the use of computers in elections to the use of computers in the professional world, and we see that even in the best of states, like New York and California, the use of computers in elections has been unprofessional and wrong from the beginning.

- Preventing meaningful observation -- If the Help America Vote Act (HAVA) had said, "We hereby ban all election observers" people would have objected. But instead HAVA said, "Here's a lot of money so the states can buy computerized voting and vote-counting equipment." It's the same thing, because when you put vote casting and counting into a computer, there's nothing to meaningfully observe. In the professional world, when people need to solve a data-processing problem, a threshold question is asked, "What are the needs of this problem area, and can computers meet these needs?" One foundational need for elections is to use technology and procedures that facilitate meaningful public observation. Computers don't meet that need.

- Computer "security" -- I still remember the brochure for DREs (touchscreen-style voting machines) addressed to county election officials that said, "You can use what you learned at home with your personal computer to run secure elections." This is like telling someone, "If you can count to 10, you can be a rocket scientist." The fact is, no corporation runs secure computers, and corporations, especially those in the financial industry, know more about computer security than just about anyone. As a short-term contractor, I have worked for hundreds of clients, and most of the financial companies in our country. Every one of them has problems with insider and outsider intrusion into their computers, as well as innocent errors. In business "security" means that your processing results are correct, and it doesn't matter whether the cause of errors is innocent or malicious. Corporations verify 100% of every processing step. They would not do this unless it was necessary in order to find their errors before their clients find them.

- Reliance on pre-testing -- For practical purposes, there is no such thing as a secure, error-free computer, and all processing needs to be verified. If corporations could test their computerized equipment, and see that it works in tests, and then rely on those tests to ensure that processing would be accurate, and avoid the expense of 100% verification, they would not verify. In this context, New York's ground-breaking 3% audit is part of an "election exception" to professional handling of computers. We have to question why our nation has accepted this kind of exception. And also we need to ask why, here in New York, it appears that many – but not all -- of our county election officials believe that pre-testing is sufficient to ensure accurate results. Why don't they know that pre-testing is not a panacea?

- Paper trails turned out to be a failed idea – Paper trails were a theoretical solution intended to solve some of the problems of using computers to handle votes. But the idea was not practically feasible. I have attached a brief paper with the details on this point. http://www.wheresthepaper.org/VVPAT_Idea_Failed.pdf

Where is New York Now?

New York is about to replace our lever voting machines with voter-marked paper ballots and precinct-based optical scanners (vote-counting computers). The new technology is already in use in some upstate counties, and the State Board of Elections plans to finish certification testing on the scanners in December this year. Upon certification of the scanners, all counties will be asked to sign their purchase contracts for them.

In spite of the imminent switch-over to computerized vote-counting, many of our county election officials appear to be ignorant of the security needs of computers, especially the need for audits.

In August, 2009, William W. Scriber, President of the Election Commissioners' Association of the State of New York, sent a letter to the New York State Board of Elections on behalf of the Association.[1] He expressed serious concerns with the State Board's proposed 6210.18 regulations that would require counties to audit (hand-count) the votes processed by at least one scanner for each contest in each election.

His letter objected to the cost of such audits, a realistic concern in this time of drastic cutbacks in most governmental budgets. But the solution is not to skimp on proper computer security. Rather the solution would be to keep the affordable lever voting machines that we already have, which have minimal and affordable security requirements.

Mr. Scriber objected to the number of ballots that the proposed regulations would require to be hand-counted. He stated "we consider [audits for every race] totally unnecessary" given the pre-election tests of the scanners that counties would be doing.

This position and rationale reveal disturbing ignorance.

In business, 100% of transactions are confirmed and yet errors are common. ATM transactions are verified three to five times each, and yet ATM errors and fraud are widespread. Many businesses employ teams of technical employees who verify computer results -- and correct the errors -- around the clock, seven days a week. None of this verification would be done if it were not needed to ensure accurate computer results.

Use of computers in the field of elections differs from use of computers in business in two ways.

- Computerized vote-counting is harder to verify. The secret ballot, which we use to prevent vote-selling and coercion, also prevents effective use of most types of business verification, which are based on the use of tracking numbers for each transaction. Using tracking numbers or other identification on ballots would violate the secret ballot and enable people to identify who cast each ballot. This is why verification of computerized vote-counting consists of hand-counting the same votes that a scanner counted in order to determine if both vote-counts produce the same tallies. The hand-counting should take place immediately upon close-of-polls while the ballots are still under continuous observers' scrutiny, so that we know the ballots were not tampered with. If immediate hand-counts are impractical, then the voted ballots have to remain in observers' view until the hand-counts take place.

- Election officials have no interest in securing voted ballots by facilitating observers' continuous observation of them, and do not want to perform sufficient hand-count audits to confirm the outcome of all races.[2] And they get away with it. In business, a person who refuses to do their job, or misuses the technology they work with, gets fired.

If the scanner in my poll site reads my ballot incorrectly or credits my vote to a wrong candidate, I won't notice and neither will anyone else. In fact there is no way for anyone to know unless the votes on all ballots processed by my scanner are secured by observation and hand-counted.

---

[1] http://www.wheresthepaper.org/ECA_6210.18_concerns.pdf
[2] This attitude is widespread -- http://www.wheresthepaper.org/HouseAdminTestimonyDougLewis3_20_2007.pdf

Scanners make mistakes.[3] The scanning "calibration" can "drift" during the election day, resulting in lost or switched votes, and no one would know. The ballot programming could contain innocent or malicious errors. The software could contain as-yet-unnoticed errors. Computers are vulnerable to many types of problems that mechanical machines don't have.

Yet our Election Commissioners' Association doesn't seem to know this. They think that testing a scanner before an election is enough to show that it will work a week or two later during the election. This would be true with mechanical lever machines, but not with computers.

Mr. Scriber's letter also says. 'We have always understood that it was the intent of the audit to check machine operation/programming and not to test each candidate. In reality the three percent audit was to test the machines functionality and not to do a partial "recount" of candidates…."

It is unclear what Mr. Scriber might mean by machine "operation/programming" or "functionality". One would think that these terms mean that votes are accurately read by the scanner, and votes are accurately credited to the correct candidate. The only way to know these things is to audit (hand-count) the votes to verify the computer's count.

It is unclear whether Mr. Scriber knows that scanners have "ballot programming" which determines which candidate gets the benefit of each vote, that separate ballot programming is done for every ballot style with separate opportunities for errors that may kick in after a large number of ballots are processed on election day. It is unclear whether he knows that scanning calibration may drift. The only way to know if the ballot programming is correct for each candidate *on election day* is to audit for each candidate after the election.

Based on Mr. Scriber's letter, it appears that not all of our county election officials understand these basics. This is why we need to halt our plans to replace our lever machines with computers now until our law mandates, and we can afford, to protect our future paper ballots with continuous observation, and audit all races sufficiently to demonstrate that the winners are indeed the winners. I urge this Committee to take all possible actions to enable our counties to keep our affordable, easily-secured lever voting machines until such time.

Thank you.

---

[3] "Ballot-Scanner Voting System Failures in the News - A Partial List," May 22, 2009. Describes 186 occurrences of malfunction including 80 incorrect tallies, 35 EMS miscounts, 22 memory card failures, 5 mark-detection failures, 13 instances of misprinted ballots, and 31 miscellaneous operational failures. Readers are cautioned to remember that although scanners have many failures, they are superior to touchscreen-style voting machines (called DREs) which have more failings and 3 times more failures. http://www.votersunite.org/info/OpScansIntheNews.pdf