

GAE Public Hearing Extended Testimony
February 21, 2008
Testimony of Denise M. Weeks

334 Hollister Way West
Glastonbury, CT 06033
Denise@CTVotersCount.org

Good evening, Chairs and members of the committee. My Name is Denise Weeks and I am a resident of Glastonbury CT. I appreciate the opportunity to comment.

I have 30 years experience working with computers, as a programmer, systems designer and project and operations manager. I managed large testing projects and developed testing best practices for several large insurance companies.

I have managed the implementation and on-going release testing of comprehensive tax reporting software for a multi-line insurance company, coordinated release testing for a comprehensive small group health insurance application and played a major role in the development of best practices for Y2K analysis and testing for the finance and investment division of a large insurance company.

My teams have been cited repeatedly for timely and accurate implementation of software changes and our testing methods adopted as best practices in other areas of the companies.

I participated in the Connecticut Citizens Election Audit Coalition observation of the post November audits, read their report and have attended the hearings held in Norwich and Norwalk.

At the one audit I observed, the ballots were counted and tallied only once, yet after announcing the results, which included discrepancies, the registrar explained to the poll workers that the results proved what everybody already knew which is - hand counting is less accurate than machine counting. As someone who has spent most of my adult life programming and testing computers I would argue against her conclusion

What is most alarming to me is the prevailing belief among registrars of voters and poll workers that machine counts are more reliable than hand counts, that the recent audits demonstrate that machines are more reliable and the conclusion by many that hand counted audits and recounts should be abandoned or replaced by machine audits and recounts.

My experience compels me to argue against these conclusions.

First, computers are programmed by people and are every bit as prone to human error as hand counts.

Second, in the November audits, registrars reported 31 instances of discrepancies between the machine and hand counts with discrepancies ranging from 10 to 54 for a candidate in a single district. The percentage of discrepancies ranged from 10% to as high as 44%. Since the discrepancies were not investigated we don't know whether they were due to manual counting errors or computer error. All we know for sure is there were discrepancies

Third, even if the audits had proven that the computers worked flawlessly in the November election, it would be no guarantee that they would work flawlessly in subsequent elections. An improperly programmed computer will miscount the votes over

and over again. Also, since all memory cards in a district should by definition contain exactly the same code, reading ballots through a second machine would not detect erroneous or fraudulent programming.

The argument is often made that we rely on computers for our banking and shopping transactions every day and should at some point be able to trust computers with our votes and eliminate the hand audit. Again, my experience compels me to disagree.

ATM and retail scanning applications provide a receipt that is verified by the user and can be corrected over time. Voting systems are reprogrammed for every election and must be right the first time since they are only used on Election Day. Voting systems must also be private in order to avoid vote selling and voter intimidation, which is why no receipt can be issued. **The only valid receipt in our voting system is the voter verified paper ballot that remains behind, and the only way to insure against programming error or fraud is to hand count the ballot.**

The argument is made that pre-election testing by registrars and pre and post election testing of memory cards can and do ensure that the systems are working properly. While such testing is a good idea it cannot protect against every programming error and certainly not against fraud.

In the hearings in Norwich, a registrar reported a case where the machine count exceeded the number of people who voted by 24, a number which coincidentally matched the number of write in votes. The registrar reported the discrepancy and was told that the poll officials must have read the write in ballots through the machine twice, a conclusion she did not accept. A equally likely explanation, based on my testing experience, would be that the machine was double counting those ballots. The lack of investigation is unsettling since a simple hand recount would likely have resolved the issue. This is also an example of a possible programming error that eluded testing by the registrars and the memory card tests.

I believe the greatest threat to the integrity of our voting systems comes from their susceptibility to fraud. And here I am not talking about collusion or wrong-doing by poll worker, though that is certainly possible.

The greatest exposure comes from the fact that our voting systems are coded in secret by a vendor and the software is proprietary and not open to examination. This creates opportunity to rig elections in ways that would elude testing. Indeed computing experts studying the vulnerability of computers have acknowledged numerous ways to alter the vote and elude detection (Shvartsman, p2), :

- The documentary Hacking Democracy demonstrates how vote totals can be altered on the very machines used in our elections. This problem has been confirmed by Dr. Shvartsman at UCONN, (Shvartzman, p4). Counters are set to +5 votes for one candidate and -5 votes for the other. This ensures that the zero tape at the start of the election prints properly and the total number of votes balances to the number of voters, yet alters the outcome.

Registrars claim that this hack would require access to the scanners, something that could not happen because of procedures, however since our systems are

programmed in secret by a vendor, even more sophisticated hacks could be delivered as part of the system as the following examples demonstrate:

- The system can be coded to contain two sets of code, one that would produce an honest result and another that would produce a fraudulent result. The system can be coded to trigger the use of the honest or fraudulent version based on a date, e.g. prior to or after the election, or the length of the voting day, the number of ballots cast or the speed with which ballots are cast, e.g. anything that would suggest a test versus an actual election (Shvatsman, 6).
- The system could be programmed so that the scanning of a particular ballot could not only trigger fraudulent code but could provide specific instructions to the systems as to how to alter the results. Such a ballot might use over-votes in several races to trigger execution of fraudulent code within the system and throw the election. Depending on how the election is going, a voter in collusion with a programmer could cast such a ballot to direct the program to alter the outcome of the election.

These are just a couple examples that computer experts put forth to demonstrate how voting systems can be tampered with without detection.

The Secretary of the State has said that her goal is to ensure that every vote is counted and every vote counts. In spite of reported voting irregularities across the country, most voters I talk to believe our vote is secure in Connecticut because we have a paper record that can be inspected if problems occur. I believe those voters would be outraged if they knew discrepancies reported after the November election were not investigated to determine whether the cause was due to an error in the hand count or the machine count. I think they would be even more outraged to learn that some are advocating elimination of hand counted audits and recounts of their ballots.

Replacing the hand count with a machine count for audit and/or recounts is a bad idea. It removes the only safeguard we have against programming errors and fraud of the type I described. I urge the GAE to:

- **To maintain manual audits and legislate manual recounts**
- **To strengthen the audits so we**
 - **Count enough of the ballots to deter and detect error or fraud**
 - **Audit ballot questions, referendums and special elections**
 - **Eliminate the exemption for towns where recounts or challenges have occurred**
 - **Mandate that discrepancies be investigated and expand the audit when discrepancies are uncovered that have the potential to impact the outcome of an election**
 - **Complete the audit shortly after the election to ensures that the candidates who take office do so based on the intent of the voters**

That concludes my testimony. Thank you for the opportunity to comment.

References

Kaiyias, Agelos, Laurent, Michel, Russell, Alexsnder, Shashidhar, Narashimsha, See, Andrew, **Shvartsman, Alexander**, Davtyan, Seda, **Tampering with Special Purpose Trusted Computing Devices: A cCase Study in Optical Scan E-Voting**, Voting Technology Research Center, Department of Computer Science, University of Connecticut, December, 2007.

http://voter.engr.uconn.edu/voter/news/Entries/2007/12/8_Tampering_with_Special_Purpose_Trusted_Computing_Devices%3A_A_Case_Study_in_Optical_Scan_E-Voting.html

1. Addendum based on other testimony delivered

One registrar who testified at the West Hartford hearing questioned the veracity of my testimony by asking rhetorically if I had any proof to back up my statements about our voting systems' vulnerability to fraud. Since the question was directed to me, I feel compelled to point members of the committee to report referenced above by Dr. Alexander Shvartsman of the UCONN Voting Technology Research Center.

Numerous registrars have testified that the scanner voting machines worked flawlessly, that voters loved them and that audits were costly, burdensome and no longer needed since the success of the audits prove that the machines worked. But what facts have they presented to support that conclusion?

That the counter on the scanner goes up by one with each ballot or balances to the number of voters checked off is not proof that the votes cast for various candidates were counted for particular candidates as the voter intended.

With all due respect and appreciation for all that registrars and poll workers do, their version of success is an illusion, just as the "ca-ching" sound of the lever machine curtain opening was no guarantee that those machines were working properly.

Much ROV testimony centered around the extensive procedures and training that they receive. One proudly displayed orange cards that she has checkers hand out to voters when the ballot clerk gets backed up. Voters then present the ballot clerk with the card to get the ballot. She even had a little Tupperware box that she saves them in for use in the next election. This well meaning improvisation introduces an opportunity for fraud: vote selling and counterfeit cards come to mind. An auditor attending the hearing shared with me that she had the same thoughts. Is such improvisation appropriate?

Was the election official who reported minus three questionable ballots in the November audits, following procedures?

Was the election official who allowed LHS to replace a scanner and reprogram a memory card during a recount, following procedures?

Was the election official who left ballots in the ballot box at the end of the election -this was discovered at the audit - following procedures?

Was the election official who left a machine and ballots unattended in an open room prior one of the November audits following procedures?

Was the election official who dismissed the fact that the number on the ballot bag seal did not match the number recorded on the night of the election and proceeded with the audit without reporting that to the Secretary of the State's office following procedures?

Unfortunately, the more I observe election officials and listen to their testimony, the more I believe that their primary concern is not with the integrity of the election but with the ease and speed with which they can get through day, whether it is election day or audit day. Many of them, in my view, lack the healthy skepticism and vigilance required to ensure the integrity of the election. Their testimony does not reflect a critical assessment of the electronic voting process against the goal of ensuring that every vote is counted and the intent of the voter is honored.