Ten Myths About Electronic Voting In Connecticut

Myth #1 – Connecticut has the toughest and strongest audit law in the country because we audit 10%.
Reality

- Connecticut audits a maximum of 3 or 20% of races in 10% of the districts. This is adequate only in the case of statewide races which are selected for the audit.
- Questions, referendums, and special elections are exempt from audits. Centrally scanned absentee ballots and all hand counted ballots also are exempt from the audits.
- In a state representative race or municipal race, the probability of detecting an error or fraud is in the range of 2-4%. This is far from sufficient.
- Towns with only one district would have municipal races audited an average of once in 20 years.
- Districts where there is an automatically recanvassed race or a contested race are exempt from audits – a state wide recanvass or contest would block all audits for the election in the entire state.
- Selection of the races to be audited is not required to be public. Audits are public, yet have no statutory prior public notification requirement.

Myth #2 – UConn reports of the post-election audits proved that our voting machines count accurately.
Reality

- In 2010 Registrars reported 29 instances of differences between the machine and hand counts with differences ranging from 6 to 40 for a candidate, in a single district. The highest percentage discrepancies was 22%. Such differences have continued at unacceptable levels, uninvestigated.
- Without transparent investigations we can't attribute the differences to either machine or human counting errors. Evidence for a complete investigation is no longer available as the ballots are no longer under seal.
- Observations of the actual audits raise questions about the credibility of the data provided to UConn. In Aug 2012 31% of reports by towns did not contain data necessary to determine the outcome of the audit, and an additional six reports were lost or never filed with the Secretary of the State.

Myth #3 –Hand counting is prone to human error. Electronic voting is more reliable because computers produce the same result over and over again. We should abandon manual audits and just run the ballots through another similar machine to validate the count.
Reality

- Computers and memory cards are programmed by humans and just as prone to human error.
- An improperly programmed computer will miscount the vote over and over again.
- Since all cards in a district should by definition contain exactly the same information, re-scanning on a similar machine would not detect erroneous or fraudulent programming.
- People can determine voter intent more exactly. They can produce an accurate/verifiable count given time, proper procedures, and controls.
- However, it is likely that publicly verifiable, "software independent", automated audits will be feasible.

Myth #4 – Auditing the paper by hand is too costly and time consuming.
Reality

- A sufficient hand audit would cost between $0.25 and $0.50 per ballot cast for the largest elections in Connecticut - a small fraction of the cost of conducting an election ($5.00 to $20.00 per ballot cast).
- The integrity of the vote and public confidence should drive decisions related to the conduct of elections. Cost, speed, and inconvenience are important, yet secondary, considerations.

Myth #5 – We can rely on procedures to catch errors and ensure the integrity of elections.
Reality

- Procedures are followed inconsistently, at best, sometimes not at all, and there is no enforceable penalty for failing to follow part or all of a procedure. Ballots and optical scanners have been left unsealed and unattended. Ballots have been unsealed and audits begun before the stated start of "public" audits.
- Only processes which are codified in the statutes are clearly enforceable.

Myth #6 - Memory card errors cannot affect the outcome of our elections because election officials conduct pre-election testing of our electronic voting systems.

Reality

- Pre-election testing cannot detect all errors and programming attacks. Pre-election testing of electronic voting systems will detect only basic errors such as 'junk' memory cards, wrong candidates, and machines that simply don't work.
- Computer science tells us it is impossible to test completely. Recent academic reports continue to outline many ways that clever programming can circumvent detection during basic pre-election testing.

Myth #7 – We don't have to worry about memory card problems because UConn tests the memory cards before and after each election.

Reality

- UConn's program is useful program, however, the trend is for fewer and fewer districts to send in cards for testing before and after the election. Selection is unlikely to be random.
- Many districts fail to send memory to UConn cards for pre- and post-election testing. In the 2012 Presidential Primary, compliance in submitting cards by local officials ranged from 8% to 18%.
- UConn reported that cards indicated that pre-election testing procedures continue not be followed consistently. How can we be sure the procedure for random selection of cards was followed?
- Over the years the number of cards tested per election have declined and reports have been delayed.

Myth #8 – If we can trust our money to ATMs and online banking, we can trust our votes to computers.

Reality

- Banks lose billions in online banking fraud every year. The savings ought weigh the costs to banks. Errors can be easily detected because the customer receives a receipt and the bank must account for all funds by double-entry bookkeeping.
- Memory cards for elections are programmed differently for each town and every election because the races on the ballot and the candidates are different in each town and in each election. In addition, voters cannot be issued any receipt to take with them because it would open the door to vote buying and intimidation.
- The only public security test of an Internet voting system, in Washington D.C., was quickly compromised.
- The only way to be sure the machines count correctly is to count enough of the paper to ensure that if fraud or error were to occur it would be detected. Secret voting precludes paper records for online voting.

Myth #9 – If there is ever a concern we can always count the paper.

Reality

The law limits when the paper can be counted.

- Audits can protect against error or fraud only if enough of the paper is counted and discrepancies in the vote are investigated and acted upon in time to impact the outcome of the election. See myths #1 and #2.
- An automatic recount (recanvass) occurs when the winning vote margin is within 0.5%. The local Head Moderator moderator or the Secretary of the State can call for a recount, but even candidates must convince a court that there is sufficient reason for a recount.
- Recounting by hand is not required by law. In early 2008 the Secretary of the State reversed her policy of hand recounts. We now recount by optical scanner.
- In 2010, the Citizen Recount showed huge discrepancies in Bridgeport, never recognized by the 'system'.

Myth #10 – The only way to ensure that all the votes are counted and that every vote counts is to count 100% of the paper.

Reality

Properly programmed scanners do a reasonable job of counting ballots. The key to safe elections is to:

1. Appoint an independent Audit Board with expertise in auditing and statistics to oversee the audits.
2. Count enough of the ballots to detect and deter error or fraud.
3. Investigate discrepancies and determine their cause, then take corrective and preventative action.
4. Expand the audit when discrepancies are uncovered that have the potential to impact an election outcome
5. Start and complete audits quickly so that data is preserved and the winners reflect the intent of the voters.
6. Codify and enforce the process so violations can be prevented or surfaced and corrected.