Teresa Hommel
10 St. Marks Pl., NY, NY 10003
www.wheresthepaper.org

Statement Against the Use of Money
Allocated under the Help America Vote Act
for the Purchase of Electronic Voting Systems for New York

Before the Governmental Operations Committee
of the New York City Council
October 18, 2004

Thank you for the opportunity to speak before you today. My name is Teresa Hommel. I have been working as a citizen activist on the issue of electronic voting for the last 16 months. My professional credentials are that I have worked with computers since 1967 as a programmer, technical writer, corporate trainer, and consultant.

I am here today to caution New York City against urging our state to move forward with the purchase and use of electronic voting systems.

There are two alternative approaches: One is for New York State to keep our old lever machines, and add one accessible ballot-marking device per polling place. The other is to switch to paper ballots and precinct-count optical scanners, with one accessible ballot-marking device per polling place.

What's wrong with electronic voting systems?

(1) They don't work reliably.

Attached to my testimony is a packet of materials. The first item is 63-page list of failures of electronic voting systems. Only six vendors are represented. There are 13 pages for Sequoia, and I put these pages first because many people think Sequoia will be the vendor selected in New York, if we go to electronic voting.

For every failure on this list, I would assume that there were many others that went undetected -- errors that you need an audit to find: votes recorded incorrectly, and wrong final tallies. Since no electronic voting system has ever been audited, we can't know how many errors of that kind have been made.

(2) Federal certification does NOT mean that a voting system works. "It has to have [certain] functions. But it doesn't have to work."

The second item in your packet is the I-Team interview with MicroVote Executives. MicroVote makes electronic voting systems. This quote comes from page 2, the candid remarks about certification made by Bill Carson.

We've had hundreds of failures of certified voting systems in this country, but some people need to read an interview like this to bring it home – certification does not mean the systems work.

(3) Even if electronic voting systems worked perfectly today, they may not work tomorrow because they are so easy to hack.

A person with moderate computer skills can read information that has been on the internet for over a year, and then hack these systems to give falsified election results. The hack takes less than a minute. You don't need direct physical access, because it can be done over a phone line and modem, a wireless communication device in the voting system, or over the internet.

Last month in Washington D.C., Bev Harris of BlackBoxVoting.org held a press conference where she demonstrated how to change the votes in a Diebold GEMS central tabulator and in a Sequoia system. She was dismissed by the major media, but in fact the "Trusted Agent Report" commissioned by the Maryland General Assembly said the same thing last January about the Diebold GEMS central tabulator (they used more technical language, and didn't publicize the exact methods like Bev Harris did). http://www.wheresthepaper.org/BBV_GEMSreport.htm

"Given either physical or remote access ... it is possible to modify the GEMS database ... without detection. Furthermore, system auditing is not configured to detect access to the database."
-- Trusted Agent Report, http://www.raba.com/press/TA_Report_AccuVote.pdf

(4) The security of these systems cannot be monitored or enforced by the people responsible for them.

The vast majority of elections professionals are not computer experts. Once they convert to electronic voting, they become dependent on vendor technicians to handle the computers. And they can't monitor what's going on because they don't know the technology.

For example: A technician walks over to the computer and says, "I better check the files." Who's going to question that? Or understand the answer if they do ask? Yet that brief access to the computer is a large-enough window of opportunity for someone to falsify an election.

(5) Computers conceal the process of ballot recording and vote counting, which is contrary to democracy.

The 2500-year history of elections tells us that whenever some part of an election procedure is concealed from public view, errors and fraud will occur. Electronic voting systems convert the heart of our elections to an invisible process, and we shouldn't do that.

(6) Computers give you speed. Audits give you accuracy.

In Albany we had two one-house bills on voting system standards that passed in February, 2004. Both bills required a voter-verified paper audit trail (VVPAT). One bill required a 2% surprise random recount, the other required 3%.

The VVPAT is essential with electronic voting, but it's only the first of two requirements. To detect all errors and fraud, we have to use the VVPAT to perform a complete audit on every election.

If a surprise random check of a small percentage of transactions could ensure the accuracy of a computer system, no bank or other company would ever spend the time and money to perform a complete audit. Companies do complete audits of their computer systems on a continuous basis, because that's the only way to find and correct errors which, if your customers see them, you'll lose your customers.

An audit performed by counting the voter-verified paper ballots in public would restore public oversight. If the tallies of paper ballots and electronic ballots differ, however, this requires an investigation into the conduct of the election (to determine whether there were irregularities by people) AND a computer audit (to determine whether the computer made an error).

Does any Board of Elections have the staff, expertise, or resources to perform a computer audit? One obstacle is that a computer audit requires thorough knowledge of the software used, and to my knowledge, all major vendors claim that their software must remain a trade secret.

At any rate, a complete audit of an election run with electronic voting systems would be far more complex, costly, and time-consuming than the effort required to securely guard paper ballots that were marked by hand, and to recount them before an audience of observers.

(7) The Help America Vote Act requires voters with disabilities to have a "private and independent vote."

That requirement should mean more than a private and independent experience in a voting booth, fiddling with a touchscreen or some assistive devices.

But in fact, electronic voting systems don't give anybody a private and independent VOTE.

Every vote cast is handed over to a large number of anonymous technical people who have been responsible for the system from its initial design, programming, testing, maintenance, storage, programming for the ballot, transportation, and installation in the polling site. And another cast of characters after the election.

A computer is only an instrument created and managed by people. Every voter using the computer is being assisted by these people, so the vote is not unassisted, private or independent. Without the complete audit I discussed before, we can't know if these assistants are recording our ballot choices, or counting our votes, honestly and without mistakes.

Voters who are blind, or have visual impairments, would get accessibility, privacy, and security if they mark paper ballots by using ballot templates like they have in Rhode Island and in other countries. There are data-to-voice scanners that can read the paper ballot back to the voter through headphones. There are accessible ballot-marking machines, such as Populex or Automark, that can assist voters with a wide variety of disabilities.

(8) Elections are not about "my vote," they are about the will of the people.

In states with electronic voting, some people have suggested that if any voter doesn't want to cast his or her vote on a computer, they should request a paper absentee ballot. But elections are not just about "my vote," they are about the will of the people--all votes. If computers are the wrong technology for elections, as I believe they are, they are wrong for all voters.

(9) You can't fix a broken democracy by throwing a computer at it.

If democracy is government "of the people, by the people, for the people," I think it is time we ask, "Where are the people?" We need to put people back into the center of our elections, and not replace citizen participation by computers.

If people knew how desperately their participation was needed, more would respond.

(10) States and big cities that use paper ballots and optical scanners.

Illinois, Chicago. 83% of the population of Illinois (10 million) votes using such systems, including Chicago. One Illinois County's rationale:
http://www.willclrk.com/votingsystem.htm#Why%20was%20the%20optical%20scan%20system%20selected?

80% of Arizona, including Phoenix.
http://www.azsos.gov/election/voter_outreach/info.htm

Michigan Secretary of State's recommendation:
http://www.michigan.gov/sos/0,1607,7-127-1640_9150-43906--M_2001_5,00.html

States that use mostly precinct-count optical scan systems also include
South Dakota http://www.sdsos.gov/2000/00pripre.htm
Minnesota
http://www.sos.state.mn.us/election/Interactive%20Election%20Guides/HTML/15.htm

Seattle:
http://www.metrokc.gov/exec/news/1998/vote421d.htm

(11) The CalTech/MIT study of voting systems found that precinct-count optical scan systems outperformed DRE voting systems in terms of residual voting errors and cost per voter.

CalTech/MIT Voting Project, http://www.vote.caltech.edu/Reports/