**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**

# Testimony of Bruce C. Funk

**Former Emery County, Utah Clerk – 23 years Election Experience**

## Vulnerabilities and concerns in considering electronic voting equipment, including optical scan, and associated election law issues

I appreciate the opportunity of giving my testimony as you consider electronic voting equipment and the associated laws that will govern their use.

You might first ask why a 23-year veteran election official from Utah would be concerned. I believe that you can benefit from my experience with optical scan voting machines and paper ballots. My purpose is only to make you aware of the vulnerabilities that I witnessed and how it took away voter confidence. The issues I wish to address are applicable to any voting machine which counts votes or tabulates the results without public oversight.

The vendor of Utah's voting machines is Diebold, later called Premier. They claim their software, equipment and any documentation as "privatized". This means they can lock out any official or others from investigating their software, voting equipment, voter registration files and any documentation including poll books and poll worker training manuals. In Utah, state laws were enacted effective June 1, 2006, making it a felony to investigate a voting machine, its software, or the tabulation software and "other" as deemed private.

However, even if a state has limited or full permission to examine their voting equipment, if the state and counties do not examine their equipment upon delivery and after maintenance, the final result is the same – election officials, candidates and voters will not know how the votes are handled, or if the votes are counted as intended.

In February, 2006, I became concerned with the new voting machines which the State of Utah required to be implemented in every county in our state. It was obvious that I needed to bring in independent, outside security experts to examine the machines' software. The most serious security problem we found was that there were three "pass worded" back doors at three different levels in the software which opened the door for malicious tampering at a previously unsuspected level.

A detailed document of the investigation is available at the web site BlackBoxVoting.org.

We found that vote flipping software could be added or activated by using the date. I personally found that the computer clock could be set for Election Day which would enable someone to add votes, but upon returning the clock to the real current date there was no log of the changes that had been made to the clock or the votes. I also found that upon concluding its work the vote flipping software removed itself.

We actually loaded other operating software onto one machine, replacing the original, and there was no log of this in the computer.

My work was incorrectly reported in the media, which said: "It was obvious there was an attempt to hack the voting machines in Emery County, but because of the advanced security of the machines we were unsuccessful." In this way the public and other election officials were misled and given false confidence.

As a result of my investigation, I was locked out of my office as an elected official after 23 years.

I am submitting this testimony in order to try to be of assistance to the Assembly of the State of New York to help you maintain honesty, integrity and voter confidence in your elections. I believe this is the essence of your responsibility as you conduct this hearing and consider your course as to how future elections in your state are to be conducted.

The most important issue in any formulation of future elections is transparency and public oversight of all election functions. If electronic machines are used to handle votes, you will lose all transparency, and all possibility of public oversight, unless you can devise some way for your election officials, candidates, and voters to ensure that every unit of your equipment counts the votes accurately on election day in some way that allows people to act as observers. I personally do not know of any way to do this with paper ballots and scanners unless the votes are manually counted immediately after the election. If you can avoid switching your elections to electronic equipment, you will avoid this entire problem that electronic machines create.