



Supplement to the testimony of Charles A. Gaston
before the Election Assistance Commission
Gaithersburg, MD, 2004 September 20

Qualifications:

I have a PhD in Engineering Science and am a Registered Professional Engineer. I worked for IBM for 28 years, and have been on the Penn State engineering faculty at the York campus since 1993. I have been writing computer programs since 1963, and since 1982 have developed many user interfaces of varying sophistication. I invented a way to eliminate hanging chads way back in 1972.

Reason for testifying:

Spurred by the election fiasco of 2000 November and by predictions that it would cost billions to fix the problems, I conceived and developed a voting technology so inexpensive that in many (if not most) counties it would cost less to use this approach than to continue with current technology. Even better, it probably is more secure, more trustworthy and more accurate than any other voting technology in existence.

Rules, standards and laws intended to remedy problems with other voting systems (unreliability, inaccuracy, voter confusion and the potential for vote manipulation) can have the unfortunate side effect of blocking this innovative approach.

It is my hope to make the nation, and particularly the Election Assistance Commission, aware that there exists a better way to vote, and to convince them that unnecessary and inappropriate barriers should not be placed in its way.

Standard thinking

versus

Innovation

Voting machines require specialized, expensive hardware.

Ordinary personal computers (even discarded ones) can become secure voting machines, or can be used to test and verify voting software.

Security is gained by secrecy.

Security is gained by openness. Nothing is secret except how any individual votes.

There is one true copy of voting results, and it is carefully guarded by voting officials.

There are many machine-readable copies of the voting results, so anyone can tally them easily, and no one can change them undetected.

SAVIOC Voting Systems
2381 Lititz Pike
Lancaster, PA 17601-3653

postmaster@savioc.com
(717) 560-5607

"Do it right the first time." 

Secretive certifying agencies are the best way to assure that voting machines work as advertised.

Completely public software that runs on readily available hardware is the best way to assure that voting machines work as advertised.

Locks, sign-offs and encryption are required to assure that voting machine software matches what was certified.

Software downloaded from the web at any time can be verified true on election day, even by people who are not voting officials.

Voting machine software is incredibly complex, consisting of a massive operating system and megabytes of specialized code.

An effective voting system, its operating system, and perhaps a hundred different ballots can fit on an ordinary diskette.

The only way to assure proper functioning of a voting machine is to add a "voter-verified paper ballot" to the "black box".

A "glass box" voting machine (where all hardware and software are public) provides greater trustworthiness without the paper.

Blind voters require sophisticated and expensive voice technology to be able to vote unassisted.


Blind voters can vote independently by using a reference ballot (Braille, large print or simple voice-on-tape) and listening to computer-generated tones indicating such things as current page and line number. (Three have done so.)

How could overly-prescriptive standards block innovative voting technology?

1. One of the easiest ways (and this is something being proposed within the IEEE P1583 standards committee) is to require all voting systems to use a proportional font! That may seem to be an innocuous requirement, but much of the simplicity and accuracy of my system results from the deliberate decision to use text mode rather than graphics. Text mode is inherently a monospaced font, where line lengths are easily calculated and properly limited. Changing to graphics mode would destroy the entire concept.
2. Another way is to place unnecessary demands on programming language or style. Such limitations might make it easier for a certifying agency to understand and follow a program, but could require the complete rewriting of something that already works flawlessly. If the software (including source code) is on the web for public scrutiny, it will be checked (regardless of programming style) much more thoroughly than one secretive certifying agency could be expected to do. The well-publicized failures of "certified" secret systems are a case in point.
3. A third way to block innovation is to create standards that are expensive to test. Major companies may have deep enough pockets to finance a certification costing a good fraction of a megabuck; innovators generally do not.

SAVIOC Voting Systems
2381 Lititz Pike
Lancaster, PA 17601-3653

postmaster@savioc.com
(717) 560-5607

"Do it right the first time." 

A request:

In deciding what standards to apply to voting machines, please keep in mind the ultimate goal: voting systems that (1) accurately record the intent of each voter, (2) preserve the secrecy of each ballot, (3) accurately summarize all votes without failure, and (4) prevent manipulation of results by anyone associated with the voting process (manufacturer, voting official, voter or hacker).

Please keep in mind also that "perfection" is the enemy of "good", and that not all that is desirable is of equal importance. Trying to patch every minute flaw in current voting systems could inadvertently slam the door on innovative systems that are better where it really counts: transparency, security and accuracy.

Further information, including completely functional software, is available at www.savioc.com.

Election Assistance Commission testimony (verbal)
by Charles A. Gaston of SAVIOC Voting Systems (www.savioc.com) 2004 Sept 20

My name is Charles Gaston. I am a Registered Professional Engineer, PhD, college professor, programmer and inventor. In a sense, my road to this meeting began in 1972, when I invented a way to eliminate hanging chads.

In November of 2000, when we still didn't know who the next president would be, and everyone was discussing chads, I mentioned in a church group that I had solved that problem decades ago. Because someone in that group worked on a newspaper, my chance remark turned into a front-page story that was picked up by the Associated Press and resulted in calls from several radio stations.

(Show New Era article)

The attention got me to thinking that maybe I could solve the bigger problem of improving voting technology substantially without straining local budgets. So I did.

This subcommittee is focusing on security and transparency. What could be more transparent than a system that uses off-the-shelf hardware and software downloaded from the web? What could be more secure from manipulation than a system in which the software and ballot can be verified correct on election day, and in which exact copies of the original results can be distributed to multiple interested parties as the polls are closed?

Such a system can be tried, tested or investigated by virtually anyone, not just those few with special access. Such a system is virtually immune to manipulation before, during or after the election. Such a system is what I offer.

(Show sandwich bag of parts)

Everything necessary to turn a PC into a voting machine fits in a sandwich bag with room to spare. Since the PC can be one of those that are being discarded daily, my approach to voting also is the only one that is actually good for the environment! I can literally rescue a PC from the dumpster and use it as a voting machine. A 20 MHz 386 with a dead hard drive is good enough.

(Get flip-card ready) (One side: red circle with \$; other side: green circle with light bulb)

True innovations flip standard thinking on its head.

<u>Standard thinking</u>	versus	<u>Innovation</u>
Voting machine hardware is expensive.		Voting machine hardware is free.
Voting software must be complex.		Voting software can be relatively simple.
Voting software must be kept secret.		Voting software can be on the web.

There is one true copy of voting results.

There are multiple true copies of results.

A special organization is required to test secret voting machines.

Truly transparent voting machines can be tested by anyone who is interested enough.

Voting officials with special access to machines and results must be trustworthy.

There is no such thing as “special access”; everything is done publicly.

Extreme measures such as locks, passwords, sign-offs and encryption are required to prevent insider manipulation.

If everything is public before and after the election, there is no opportunity for insider manipulation.

Disabled access adds significantly to the cost of a voting machine.

Wheelchair access costs nothing; access for blind people costs less than \$75, and requires no different software.

Computerized systems can eliminate overvotes completely and can clearly warn about undervotes; however, in some cases they have produced results that are unbelievable and unexplainable. Furthermore, the “black box” nature of most machines fuels suspicion that they may harbor malicious code.

It is vital that the EAC’s actions help restore confidence in voting technology, but it is important that those actions do not block important innovations – mine or others. As one specific example, suppose that a standard includes the requirement that text must be in a proportional font. (And this has been proposed within the IEEE P1583 standards group.) That seemingly innocuous requirement would rule out my system, which operates entirely in native monospaced text mode, for reasons of simplicity, accuracy and reliability.

It is my sincere hope that the EAC focuses clearly on the truly important factors of accuracy, security and trustworthiness, and does NOT get bogged down with prescriptive details that could squelch real innovation.

I’d be delighted to discuss further details of my approach with anyone.