

Charles E. Gorry, Ph.D.

455 Bear Creek Road
Colorado Springs, CO 80906-5820

Telephone: (719) 520-1089
Facsimile: (719) 328-1588
eFax: (509) 472-5275
Instant Messenger: drceccorry
E-mail: cccorry@pcisys.net
Home page: <http://boulder.earthnet.net/~ccorry>
Domestic Violence Against Men: <http://www.dvmen.org>

February 24, 2001

Senator Alice J. Nichol
200 E. Colfax, Room 329
Denver, CO 80203

Dear Senator Nichol,

I am writing to express my grave concerns about HB 01-1135 creating a pilot program for networked electronic election systems (NEES). My understanding is that bill is now before the Colorado Senate committee on government, veterans and military affairs, and transportation that you chair.

There is nothing more fundamental to our republic than an honest election.

Conversely, American history provides numerous examples of vote fraud, ballot box stuffing, and rigged ballot counting. We can thus be certain that such attempts will be made with any new system put in place.

It isn't how the citizen's vote, but who counts the votes that matters, a statement originally attributed to Joseph Stalin. The recent presidential election brought that axiom to the forefront and undoubtedly underlies the present actions of the Colorado General Assembly to undertake the pilot program mandated in HB 01-1135.

Electronic elections are not a step to be taken lightly or hastily as reflected in the six year trial period mandated in HB 01-1135. However, the protections stated in that bill are illusory and do not provide the safeguards I believe the legislature intends. It is those matters that require study and are the basis for my recommendation that HB 01-1135, as currently written, not be passed by the Colorado Senate.

I have used computers, large and small, since 1960 in many international and defense programs, both classified and unclassified. Additionally, I helped develop one of the first 100 Web sites in 1992, and for the past five years have earned my living as a relational database consultant, frequently developing sites similar to what will be required for computer voting.

Thus, I fully appreciate the need for a pilot program to provide the basis for electronic voting in the future, and feel that HB 01-1135 is a step in the right direction. However, in reading the details of HB 01-1135 I find the language vague, hasty, and poorly informed with regard to the bill's objectives.

The major shortcoming I see is the lack of understanding of computer technology.

It is thus my unequivocal recommendation that the Senate table the measure to provide time for more study and input from qualified, independent computer experts. As one such, I have outlined my concerns below.

Heading the list of potential problems is security.

Fellow, Geological Society of America

Marquis Who's Who in the World, 16th — 18th Editions

Marquis Who's Who in America, 53rd — 55th Editions

Marquis Who's Who in Science and Engineering, 4th — 6th Editions

Marquis Who's Who in the West, 27th & 28th Editions

2000 Outstanding Scientists of the 20th Century

Strathmore's Who's Who, 1998-1999 and 2000-2001 Editions

Computer security

I would hope it is evident that with computer voting the easiest and cheapest way to win an election is to pay off the programmer. HB 01-1135 makes it a felony to do so but the technology makes the present wording meaningless and impossible to detect or prosecute.

Computer hardware and security

It is unlikely the computer hardware used will be made or assembled in the United States. However, the present legislation does not require any sort of individual testing of these machines prior to placing them in service.

The American military and similar government agencies have numerous tests they run on computers before they are used in classified applications. Testimony on such testing should be sought and appropriate acceptance procedures specified in the present legislation or revisions made to § 1-5-608.5 C.R.S. to cover the requirements for such testing.

Without such control there is no hope of ensuring the computers are accurate and reliable. Computer viruses or trojan hoses may be present on the machine when purchased or inserted later via any extant communication link or insertable media, e.g., CD-ROM, with unknowable results. Such viruses could easily go undetected and would not be likely to show in the public code.

When they first started making handheld calculators Texas Instruments (TI) ran tests to see how far off the results could be before students complained. The sad answer was the students believed the calculator, or computer no matter how inaccurate TI made the results. My experience as a professor showed that, for most people dealing with a computer, GIGO means Garbage In, Gospel Out.

Voting machines **must** demonstrably produce accurate results. Manufacturers claims are worthless without independent and repeated testing. Such tests must also be required after any upgrades specified under § 32-1-808.5(i) in HB 01-1135.

Access to the hardware for testing by an independent authority before and after any election must also be provided for with the results made public. By this I mean each machine, not the entire NEES as spelled out in § 32-1-808.6(a) of HB 01-1135. Also, § 1-5-608.5 C.R.S. is inadequate to provide any real protection against vote fraud.

The problem from my perspective is that the requirements presently spelled out in HB 01-1135 are too general. As a result the proposed legislation lends itself to a "*black box*" approach to electronic elections with no one quite sure what the magic "*black box*" is doing and without the legislated authority to find out.

Computer software and security

The code used in the computer to do the vote counting, whether software or firmware, must be public information if there is to be any hope of detecting fraud. Conversely, the source code for current voting machines is proprietary information. Attempts to obtain the source code for voting programs have not been supported by the courts. Thus, the requirement for public availability **must** be spelled out in the enabling legislation.

There is a maxim that the only way to protect the computer is to shoot the programmer. Short of that the legislation must invoke restrictions on who can program voting machines. A Colorado felony is meaningless to a programmer in China. Also, an indentured servant here on

an H1-B visa is going to be quite amenable to making some virtually undetectable changes to computer code in exchange for some cash prior to their return to India.

I would strongly recommend that the legislation require that access to the computer programs used in voting machines, and access to the machines as well, be limited to American citizens, and that all such citizens undergo background and security checks before being allowed such access.

HB 01-1135 currently makes no such restriction. The widespread use of foreign nationals for software coding and hardware configuration in the computer industry ensures such individuals will have access to the voting programs and machines without such a restriction.

Computer networks and security

It makes little difference how well the hardware is tested, or the source code for the programs controlled if the computer is on a public network such as the Internet.

It should be regarded as a given that any physical connection between the voting machine and a public network will be breached. The CIA, FBI, and military computers have all been "*hacked.*"

In an election there is much more at stake than with those limited systems.

The military, and other government bodies doing classified work have the concept of an "*air gap*" to avoid the direct transmittal of information between classified and unclassified machines via an electronic network.

An example with current voting machines would be to have optical scanners count paper ballots at the local precinct. When the polls closed the scanner would print out vote totals and the election officials would then phone the results to the election headquarters where they would be entered in the voting computer. The results for the precinct entered in the machine would then be sent back to the precinct for verification.

The optical scanner itself must not have any external connection via modem or any other communication device if security is to be maintained. And once programmed and tested, such scanners must be sealed until an election is over.

For Internet voting some other variant will be necessary but the "*air gap*" concept must be incorporated into the legislation if public confidence in the system is to be established and maintained.

Secret ballots

The proposed legislation in HB 01-1135 includes some detail in § 32-1-808.5(a) about means of identifying an eligible voter. However, the present statement is incomplete.

To meet the requirements of § 32-1-808.5(a), (e), (f), and (m) what the computer **must** contain for electronic balloting is information about:

- The identity *and* address of the voter.
- That the voter has registered and is eligible to vote, e.g., a citizen, no felony conviction, etc.
- That the elector has not previously voted in the current election.
- What candidates and issues the citizen is eligible to vote for in the present election based on their current residence.

- That the voter has properly and correctly filled out the ballot.

From these requirements it logically follows that the computer must then store information as to how the individual has voted if computer balloting is used.

This violates the concept of a secret ballot.

Since eligibility to vote is dependent in part on such things as criminal records, combined with the requirement that a voter only cast one vote in an election, computer voting will surely lead to demands for a national database.

The potential abuses of such a database totally unrelated to voting are immense.

Voting information will also be sought for purportedly innocuous information such as demographics for campaign planning, e.g., how many in a given precinct or ZIP code area voted for a particular Republican or Democratic candidate, or for or against a tax increase.

The dangers of even that limited information for punitive purposes should be obvious, but the next step of determining how individuals voted will surely soon follow.

The old adage that: *“If something can be done it probably will be”* is still valid. Thus, it is essential that any legislation strictly control voting information, associated databases, and provide for rigid test requirements to insure the controls are in place and enforced. Severe penalties for violating such restrictions must also be enacted.

Limitations of computer voting

I have tabulated below some more general concerns about electronic balloting. One or more of these problems will exist with any electronic election system implemented and such issues need to be addressed in the enabling legislation. However, that is not presently done in HB 01-1135.

- In an Internet, or other network or computer balloting system, the voter marks no ballot that is preserved outside the computer.
While § 32-1-808.5(m) provides a hard copy of the elector’s ballot no means are provided for using those copies to verify an election and my understanding is current law requires ballots to be recounted by the same method originally used.
- A “*recount*” of computer ballots is meaningless.
- HB 01-1135 § 32-1-808.5(k) requires that tabulation and audit trails be contained within the computer.
There is no audit trail outside the computer and manual or other independent means of recounting or verifying the balloting is impossible with electronic balloting.
- Who can vote for what and whom depends on where the voter resided when they registered. That may not coincide with where they live now.
This is a major problem with Internet voting that would allow ballot box stuffing from Iraq, or anywhere else on the planet.
- Communication links may be accidentally or deliberately broken or manipulated to control balloting. HB 01-1135 §32-1-808.5(l) requires transmitting information over a secure network but, in fact, no such network has ever been proven to exist (including Sipranet).

For example, a dummy system could easily be put in place indicating a vote was properly sent and recorded that, in fact, never reached the computer. At the same time the dummy system could send a vote of its own to the computer doing the counting.

Or the communication link can be rigged to modify the vote in transit. Internet connections typically go through 15 to 20 separate machines enroute to their destination.

For Internet voting, vote modification may be accomplished by someone in another country not subject to Colorado law.

- Adequate testing of the myriad of ballots present in general elections, and even many local elections, is impossible as a practical matter. At present the only such limitation in HB 01-1135 is associated with votes on TABOR issues. Thus, § 32-1-808.6 is well intentioned but inadequate. Further study is required.
- Computer or communication malfunctions can cause the inadvertent or deliberate loss of electronic ballots. § 32-1-808.5(g) calls for uninterrupted availability while the polls are open but makes no provision for what rules are to followed when breakdowns do occur.
- Few, if any, poll watchers can verify the accuracy of the balloting even if source code for the voting programs is available to them (not presently the case) due to lack of expertise with said programs. That issue needs to be addressed.
- It is quite easy to present one listing of the computer code for verification while the computer is actually running a different version of the same program.

That may be done either by accident or deliberately.

- A substantial percentage of the electorate, estimated at approximately 10%, will not be able to use the computer either due to computer anxiety/phobia or other handicaps.

Efforts to ease those problems as required under § 32-1-808.5(e) and (j) are certain to increase computer bugs or provide opportunities for deliberate manipulation of the vote totals.

- Inadvertent or deliberate “errors” or “bugs” in the computer code are virtually impossible to detect unless they cause gross mistakes.

A computer byword states that all nontrivial programs contain bugs. If there are no bugs in the program it is, by definition, trivial.

Voting algorithms with complex candidacies, initiatives, precincts, special districts, etc. are not a trivial programming problem.

By the same logic it is a certainty that I have not thought of all the potential ways a NEES can be accidentally or deliberately corrupted.

- Optical scanners, or similar devices, reading hand-marked paper ballots at a local precinct are subject to errors or manipulation if they are connected to a network, e.g., through a modem, or if their software or firmware are corrupt.

If the paper ballots are recounted by simply running them through the same machine, as mandated under current Colorado law, such errors or corruption are not likely to be detected.

- Computer counts of ballots may not be accurate due to either deliberate manipulation or flaws in the software or hardware.

An example: the computer in a precinct might not recognize that a citizen was authorized to vote on a local initiative due to an oversight, or bug, in the programming.

Conversely, the voter might be presented with a computer ballot that allowed them to

February 24, 2001

vote on initiatives or candidates their address or party affiliation did not make them eligible for.

- Transferring all vote counting to a central computer makes it impossible to determine local balloting errors and enhances the opportunities to manipulate the count.
- Programmers commonly leave themselves “*back (or trap) doors*” while developing computer code to facilitate testing and debugging.

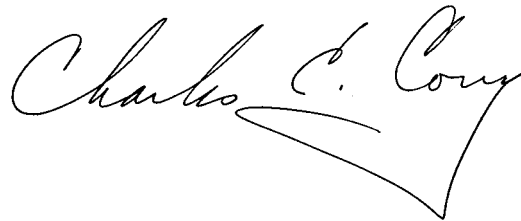
Such features facilitate later manipulation of the code, either authorized or unauthorized.

It is my hope that the comments above will cause your committee, and the Colorado Senate to carefully consider the problems inherent in a networked electronic election system (NEES) before passing any legislation with regard to this fundamentally important issue.

HB 01-1135, as passed by the House, is not up to the demands and requirements of the issue. The bill does contain important first steps that do need to be taken and provides a considerable and essential period for testing any NEES.

That such electronic election systems will be needed and used in the future is unquestioned. But with so many imponderables and known problems at present I ask in the strongest possible terms that more time be given to studying this basic issue before hastily passing superficial legislation such as HB 01-1135.

Sincerely,

A handwritten signature in cursive script that reads "Charles E. Corry". The signature is written in black ink and is positioned to the right of the word "Sincerely,".

Charles E. Corry, Ph.D., F.G.S.A.

cc: Senator Andy McElhany