Charles E. Corry, Ph.D.

455 Bear Creek Road
Colorado Springs, CO 80906-5820

Telephone:	(719) 520-1089
Instant Messenger:	drcecorry
Email:	ccorry@ejfi.org
Home page:	corry.ws
Equal Justice Foundation	www.ejfi.org

March 2, 2006

State, Veterans, and Military Affairs Committee
Colorado House of Representatives
200 East Colfax
Denver, Colorado 80203

Dear Representative:

I am writing in opposition to *SB06-062 Concerning electronic voting by certain electors who are absent from the state on election day* that was passed by the Colorado Senate and is now scheduled to come before the House State, Veterans, and Military Affairs committee.

Summary

- SB06-062 proposes to accomplish by legislative fiat what no competent and informed scientist or engineer thinks is possible with today's technology or equipment.
- This bill authorizes the use of Internet electronic mail for voting, a project analogous to one that was abandoned two years ago by the Department of Defense after expending $22 million dollars.
- The project is to be accomplished by a state department with no scientific or engineering staff, with no financial support (zero fiscal impact), and extremely limited technical and security project management experience.
- SB06-062 abrogates the Constitutional right of an elector to a secret ballot if they choose to vote by a ballot returned by electronic means.
- The demand or need for Internet electronic mail voting has not been demonstrated. Absentee voting by facsimile authorized in 2003 has not been widely used.

Overview

There is nothing more fundamental to our republic than fair and honest elections based on voting by a secret ballot.

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. Therefore, we must consider the obvious fact that, if voting by electronic mail is authorized, a U.S. general election would offer one of the most tempting targets for cyber-attack in the history of the Internet, whether the attacker's motive is overtly political or simply self-aggrandizement.

Only someone whose computer has never been hacked, or who doesn't own one, would consider Internet electronic mail (email) a safe and secure method for voting. I would hope that

Fellow, Geological Society of America
Marquis Who's Who in the World, 16th — 23rd Editions
Marquis Who's Who in America, 53rd — 60th Editions
Marquis Who's Who in Science and Engineering, 4th — 8th Editions
Marquis Who's Who in the West, 27th — 34th Editions
2000 Outstanding Scientists of the 20th Century
2000 Outstanding Scientists of the 21th Century—First Edition
Strathmore's Who's Who, 1998-1999 and 2000-2001 Editions

the widely-publicized problems with spam, anti-spam, hacking, identity theft, phishing, voter registration scandals, man-in-the-middle attacks, spyware, viruses, worms, and etc. with the Internet and email, together with common sense, would lead you to vote against this bill.

Citizens' faith in electronic voting is **not** bolstered by incidents such as one the first week of February 2006 when Republicans in Congress voted to choose a replacement for Speaker of the House Tom Delay. The initial vote resulted in more votes being electronically tabulated than Republican members of Congress. That isn't the only known incident of a voting miscount in Congress. On a May 1988 Dellums-Boxer amendment to the Strategic Defense Initiative (SDI) in the House of Representatives to kill SDI funding there were 358 ayes for the amendment and 237 nays, which added up to much more than the 435 Members of Congress. A manual recount showed the amendment was actually defeated 299 to 118 (see *www.csl.sri.com/neumann/illustrative.html* and search on Dellums). And if electronic voting can't be trusted to reliably count a few hundred votes in Congress, why should the much greater dangers of Internet voting be imposed on citizens?

Secure Electronic Registration and Voting Experiment (SERVE)

SB06-062 is not the Colorado legislature's first attempt to enable Internet voting. In 2001 HB01-1135 passed the House but was defeated in the Senate State, Veterans, and Military committee in large measure based on my testimony.

Since then, with its infinitely greater resources and engineering abilities, the Department of Defense attempted to establish means of Internet voting for military and government officials stationed outside the continental United States.in a program known as Secure Electronic Registration and Voting Experiment (SERVE) (for a review of SERVE see *www.ejfi.org/Voting/Voting-29.htm*). The eventual goal of SERVE was to support the entire population of eligible overseas citizens plus military and dependents, estimated to number about 6 million.

There is no known method by which Internet voting can simultaneously[1] be made secure, provide a secret ballot, ensure that only the eligible citizen voter is receiving or submitting the ballot, prevent fraudulent votes from being transmitted, or valid votes from being intercepted. Such systems are also subject to denial of service attacks that could well disrupt the entire voting process, as happened when Canada's National Democratic Party attempted online Internet voting in January 2003 conducted by Election.com. That denial of service attack was also associated with strong suspicions of vote rigging.

The problems with Internet voting of any kind, email or otherwise, are fundamental in the architecture of the Internet and of the personal computer (PC) hardware and software that is ubiquitous today. These problems cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough. It is probable that they will not be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet.[2]

1. It is clearly possible to *individually* satisfy the requirements for voting by electronic mail. It is the requirement that the conflicting conditions of maintaining a secret ballot while positively identifying the voter, determining their eligibility to vote on the issues and candidates on a given ballot in a particular election, maintaining ballot control (one man, one vote), and providing the voter the correct ballot are all *simultaneously satisfied* that makes the problem of Internet voting currently impossible *(see draft system architecture on page 8 for further details).*

As a result Internet voting as attempted in the SERVE program was very expensive. For the initial experiment the cost was about *$74,000 per ballot cast* in the 2002 election. The second year of the program promised to lower costs to *just* several thousand dollars per ballot in 2004 before the program was cancelled after a security review by Wagner, Rubin, Jefferson, and Simons in January 2004 (summary attached).[3]

Before the SERVE program was cancelled the Department of Defense is reported to have expended $22-million-taxpayer dollars. To me SB06-062 appears to be a renewal of the failed DoD project with the added handicap of no funding and using an even less reliable method for Internet voting than a secure browser.

Accenture

It is of interest to note that the prime contractor for the SERVE program was Accenture, who formed a strategic partnership with Election.com for the project. Accenture is based offshore in Bermuda to escape U.S. taxes and more than half their partners are not U.S. citizens.

There were grave concerns with national security in the SERVE program with regard to the contractor's ownership by foreign investors. Many of the investors in the contracting companies, who often appeared to have controlling interest, were foreign nationals. It was clear the program had all the ingredients for a disastrous breach of national security.

Just a few months ago the Colorado Secretary of State dismissed Accenture from a contract to develop a statewide voter registration database, as have many other states, and Colorado is not in compliance with the Help America Vote Act (HAVA) as a result. In December 2005 the Colorado labor department terminated another contract with Accenture after pouring $35 million into a jobless insurance program that didn't work.

If a program for Internet voting is renewed it would be logical for the Secretary of State to negotiate with the company with the most experience with the problems, i.e., Accenture. Why in the world would legislators now want to authorize a program that is quite likely to involve Accenture again?

Lost ballots

There is also the problem that anti-spam security measures on the Internet frequently result in lost email, particularly with international messages or ones with attachments. Often that occurs without the sender or the recipient being aware their messages were blocked. With SB06-062 that means lost ballots.

Capabilities of the Colorado Secretary of State

Contrast the experience of the Department of Defense, with its comparably infinite resources, a multimillion dollar program with numerous scientists and engineers involved, with what SB06-062 expects of the Colorado Secretary of State:

- There is no engineering or scientific staff.
- The director of elections[4] is an attorney with no technical experience or education.

---

2. Banking transactions, purchases, and other financial exchanges are routinely made on the Internet using HTTPS, a more secure and encrypted version of the Hyper Text Transport Protocol (HTTP). For more information see *en.wikipedia.org/wiki/HTTPS.* The difference is that in these exchanges an unbroken transaction record is required. In voting the transaction record must be broken to maintain a secret ballot.
3. For more information on voting security problems I refer you to the complete security report on the SERVE program at *servesecurityreport.org/paper.pdf.*

While SB06-062 is framed in terms of the Secretary of State simply establishing procedures for email voting, that is a sham without the technical resources to do so in a safe and secure manner. Based on my experience as a system and database architect, on page 8 I've roughed out the system requirements for electronic mail balloting. Even if the program outlined there was successful it quite obviously would be extremely costly, in direct conflict with the no fiscal impact reported for SB06-062.

And if there is no intent to implement such a dangerous experiment as email voting, with its attendant costs, why is this legislation necessary?

Insider security attacks

It is well established that any computer-based voting system is easy to rig by company insiders and vulnerable to attack by outsiders. An insider attack is not an abstract issue considering the following report from the January 8, 2004, Denver Post, that occurred after I was asked by a candidate to look at irregularities in the November 2003 Denver school board election when it was found that there was a greater than 30% undervote in her race.

Examination of the ballots used in that election revealed problems with markings on the back of the ballot that may have caused the undervote when read by the Sequoia optical scanner.[5] However, we were assured by Mr. Thomas Cole at a meeting with the Denver Election Commission on December 12, 2003, that his setup and testing would have caught any such errors prior to the election. At the time Thomas Cole was the lead technical expert for the Denver Election Commission and had programmed and tested the Sequoia voting machines for the November 2003 election.

The following was published after that meeting:

City employee charged with theft

Denver Post, Metro briefs, Thursday, January 8, 2004 — An employee with the Denver Election Commission was charged Wednesday with felony theft, forgery, and embezzlement.

Thomas P. Cole, 30, is accused of stealing more than $44,000 by forging payment vouchers and buying computers and other electronic equipment, which he took home for personal use, said Lynn Kimbrough, spokeswoman with the Denver district attorney's office.

Cole came under suspicion during the course of a routine internal audit of purchases, according to the commission, and he has been placed on "investigatory" leave.

The alleged crimes took place during 2003, Kimbrough said.

The problems described above were difficult to discern even with paper ballots available for direct examination. Election manipulations by an insider like Mr. Cole with Internet electronic mail balloting would be virtually impossible to detect.

4. Bill Compton and Drew Durham, the former HAVA director in the Secretary of State's office, helped draft the state request for a computerized voter-registration system, served on the committee that chose Accenture and helped negotiate its contract without letting anyone bid for the job. Durham later moved to the Colorado Department of Labor and Employment where he was also involved with the failed Accenture contract there. See Denver Post, Denver &The West, December 21, 2005, and January 4 and January 12, 2006.
5. Later events have determined that there are also problems with the fold in mail-in ballots interfering with their being accurately read by optical-scan voting machines.

Secret ballot

Section 8 of the Colorado Constitution mandates that:

> "All elections by the people shall be by ballot, and in case paper ballots are required to be used, no ballots shall be marked in any way whereby the ballot can be identified as the ballot of the person casting it."

Clearly the intent here is to maintain secret balloting for all voters, something impossible with Internet voting via email. However, section 1 on p. 3, lines 3-7 (sans strikeouts) of SB06-062 as passed by the Colorado Senate states that:

> "(b) The instructions for completing an absentee ballot pursuant to this section shall inform the elector that an absentee ballot returned by electronic means is not a confidential ballot."

If this dangerous legislation is passed and implemented, at some point it is certain that some soldiers and sailors will not be able to vote unless they surrender their right to a secret ballot.

A secret ballot is the cornerstone of democracy and one of the most effective methods yet invented of keeping tyranny in check. I do not believe the legislature has the authority to abrogate such a basic Constitutional right by way of legislation. The right to a secret ballot must be preserved.

There is also more than passing interest in email or any other messages sent by overseas military personnel, many of whom have high-level security clearances and are working on classified projects. In time of war *all* military mail is subject to censorship. Thus any email ballots of these military men and women will be open to review by higher command and some level of intimidation, direct or indirect, should be presumed, compelling these people to vote a politically-correct party line.

In addition, copies of email messages, together with identifying header information are kept on each and every server used to forward the message. Typically that involves 10 to 20 servers for every message sent via the Internet. Also, copies of the email are kept indefinitely on both the sending machine and the receiving machine where they are available to anyone with administrative privileges for those machines. Both the FBI, with their Carnivore program, and the National Security Agency (NSA) monitor international emails as well and any other man-in-the-middle on any of these servers has access to the ballots as well.

That is hardly the ideal we desire for a fair and honest election and clearly violates the rights of electors to cast a secret ballot.

Where is the need for electronic mail voting?

I am also at a loss as to the demand for such legislation? As the bill is presumptively designed chiefly to aid deployed active-duty military to vote I assume El Paso County would likely be a primary area in Colorado that would utilize Internet voting. After the passage of legislation in the 2003 session permitting balloting by facsimile machines, which SB06-062 now proposes to modify and expand, I asked the El Paso County Clerk how often electronic voting had been used. I received the following response:

From: "Susan Russo" <susanrusso@elpasoelections.com>
To: "'Dr. Charles E. Corry'" <ccorry@ejfi.org>
Subject: RE: Ballots received by fax

Date: Wed, 8 Feb 2006 14:57:17 -0700

Dear Dr. Corry,

In the 2004 General Election, we had 120 UOCAVA[6] electors return facsimile ballots. Please keep in mind that these are not all overseas electors. Military service member and spouses that are absent from the state can also utilize this option. Of the 120, we had 5 electors that are overseas, no longer paying Colorado State Taxes that voted by facsimile ballot for only Federal offices.

In the 2005 Coordinated Election, we had only 2 individuals (UOCAVA) that cast facsimile ballots. True overseas electors are not eligible to cast ballots in Coordinated Election (no federal offices on that ballot).

Best regards,
Susan A. Russo
Election Consultant

Extrapolating El Paso County's experience statewide suggests perhaps 40 ballots were received by fax in 2004 from overseas. There is a very limited demand for electronic balloting to date and even an order-of-magnitude increase in 2006 would be under 400 ballots statewide.

One might make the argument that today computers with email capability are more widely available than fax machines and thus more people would email ballots than can fax them. However, while a fax transmission is relatively secure,[7] email is not. Nor are the individual PC's or the network used to transmit an email ballot to be trusted.

Inasmuch as any communication by military personnel in time of war is subject to prior censorship, it is unlikely voting by any electronic means will be popular with soldiers and sailors.

Thus, SB06-062 does **not** appear to be driven by any pressing demand or need of our military men and women.

I see no reason why service members within the United States cannot continue to use the well-established practice of absentee voting by U.S. Mail. It is also my understanding that the U.S. Postal Service has a program in place to deliver military absentee ballots by Express Mail from overseas.

6. UOCAVA — Uniformed and Overseas Citizens Absentee Voting Act. For details see *www.usdoj.gov/crt/voting/misc/activ_uoc.htm.*
7. A fax transmission can be intercepted but it is more difficult from a practical standpoint as the telephone system is much more secure than the Internet.

Fiscal impact

Currently it is claimed SB06-062 carries no fiscal impact. I am at a loss as to how the Colorado Secretary of State will implement a program that has previously defeated legions of scientists and engineers, and on which the Department of Defense spent $22 million before dropping the program, with no fiscal impact?

Clearly Internet email voting as contemplated by SB06-062 would cost millions to adequately implement even in cooperation with other states or the federal government. And the likely use by UOCAVA voters would be minimal based on present experience.

Is it really in Colorado's best interest to spend thousands of dollars per ballot cast to provide the minimal convenience of Internet voting via email? In the very great majority of cases the U.S. Post Office has been handling absentee ballots from overseas and at home for many years now without major problems. Further, the Post Office is working diligently to improve even their present high standards.

Most problems with absentee ballots don't originate within the postal system but in the county clerk's office, e.g., absentee ballots received but not counted. SB06-062 certainly doesn't address those problems but quite definitely would make the life of the county clerks more complex, costly, and difficult with yet one more new and untested method and associated technology. And there is no funding for the counties to make the computer hardware and software upgrades sure to be necessary under SB06-062.

SB06-062 is therefore either a solution in search of a problem or another likely pork project for Accenture or a similar contractor. Past experience suggests the latter.

For all the above reasons I urge you to vote **No** on SB06-062 *Concerning electronic voting by certain electors who are absent from the state on election day* when it comes before you.

Sincerely,

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

Encl:

Rough draft of system architecture for email voting

Summary of SERVE security experts findings

Curriculum vitae for Charles E. Corry

Rough Draft Of System Architecture For Email Voting (SB06-062)

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

The following draft is based on 30 years of project management experience and many years of system and database design and architecture work.

The first requirement is that basic voting principles (see *www.ejfi.org/Voting/Voting-8.htm*) be satisfied.

One man, one vote — demographics

- Elections are generally handled by the county clerk for each county independently of other counties although in a few cases cities may run an election independent of the county clerk. However, the county clerk is still responsible for maintaining the list of registered voters.
- Colorado has 64 counties with populations ranging from 550,000 down to about 800. Obviously the smaller counties don't have the financial and technological resources the large counties do but a larger percentage of their young men tend to go into the military.
- In smaller counties on the Western Slope upwards of half the young men in the Mormon communities go on a mission. So larger numbers of missionaries are likely from smaller counties.
- Thus, equal rights and access demands the small counties have the same facility for electronic voting that the larger counties do but no funding is provided.

County impacts

- Email voting obviously requires valid email addresses that are not currently available to county clerks. Also, about one-third of email addresses change within a given year. High maintenance.
- Encryption would also require storing keys to send and decode ballot for each voter and ballot style. High maintenance and often beyond skills of county clerks or local IT personnel.
- Voting based on physical address. People often move but keep the same email address. How is this to be dealt with?
- Secure mailserver needed for each county. High cost to maintain network, security, and upgrades.
- Must be capable of recognizing and fending off denial of service and other attacks.
- Transparency: System must be available for public inspection and review. Security conflicts.

Emailing ballot

- Electronic ballot must have some way to identify it as coming from the voter's county clerk, e.g., a watermark in an Acrobat PDF file if the voter is to print and fill out and mail back a paper ballot, or a digital signature for a public key held by the county clerk. Required to minimize spoofing or fooling the voter into thinking they have voted when they haven't or using a fake ballot to find out how an elector would vote.
- Electronic ballot must contain unique identifier for ballot control. Essential to stop ballot box stuffing.
- An election commonly has 50-75 different ballot styles at least in the larger counties. Electronic ballot and encryption key would be required for each style and voter must get the proper ballot based on their residence.

- Many email addresses do not allow attachments to messages. Attachments may also cause a user's mailbox to overflow preventing them from receiving the ballot.
- To ensure voter gets the ballot, options are needed if voters email box (disk storage) is full or message bounces. Return receipt needed but many users don't respond.
- Public Internet transmission is only option. Even for military voters the Department of Defense is extremely unlikely to allow use of classified facilities or networks.
- Ballots must be usable on all common computers and operating systems: Currently that would include at least Microsoft (Windows 98 through XP), Macintosh (OS 7 through 10), Linux, and UNIX (several flavors). High maintenance required as various operating systems are upgraded.

Marking ballot

- For ballots to be returned electronically voter must be able to open and mark ballot on any common computer with common operating system.
- Voter must not be able to alter or erase unique ballot identifier.
- Voter must be able to reopen ballot after closing and be able to make changes to their votes.
- Once sent to county clerk the marked ballot must erase itself from the user's computer and also from any server en route to county clerk to preserve secrecy.
- Ballot must be encrypted during transmission to minimize value of intercepts and preserve ballot secrecy. Likely this would require voter to obtain encryption key and that would cause confusion among technology-challenged voters.
- Handicap accessible. What handicaps electronic voting methods need to handle is yet to be defined.

Counting ballots returned by electronic mail

- Date and time stamp for receipt of ballot. Requires county clerk's mailserver to be connected to network time server.
- Unique identifier for ballot received must be matched with ballot emailed to voter.
- Inform voter that their ballot has been received and successfully decoded. Provisions for handling problems decoding ballot needed.
- Remove unique identifier from ballot before counting or transferring. Could be printed and then identifier removed from top of ballot as done with other ballots.
- Count votes in presence of at least one representative from each major party plus interested poll watchers.
- Tabulate number of ballots returned by email and fax for UOCAVA.

My guess is that the above outline doesn't cover half the problems associated with Internet electronic mail voting. Actually, the SERVE program, which was browser based, is starting to look simple and cheap.

There is an ancient engineering principle called **K.I.S.S.** (Keep It Simple, Stupid). Electronic mail voting certainly violates that principle.

Another fundamental principle is: **If it ain't broke, don't fix it.** We have a tried and true method for absentee voting that has provided quite satisfactory service to overseas citizens still eligible to vote in Colorado for many, many years. While the U.S. Mule is a bit sway backed he's still getting up and over the divide most winters. Lets stick with snail mail as it's cheaper and easier for everyone.