

Debra Bowen
California Secretary of State
1500 11th. St.
Sacramento, CA 95814
7/28/07

Dear Secretary Bowen,

I think Electronic Voting is a bad idea.

I voted in the last few elections using the Ink-A-Vote card system with Electronic Verification. The card is both the ballot and the paper trail all in one. The electronic verifier machine tells me immediately of any card errors. The cards represent a distributed, simple, open voting system, and very difficult to influence or damage.

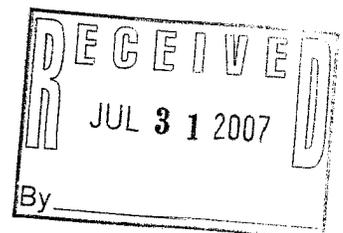
Electronic voting systems suffer from vendors that won't tell us how they work, no simple paper trail, shaky security tools, and now, as of the New York Times article by Christopher Drew dated July 28th, vulnerable to computer hacking.

I'm perfectly willing to wait for ballot transportation and a card reader to count the votes. I don't need instant access to what may easily be a compromised tally.

Thank you,



Greg Kozikowski



From: Mclean, Marianne
Sent: Monday, July 30, 2007 11:06 AM
To: Voting Systems
Subject: Appalled

I was appalled to hear that hackers were able to break through the security of voting machines here in CA. How can I trust that my vote really counts when it could be arbitrarily changed by someone with their own agenda. I would rather go back to the old way of voting than feel more discouraged about my government than I already do. Please fix this problem.

Sincerely,
Marianne McLean

From: Barb Bruns
Sent: Sunday, July 29, 2007 5:16 PM
To: Voting Systems
Subject: No Dre's

With respect, I urge you to not allow Dre's for casting votes. We need a transparent, counted, paper *ballot system - essential for our democracy.*

Barbara Bruns

07/30/2007

From: Allegra
Sent: Sunday, July 29, 2007 12:05 PM
To: Voting Systems
Subject: Meeting on voting machines on Friday

Ms. Bowen was voted in to solve the voting machine problems. She must argue to have the voting machines decertified. It is the most important issue because the rest of the country will be watching California, so we need to get this right. Go for it Ms. Bowen. We're counting on you.

From: Bob Elyea
Sent: Sunday, July 29, 2007 9:46 PM
To: Voting Systems
Subject: Hackers Break Into California Voting Machines

Dear Ms. Bowen,
Thank you for investigating these machines and finding this out at this time. Obviously this strengthens our case of what happened in the 2004 election in Ohio and other places. I hope everyone on Capital Hill will take note of what has been exposed by you in California. Keep up the good work!

Sincerely,

Robert Elyea

07/30/2007

From: Nicole Holland
Sent: Sunday, July 29, 2007 4:59 PM
To: Voting Systems
Subject: hacked

I'm appalled that our voting machines can be hacked into and votes altered. We need a paper trail. There should always be a paper ballot to verify that the correct vote was entered into the tally.
Nicole Holland

07/30/2007

From: smhslgdg
Sent: Sunday, July 29, 2007 8:05 PM
To: Voting Systems
Subject: Electronic voting machines

To Deborah Bowen:

I support any moves to go to paper ballots, and to the decertification of the touch screen and other electronic voting machines. The recent tests showing that these machines are 'hackable' weaken any remaining confidence in our election results.

Please give us paper ballots, with the ability to recount if necessary. There is no need to declare winners the morning after an election; use exit polls as indicators and give final results a day or two later if necessary.

As our system now exists, there can be little joy in exercising our right to vote when results have been so questionable and so harmful to our country in recent years.

Thank you for your hard work - my vote for you was one success!

Jonna Allen

AOL now offers free email to everyone. Find out more about what's free from AOL at AOL.com.

From: Joan Mason
Sent: Sunday, July 29, 2007 12:08 PM
To: Voting Systems
Subject: DRE Decertification

Dear Secretary Bowen:

We are very happy that you have had an independent "Top to Bottom Review" of the California voting systems. For too long a cloud has hung over the voting system used in recent elections in California as well as other states. In light of the fact that these independent, state approved teams of analysts were able "to bypass both physical and software security measures in every system tested" , we call on you to decertify these machines in the state of California.

Perhaps it is time for a transparent, counted paper ballot (not a ballot with a paper trail) to be used in future elections. It is time to bring confidence in the voting process to California. Thank you for your time.

Joan Mason
Walter Mason
Victoria Mason

From: Chuck Garner¹
Sent: Monday, July 30, 2007 8:37 AM
To: Voting Systems
Subject: Diebold optical scanners in Lassen County

Dear Secretary of State Bowen:

Here in Lassen County we are forced to use Diebold voting machines, and the only way we can get rid of this corruption is for you to deny certification for their use. I've been writing letters to our local weekly, the Lassen County Times advocating a return to hand counted paper ballots at the precinct level but without your denial of certification nothing will get done. Thank you in advance for any consideration you may give to this request.

Sincerely,
Chuck Garner

07/30/2007

From: JOANNE N NAGY
Sent: Monday, July 30, 2007 4:22 AM
To: Voting Systems
Subject: decertify

Dear Secretary of State Bowen

We need to have the votes counted as voted. We need to know that those elected in California voting are the ones actually preferred by the people who bother to vote.

The voting turnout for non-presidential voting days is so low that a little hacking could bring us results not chosen by the voters in Calkifornia.

There is still time for all the precincts to implement a paper ballot for all 3 of next year's elections.

In my opinion, there is no need to rush with the results of an election. A few days later would be fine since no one will take office right away anyway.

So, revert to paper ballots and let us get on with rebuilding our democracy by honestly chosen representatives.

Joanne Nagv

From: Ann Stiles
Sent: Sunday, July 29, 2007 11:35 PM
To: Voting Systems
Subject: Decertify voting machines!

Dear Ms Bowen,

Thank you for all the work time and effort you have given to us citizens. Please decertify all electronic voting machines. Many people do not know or understand that our most important civil right our vote has been privatized.

Our government has required us to purchase cheap hackable machines at high prices. A win for the corporations and we lose, the right to count our votes. Our country has voted on paper ballots counted by the people for over 200 years. If we need more counters many citizens will volunteer.

Sincerely, Ann Stiles

07/30/2007

From: Richard Duncan
Sent: Sunday, July 29, 2007 6:50 PM
To: Voting Systems
Subject: Decertify the machines!!!!

I want you to know that I was greatly heartened when you ran for office with the professed goal of determining the reliability of the touch-screen voting machines. I am doubly heartened to learn the results of your recent tests of same and to determine that the voting machines are indeed "easily hackable." Count on me as a San Diego resident to back you 100% should you take the courageous step of de-certifying the use of those machines for the upcoming election. Those machines have made a mockery of our once grand election process.

I realize you will be under great pressure to retreat from your election goal, but keep in mind that those who are likely to want to keep the machines MUST be limited to one vote each (rather than the hundreds or perhaps thousands they will have, if the machines are used.)

Frankly, I recommend we use paper ballots this next election, as a check and balance on any electioneering fraud possibility. Lets have an honest, straightforward election this next time. The stakes are too high to risk any system which can be manipulated behind the scenes.

You are to be commended on your actions and you are making the title "Public Servant" once again an accurate statement. No matter what you may be threatened with, stand firm in the face of adversity.

Rev. Dr. Richard Duncan

Get the free Yahoo! toolbar and rest assured with the added security of spyware protection.

<http://new.toolbar.yahoo.com/toolbar/features/norton/index.php>

From: margarita
Sent: Sunday, July 29, 2007 12:25 PM
To: Voting Systems
Subject: De-certify for Democracy

Esteemed Secretary Bowen,

Please de-certify the touch-screen voting machines.

Matt Bishop's report (albeit incomplete) confirms what many California voters have long suspected--the machines are easily manipulated by perons with the know-how and the intent to subvert the will of the voters.

Paper ballots are the only verifiable means of ascertaining the wil of the voters. A so-called "paper trail" is a misleading ploy that attempts to infuse public confidence in a voting system that can still be manipulated.

Tha manufacturers of these machines (such as Diebold, Hart, and Sequia) should NOT be given a second chance. They are not trustworthy. Thus, conditional re-certification is not an option that will assauge public confidence.

Please stand up to these powerful interests and fight for the cornerstone of democracy--votes that are counted as they were cast. Regardless of political stripe.

Thank you very much for your dedication to democracy.

Margarita

From: Marilyn Cummings
Sent: Monday, July 30, 2007 12:33 PM
To: Voting Systems
Subject: decertification of HACKABLE voting machines

Dear Ms. Bowen,

Why do we even need any discussion?

The right to vote and to have our votes counted accurately is the very foundation of our Freedoms. There is nothing else if we lose these rights.

I feel our last 2 elections were fixed and look at us now. The Constitution is in shreds. I know of violations myself which I reported and never received any return calls, etc.

Unbelievable!

Please do not let us be the generation who brought an end to our wonderful freedoms outlined in the Constitution given to us by our Founding Fathers.

We have lost the media, ethics, most of representative government, please let us at least have an honest vote for our children's sake so we can preserve the "government of the people".

Keep America alive! Decertify and let us go back to paper which served us well for 200 years and is still used on most, if not all, other countries.

Don't be naive, these corporatists are bent on owning the country.

Marilyn Cummings
San Diego

From: Jim Eldon
Sent: Monday, July 30, 2007 1:44 AM
To: Voting Systems
Subject: complete transparency required

Honorable Secretary of State Bowen,

You were quoted in the L.A. Times saying, "Our very existence as a democracy is dependent on our having voting systems that are secure, reliable and accurate."

No system is as secure, reliable and accurate as a system using paper ballots, publicly hand-counted at the precinct.

For the sake of our Democracy, I urge you to decertify all computerized voting and vote-counting machines and establish such a paper ballot system.

Jim Eldon

From: Stephanie Remington
Sent: Sunday, July 29, 2007 9:35 PM
To: Voting Systems
Subject: ban DREs -- require paper ballots

Dear Ms. Bowen,

Thank you for requesting a study of DRE voting machines. The results of this and other studies makes it abundantly clear that these machines can be (and have been) compromised all over the United States. The integrity of our democracy, therefore, has been similarly corrupted.

It is also obvious that in most situations there is no remedy for fraudulent totals resulting from manipulated machines, because evidence of it can be erased during their rigging. A paper trail produced by a corrupted machine is as fraudulent as the electronic result. And it is impossible for a voter to verify whether the vote s/he casts by this method is counted by the machine as the voter intends. It's insane to have to guess or hope that vote totals are accurate.

The key is to determine election results by counting verifiable paper ballots to determine election results. Storing a "trail" of unverifiable totals produced by potentially corrupted DREs, in case anyone demands that a few of them be counted makes a sham out of democracy.

I will not trust the results of any future election until DRE voting machines are banned and votes are cast on paper ballots – either mechanically marked or produced by a non-tabulating electronic voting machine that prints a ballot which is submitted for counting.

Please ensure that California mandates paper ballots – not a paper trail – for all upcoming elections.

Thank you.

Sincerely,

Stephanie Remington

07/30/2007

From: DEMOREP1
Sent: Saturday, July 28, 2007 11:49 AM
To: Voting Systems
Subject: PAPER MAIL BALLOTS NOW

PAPER MAIL BALLOTS NOW -- regardless of ALL of the MORONS who love having hackable E-voting systems (loved also by the domestic and foreign hacker ENEMIES of Democracy -- especially Stalin and Hitler type tyrants).

Oregon Vote by Mail ---- NO lines on Election Day (with NO rigged UNEQUAL voters per E-voting machine -- such as in Ohio 2004).

<http://www.sos.state.or.us/executive/votebymail.htm>

Get a sneak peek of the all-new AOL at <http://discover.aol.com/memed/aolcom30tour>

From: Dedavis123
Sent: Sunday, July 29, 2007 4:11 PM
To: Voting Systems
Subject: Please decertify

Dear Sec. of State Bowen:

Cannot urge you strongly enough to please banish electronic, computerized voting machines in California --- P L E A S E ! -- especially since a Univ. of Calif. Berkely study, reported in the San Diego Union-Tribune Friday 7/27/07 (FRONT page), found the machines are easily hackable, even by meddlers with low computer skills. If Canada can do it, why can't we -- completely PAPER balloting and hand counting or at least thoroughly reliable, verifiable OCRs (optical character readers) with complete paper trail, P L E A S E !

Nothing is of more importance to the rescue of democracy in California and our country.

REGISTERED D E M O C R A T WHO VOTED FOR YOU 11/06 >

David E. Davis

Get a sneak peek of the all-new AOL at <http://discover.aol.com/memed/aolcom30tour>

From: Gary Smith
Sent: Sunday, July 29, 2007 3:38 PM
To: Voting Systems
Subject: Written Comment, Top-to-Bottom Review

Gary Smith

Greetings:

Please find my enclosed written comment below, Thanks.

The Secretary of State (SOS) Top-to-Bottom Review is a good idea but unfortunately is leaving a huge hole. This review of our voting process will further ensure California voters their votes are counted accurately and securely when completed. I just wonder when the Top portion of the Top-to-Bottom Review is going to take place? The SOS is currently reviewing the bottom level, the voting machine at the polls, and the middle level, the vote counting computers at the 58 county elections offices. Hacking at the bottom level would gain some votes but probably would not change a state or national election. The hacker could use the voting machine at the bottom level to get at the middle level, county vote counting server. The middle level county computer could maybe change the outcome of a statewide or national race, definitely not acceptable even if the outcome was not changed. But the big prize is the top level, the SOS vote counting computer in Sacramento with 8 million votes. Change those results and now you have a real chance of affecting the outcome of a big election and you might not get caught due to the large numbers. This could make the risk of going to real federal prison for rigging an election worth it. Is the SOS vote counting computer secure? Will there be red team testing of the SOS vote counting system? Will the code review team be looking at the SOS system? How do the counties get their data into the state computer? The top level of the voting system, (SOS) should be looked at just as closely as the bottom and middle level. Secretary Bowen stated that "My goal is to have election results that are beyond question or doubt". I hope the complete review gets done before the February Presidential Primary election so the voters can have full confidence in our voting system and our officials.

07/30/2007

From: John
Sent: Sunday, July 29, 2007 10:05 PM
To: Voting Systems
Subject: Voting

"Dear Sec. of State Bowen:

I cannot urge you strongly enough to please banish electronic, computerized voting machines in California --- PLEASE! Especially since a University of California / Berkeley study, as reported in the San Diego Union-Tribune on Friday, 7/27/07 (Front page), found the machines are easily hackable, even by meddlers with low computer skills. If Canada can do it, why can't we? -- Completely PAPER balloting and hand counting, or at least thoroughly reliable, verifiable OCRs (optical character readers) with complete paper trail. PLEASE!

Nothing is of more importance to the rescue of democracy in California and our country.

Signed: John F. Thomas, A REGISTERED DEMOCRAT

From: hacheson26@
Sent: Monday, July 30, 2007 11:39 AM
To: Voting Systems
Subject: Voting Systems

Ms. Bower,

Please Decertify the electronic voting machines. I want paper ballots only in California elections.

From: kathyF
Sent: Sunday, July 29, 2007 11:10 PM
To: Voting Systems
Subject: voting systems

Honorable Debra Bowen,

We are being asked to trust our elections to computers found to have numerous security and reliability problems, run on secret, proprietary software, written and owned by private corporations with no way to independently verify our votes.

You know what happened in 2006: Voting machines not working at precincts nationwide creating hours-long waits to vote, verified vote switching in many areas, in Sarasota, Fl alone --- 18,000 votes LOST in the congressional election due to problems with paperless, electronic voting machines (DRE's). We can't afford any more of these catastrophes, we cannot let that happen in '08, there must be a ban on Direct Electronic Direct Recording Electronic (DRE) touch-screen voting machines .

a.. Paper Ballots --- ALL voting machines must produce a paper BALLOT, not just an unverifiable paper trail

b.. Audits --- ALL voting machines must be audit-able and audits mandated in close races.

c.. No Secret Source Code --- ALL voting machine vendors MUST make the machines' software available for inspection

d.. Ban on Wireless Devices --- Prohibits wireless technology in voting machines

ALL VOTES MUST BE COUNTED CORRECTLY IN EVERY ELECTION, including all mail in and absentee ballots.

Kathleen Percy

From: Jeffrey Vance
Sent: Monday, July 30, 2007 4:17 AM
To: Voting Systems
Subject: voting system test result

Dear Ms Bowen,

Thank you for doing this. Its why we elected you. If we can't even have faith in our voting system, our democracy becomes a farce.

But be strong! Huge pressures from the interested parties will never be as powerful as the millions who believe in the importance of what you are doing. Stay strong and we will NEVER leave you!

If decertification is the only way to ensure secure voting, DECERTIFY. Pencils and paper are fine. We're behind you. We've got your back. Go Girl!

Jeffrey Vance

From: Elisaveta Wrangell
Sent: Monday, July 30, 2007 6:55 AM
To: Voting Systems
Subject: Voting machines

Dear Secretary of State Bowen:

Many thanks for holding a hearing on electronic voting machines. They have been a concern to many of us citizens for some time.

Any system that can be altered by the touch of one corrupt hand is not a viable system for a democracy. Psychologically and logistically, it is far more difficult to persuade a group of vote counters to falsify vote results (and openly acknowledge their trespass among themselves) than it is to persuade one predisposed soul to falsify results on his own and in secret.

Hand counting is not a long process, it is infinitely less costly, and for it now seems to be the only system that remains true to the spirit of checks and balances.

Sincerely,

Elisaveta Wrangell

From: Skip Estes
Sent: Sunday, July 29, 2007 11:55 AM
To: Voting Systems
Subject: voting machines

Please de-certify these voting machines! We need a hand counted paper ballot period. We should never again have Corporate control of our elections...

Ellis Estes

07/30/2007

From: Dolores Bialecki
Sent: Sunday, July 29, 2007 7:21 PM
To: Voting Systems
Cc: Dolores Bialecki
Subject: Voting machines

Secretary of State:

We the citizens are extremely concerned that we have lost our vote. I implore you to get rid of these hackable machines so we can regain some confidence in the integrity of the vote.
Thank you for your work toward that goal.

Dolores M. Bialecki

From: David
Sent: Monday, July 30, 2007 12:07 PM
To: Voting Systems
Subject: Voting Integrity

Dear Secretary Bowen:

My message is simple and straightforward.

Decertify all the DRE's existing in California.

Demand hand-counted paper ballots.

The monies the Counties set aside for the purchase of the DRE's can be used to pay for staff to count the ballots per precinct.

Or, simply ask for volunteers to give some of their time to count the ballots in each County and have the count monitored by a neutral third party, not the ROV's. They simply declare the winners and losers.

I reside in San Diego County. The ROV was a long-time employee of Diebold Corp. The Deputy ROV was involved in the Cuyahoga County, Ohio voting fiasco. I do not trust their impartiality and honesty in the coming elections.

Thank you,

David Zegler

From: debslp
Sent: Monday, July 30, 2007 10:49 AM
To: Voting Systems
Subject: voting fraud

Dear Ms Bowen

Pleeeeeeze stand on principle-not politics and DE-Certify these machines-use the science and not the politics-our democracy depends on people with the courage of their convictions-even if they might be convicted for their courage-do the right thing.

Sincerely,
Deborah Storton

07/30/2007

From: Larry & Vivian Sherrill
Sent: Sunday, July 29, 2007 8:07 PM
To: Voting Systems
Subject: Verifiable voting machines

Dear Ms. Bowen:

I voted for you in 2006, and I feel confident that you must feel as I do about the recent University of California study regarding computerized voting machines. They've been shown to be hackable by even people who have limited computer skills. These machines are NOT dependable.

Our democracy must be protected, and that means protecting the integrity, verifiability, and secrecy of our vote.

Please decertify these suspect electronic, computerized voting machines, including (but not limited to) Diebold.

I support completely paper balloting, and even hand counting. If machines must be used, they should be thoroughly reliable, verifiable OCRs with a complete paper trail.

Please.....act to protect our vote.

Thank you,
Vivian Sherrill

From: Wren Osborn
Sent: Sunday, July 29, 2007 9:41 PM
To: Voting Systems
Subject: Use of electronic voting machines

Nothing is more important to our democracy than our knowledge that our vote is counted and counted correctly. We must have faith that our voice will be heard. For years now we have read reports and seen videos documenting problems with electronic voting machines. Secretary of State Bowen has just told us that the machines can be hacked into. So I really don't understand why we are still talking about using electronic voting machines. Yes, paper ballots can go missing, but it's a lot harder to rig an election with paper than with computer chips.

In addition to their vulnerability, electronic voting machines are expensive to buy, are prone to having problems during an election, require expensive maintenance and storage, and cause difficulties for poll workers. (And poll workers cannot prevent hacking, especially when their attention is on helping people vote.) And electronic voting machines do not, contrary to popular belief, follow the HAVA rule of access for the disabled. For what they cost they should guarantee accuracy. They don't and can't so I'm for using paper ballots. They're a lot cheaper. They are a paper record in and of themselves. And I am for hand counting.

Wren Osborn

From: Gary Fariss
Sent: Saturday, July 28, 2007 4:02 PM
To: Voting Systems
Subject: Top To Bottom Review Public Hearing comment

It's a mess!

The introduction of electronic voting machines to our elections has opened a pandora's box of complexity that defies cost-effective, hacker-free solution. My suggestion:

Throw them out! Call a computer recycle company and have them hauled away.

Move to all mail-in elections. You already have to print absentee ballots for 42% of the voters. You already have the machines to read and tally those ballots.

Get rid of the Diebolds, Harts, and Sequoias. They'll be obsolete in a few years anyway.

Shut down the polling places, they belong to an earlier century.

Insure that the absentee ballot reading machines are open-sourced. All specifications and software should be available for anyone to examine, analyze, and reproduce.

Insist that all counties implement the same process and procedures.

Setup glass rooms on the stages of auditoriums so that anyone can watch the ballot counting machines being fed and the results being produced.

Close the loop by creating a website wherein a voter can submit his ballot number and insure that his ballot has been counted.

It's a no-brainer!

Regards,
Gary B. Fariss

From: carolynmyhre
Sent: Sunday, July 29, 2007 12:49 PM
To: Voting Systems
Subject: Remove Touch Screens

Dear Deborah Bowen,

As a voter (for you) I would like to thank you for following up on your promise to investigate voting machines. I would like to encourage you to outlaw touch screen machines at this time, and possibly forever. Please bring back paper ballots.

In the last election, I chose to vote by absentee ballot in order to be sure that my vote would count. Then I heard that not all the absentee ballots in San Diego had been counted. I don't know whether that rumor was true, but it would not surprise me if it were.

In my estimation, we need public financing of elections and paper ballots.
Carolyn Myhre

07/30/2007

From: Lansing Sloan
Sent: Monday, July 30, 2007 11:45 AM
To: Voting Systems
Subject: remarks in view of July 2007 top to bottom review report

Hello,

I lack time to read the July 2007 reports of the top to bottom review before the comment deadline of July 30. I have looked at the first few pages of the overview by Matt Bishop and it looks reasonable.

The shortage of time, and the lack of cooperation described in Bishop's report, are somewhat dismaying; and it would have been nice to have been able to pursue the additional leads mentioned. But even with much more time, I doubt that all problems would have been detected. Still, the top to bottom review has to have been valuable. Well done. I expect that similar such reviews will be appropriate and will be conducted in the future.

Given that problems were found with all of the evaluated systems, I have no objection to decertifying all of them.

My main desire is to improve the election system in the long run, and (as I have said previously) I consider it acceptable to take some risks in the 2008 elections if those risks are likely to result in safer future elections.

Best of luck to you in acting upon the results of the review.

-- Lansing Sloan

P.S. I formerly communicated to you using the email address
That address still works, but not for much longer.
I have sent this comment using my current email address

07/30/2007

From: DreamCatcherSS
Sent: Saturday, July 28, 2007 11:40 PM
To: Voting Systems
Subject: Question

Why do you have to put everything in PDF (adobe) format? Everytime I open a PDF I slows my computer considerably then I have to reboot and clean. I it takes more time to put things on the internet in HTML but please, PLEASE make the effort.

Yes I know it's not your fault but you could be more helpful for those of us who can't afford the latest computers with more storage capacity.

Thanks
Chandra

From: Marselle Sloane '
Sent: Monday, July 30, 2007 8:18 AM
To: Voting Systems
Subject: Please do away with the DREs

We really must have ballots we can trust or we'll never again have an election whose results we can trust.

Thank you.

Marselle Sloane

..

"War against a foreign country only happens when the moneyed class think they are going to profit from it." - George Orwell

"Brevity is the soul of lingerie" - D. Parker

From: Robin Steele
Sent: Monday, July 30, 2007 10:20 AM
To: Voting Systems
Subject: Scrap the E-Machines!

Dear Secretary Bowen:

It is far more than apparent that electronic voting machines will be the death of American democracy -- unnecessary, unreliable, untrustworthy, there is absolutely no compelling reason to compromise our most sacred franchise for whatever "modernization" or convenience these wolves-in-sheeps-clothing these things may claim to offer.

Scrap the e-machines!!

Robin Steele

From: Julia Kauffmann
Sent: Monday, July 30, 2007 10:17 AM
To: Voting Systems
Subject: De-certify electronic voting machines

My name is Julia Kauffmann. I have been a resident of California since 1980. I feel we should de-certify all electronic voting machines that have proprietary software and no paper ballot.

Actually, I think we should return to paper ballots only - the low tech solution is the best in this case. Even the optical scan tallies can be manipulated, although at least the optical scanned ballots can be counted if needed.

We should cut our losses and get out - the electronic machines are designed for election rigging.

Julia Kauffmann

From: Doug Lenier
Sent: Monday, July 30, 2007 1:40 PM
To: Voting Systems
Subject: Voting Machines

Privatizing the vote in this country by allowing electronic voting on machines made by private corporations, who hold that the public, due to **their** privacy concerns and patent law, are not allowed to know the source code of the software used, **MUST** be prevented from counting our votes.

The very beating heart of democracy cannot be controlled by for-profit corporations that have a direct stake in the outcome of contests. This was painfully evident in the '04 presidential campaign, when the chairman of Diebold systems vowed publicly to do: "whatever it takes", to bring in the election for Bush and the Republicans. This was a direct affront to the voting rights that we have fought so long and so hard for, and the result bore out the veracity of suspicions by those who would like the vote count in this country to remain above partisan politics.

I am calling upon you, as Secretary of State to remove **all** electronic voting systems in California, with or without paper trails, and return to the types of systems that have served this state for well over 100 years. In my county of Los Angeles, for example, the "Inka-Vote" system with optical scanning equipment used to tabulate results, has worked well for us, and could be reliably used in any precinct in the state for very quick and unassailable tabulations.

Please move post-haste to implement this change and guarantee a future of **public** vote-counting in California, as a workable model for the entire nation.

Respectfully,

Doug Lenier

07/30/2007

From: Gary Mudrick
Sent: Monday, July 30, 2007 1:04 PM
To: Voting Systems
Subject: FRAUD AND COMPUTER VOTING

Please do all you can to save us from false voting machines. Go back to paper pencil voting only, and hand counting. Thanks. gary.

07/30/2007

From: cschaefer7(
Sent: Monday, July 30, 2007 1:08 PM
To: Voting Systems
Subject: Electronic voting systems

Dear Debra Bowen, please continue to fight for the rights of voters by discarding the hackable electronic voting machines and returning to a paper ballot, with a paper trail. We need to believe in the voting system and be assured that there will be one vote counted per qualified voter. Thank you, Craig Schaefer,

AOL now offers free email to everyone. Find out more about what's free from AOL at AOL.com.

From: Salsa4all(
Sent: Monday, July 30, 2007 1:08 PM
To: Voting Systems
Subject: Please DECERTIFY!

Dear Madam Secretary,

I voted for you because of the voting machine issue. It's imperative that you decertify these evil devices, owned and operated by Republicans/neocons, con being the operative word..

We have so few of our Constitutional rights left, and the vote has been rigged at least since the Supremes appointed W in 2000. I fear California will become the next FL or OH.

The flawed argument that we can't use a paper ballot won't fly. It worked before, and works in other countries. One of the major problems (aside from rigging) with electronic votes is that the electronic winner wins, even if later proven to have lost. We can wait a day to actually count votes before announcing the real winner.

Obviously, this may be moot if W declares martial law and decides to be dictator for life. In that case, California must secede from this evil empire. Were I young and healthy and had means, I would hotfoot it to Costa Rica, but it appears I will die here. I'm dying every day of a broken heart over the loss of our Constitution, and hold on only to the hope that my vote will be counted.

I'll do anything you ask to help you overturn this travesty of justice.

Most sincerely,

kathleen wyrill

Get a sneak peek of the all-new AOL.com.

From: Martin Morrow
Sent: Monday, July 30, 2007 1:13 PM
To: Voting Systems
Subject: crooked machines

Whatever it takes, please decertify these crooked machines
M. L. Morrow

07/30/2007

From: Karena & Michael
Sent: Monday, July 30, 2007 9:00 AM
To: Voting Systems
Subject: Voting machines review

Dear Secretary of State Bowen,

I am a California voter born and raised and I vote consistantly. **I am sending you my opinion that we scrap the electronic voting systems forever.** I have so little faith in these machines that I now vote by absentee ballot, votes which I can only hope are not tallied, then entered into the same questionable voting machines! While I am amazed by the technical advances of some very helpful computerized equipment, these voting machines will never be secure as long as people design them and elections are so heated. Politicians are just people and in every group of people there have always been some honest ones and dishonest ones. Elections can mean more to some people as to sway them towards dishonesty and unfortunately, unscrupulous downright corruption. I have hopefully made myself quite clear in my disapproval in the continued use of these machines in any Californian and US election...I repeat, **SCRAP THEM ALL!!!**

Thank you for the research which has been done and I look forward to the reults of the public hearing. I have bookmarked your web page. Signed, Karena Vance, Santa Cruz, California

07/30/2007

From: Tarta Smitheman
Sent: Monday, July 30, 2007 9:14 AM
To: Voting Systems
Subject: Paper trail, please!

Please, PLEASE return all of California to paper ballots. And let the voting machines be owned and operated by the State! Thank you for your investigation. And I fervently hope that you opt for an unbiased, hacker-free method by which to hold future elections, even if that method is slower and less high-tech.

The Federal Election Commission wants to use privately owned, electronic machines. That are owned by two companies, that are run by two brothers, who are both involved with Republican campaigns; This is hardly an exercise of democracy. Please don't take pointers from the Feds.

Sincerely,
Tarta Smitheman

Don't get caught with egg on your face. [Play Chicktionary!](#)

From: Lori Mason
Sent: Monday, July 30, 2007 9:06 AM
To: Voting Systems
Subject: hackable voting machines

Dear Sec. of State Bowen:

The right to vote is the cornerstone of a democracy. Without the assurance of the integrity of the counting of our votes, the act of voting becomes a pointless sham. Therefore, to ensure that every vote is counted, we must get rid of electronic, computerized voting machines in California. A University of California Berkeley study, as reported in the San Diego Union-Tribune on Friday, 7/27/07 (front page), found the machines are easily hackable, even by meddlers with low computer skills. If Canada can do it, why can't we? -- Completely PAPER balloting and hand counting, or at least thoroughly reliable, verifiable OCRs (optical character readers) with complete paper trail. PLEASE!

Nothing is of more importance to the rescue of democracy in California and our country. This change MUST happen BEFORE the election in 2008.

Thank you,

Lori Mason

Head Handmaid

StrictlyHandmade.com

From: Debbie Fritsch
Sent: Monday, July 30, 2007 9:14 AM
To: Voting Systems
Subject: Please decertify electronic machines!

Dear Ms. Bowen:

I voted for you in large part so that you could restore integrity to the voting process in California. Hopefully the rest of the country will follow, because my vote doesn't count unless every vote is counted accurately. Please decertify the electronic voting machines so that democracy has a fighting chance in the US-this is truly a desperate situation.

San Diego somehow ended up with a discredited former Ohio election official and a Diebold saleswoman running our elections. These people pose a sufficient challenge to accurate vote counting without easily hackable machines.

DEMOCRACY DEPENDS ON YOU - PLEASE DECERTIFY THE ELECTRONIC VOTING MACHINES IN CALIFORNIA!

Thank you.

Deborah K Fritsch

07/30/2007

From: adele cabot
Sent: Monday, July 30, 2007 9:22 AM
To: Voting Systems
Subject: No voting machines

Dir Sir,

In light of the news that hackers broke into voting machines, won't you please go to paper ballots. Voting is the sacred right of Americans and we need to know, especially now, that every vote counts and is being counting as it was cast. Please protect our precious freedoms and find the voting machine that is not hackable and is recountable.

thank you
Adele Cabot

PC Magazine's 2007 editors' choice for best web mail—award-winning Windows Live Hotmail. [Check it out!](#)

07/30/2007

From: Warner, Cathleen (ABA)
Sent: Monday, July 30, 2007 9:42 AM
To: Voting Systems
Subject: Diebold machines

Dear Deborah Bowen,

I am complete against these easily hackable voting machines being used in any election in California. As a voter in San Diego County where these machines are used (and as a poll worker in the last election in charge of these machines) I urge you to de-certify them for the integrity of all elections in the state of California.

Thank you,

Cathy Warner
Loan Officer Assistant

"Please be aware that e-mail is NOT a secured communication vehicle, and that others may in certain circumstances be able to view its contents. As a result, while we are happy to provide this information by e-mail, we do NOT conduct actual business transactions by e-mail. Please contact the sender directly if you have any concerns about this message. All loans subject to credit approval and property appraisal. Equal Housing Lender.

This communication is a confidential and proprietary business communication. It is intended solely for the use of the designated recipient(s). If this communication is received in error, please contact the sender and delete this communication."

***The following annotations have been made

Please be aware that e-mail is NOT a secured communication vehicle, and that others may in certain circumstances be able to view its contents. As a result, while we are happy to provide this information by e-mail, we do NOT conduct actual business transactions by e-mail. Please contact the sender directly if you have any concerns about this message. All loans subject to credit approval and property appraisal. Equal Housing Lender. This communication is a confidential and proprietary business communication. It is intended solely for the use of the designated recipient(s). If this communication is received in error, please contact the sender and delete this communication.

From: Andrew Pavelchek
Sent: Monday, July 30, 2007 9:44 AM
To: Voting Systems
Subject: Electronic voting machines are counterproductive in a democracy.

Dear Madame Secretary,

Let me first preface my comments with some of my background. I have worked as a hardware designer and as a computer programmer for most of my career and now manage development teams. I have worked on the development of secure and classified military systems and commercial telecommunication systems. I wouldn't consider myself an expert in any one of these fields but have a broad breadth of experience at a reasonably deep level. Also, as a long time voter, I remember longing for electronic machines so that I wouldn't have to vote with the apprehension of spoiling a ballot and having to either forsake a vote or start over. At one time I considered voting machines a panacea. But I was relatively inexperienced and politically naive. I have come to the conclusion that hand marked physical ballots are the only way to protect the voting process and consequently keep the voters faith in democracy. Paper ballots are the only current solution that fits the bill. I was recently convinced that even a paper trail equipped voting machine is not adequately secure against fraud.

Fair, honest elections require constant vigilance and your office is tasked with that. Please immediately halt the use of any voting machines that lack a paper audit trail and move to return to paper ballots at the earliest feasible date.

A. Pav.

From: Lokensgard, David
Sent: Monday, July 30, 2007 10:01 AM
To: Voting Systems
Subject: Direct Recording Electronic Voting - Against

I want to add myself to the large number of people who object to non-verifiable DRE voting systems. As a voter, I have zero faith that my vote can be correctly cast and counted and, equally importantly, re-counted when the situation calls for a recount if these systems are used. A "paper trail" or audit trail is not enough protection, since these things are not ballots nor recorded votes subject to recount.

What we voters want is a physical ballot that we mark to correspond with our intended vote, is subject to physical scrutiny, and cannot be changed by electronic means. If we have that, we have a hope of preserving the integrity of this fundamental democratic right. Without that, there is no way of ensuring that electronic manipulation cannot occur.

David Lokensgard

From: sempreciao
Sent: Monday, July 30, 2007 1:50 PM
To: Voting Systems
Subject: Voting Machines

Dear Secretary of State,

I would like to strongly urge you to take a stand in support of HONEST VOTING RESULTS for California. Don't acquiesce to the voting machine manufacturers' pressures to certify machines that could be tampered with. Let's go back to paper balloting if that is necessary...for any upcoming elections and all elections in the future....anything is better than fraudulent results.

This is one of the most basic and important issues in order for us to preserve what little is left of our democratic Republic. Your campaigned on this big time.....**I voted for you because of this important issue** and worked for your campaign and urged everyone I knew to vote for you.....DON'T LET US DOWN.

Sincerely,
JoAnn Hastings

AOL now offers free email to everyone. Find out more about what's free from AOL at **AOL.com**.

From: Patricia Wrangell
Sent: Monday, July 30, 2007 4:41 PM
To: Voting Systems
Subject: Scrapping current electronic voting systems in California

I am a voter in Riverside County (Sequoia II electronic voting system). Not ggod enough. You have my vote for scrapping it.

Patricia D. Wrangell,

Take the Internet to Go: Yahoo!Go puts the Internet in your pocket: mail, news, photos & more.

From: annz
Sent: Monday, July 30, 2007 4:09 PM
To: Voting Systems
Subject: AlterNet: In Violation of Federal Law, Ohio's 2004 Presidential Election Records Are Destroyed or Missing

This story has been forwarded to you from
<http://www.alternet.org> by annz@nethere.com

Debra Bowen,
This is why the media and the public must be allowed to observe the vote count of hand counted paper ballots. The Registrar and their staff need to be watched also.
Ann Zegler,

In Violation of Federal Law, Ohio's 2004 Presidential Election Records Are Destroyed or Missing
<http://www.alternet.org/story/58328>

In 56 of Ohio's 88 counties, ballots and election records from 2004 have been "accidentally" destroyed, despite a federal order to preserve them -- it was crucial evidence which would have revealed whether the election was stolen.

From: Gloed98
Sent: Monday, July 30, 2007 4:05 PM
To: Voting Systems
Subject: voting:paper trail

Our most precious right in our democracy is the act of voting. In recent years this has been turned into a cheating, unacceptable situation. It is imperative that we have a paper trail, when we vote. We cannot accept any other system.

Get a sneak peek of the all-new AOL.com.

From: Lou Newell
Sent: Monday, July 30, 2007 5:43 PM
To: Voting Systems
Subject: Top Down review

As I watched the proceedings on TV today, it occurred to me that the major efforts have been related to physical security and hacking. While these are real concerns, it seem to me that the real problem is verifying that the machines are properly programed. In the case of punch card or optical scan systems, the programing (and the machine) can be tested by the use of a "test deck" and comparing the results with the expected result. Multiple passes would convince the most skeptical observer. The same method will not work with direct entry machines as there is no way to insure that the person entering the data does it the same way each time especially on a complicated ballot.

Lou Newell

From: DJ Leif
Sent: Monday, July 30, 2007 3:39 PM
To: Voting Systems
Subject: Voting machines need better oversight

I am glad to hear that you are looking into our voting machine systems. I am appalled that this is still an unresolved problem...and a grave problem it is.

The success of democracy is dependent on the wisdom of citizens being transmitted through the vote. The desire to vote is based on the knowledge that our vote makes a difference. If the issue of vote security is not completely and unequivocally addressed, even the suspect of voting impropriety can seriously jeopardize our fragile democracy.

Based on what we already know, votes that turn out to be statistically extremely close, as with our past two elections, are highly improbable. How can we vote for change, if our votes cannot be verified?

Please address this problem, and broadcast it so as to get national attention.

This is the single most important reform we need to make in this country.

Thanks,

Leif

From: Rebecca WWWW
Sent: Monday, July 30, 2007 3:23 PM
To: Voting Systems
Subject: voting systems

How can we ever trust voting machines if there is no paper trail to back up the so-called results?

Ready for the edge of your seat? [Check out tonight's top picks](#) on Yahoo! TV.

July 28, 2007

The Honorable Secretary of State Debra Bowen
1500 11th Street
Sacramento, CA 95814

Re: Top to bottom review of voting systems

Dear Honorable Secretary,

Thank you on behalf the people of the State of California for your work on ensuring the security and validity of the election process in California. Your top to bottom evaluation of electronic voting systems is an important step in the re-democratization of the electoral system in California and, indeed, the nation. The example you have set will, hopefully, inspire other Secretaries of State to follow suit to examine the voting machines in such a way as to rebuild the public trust we need restored to the electoral system.

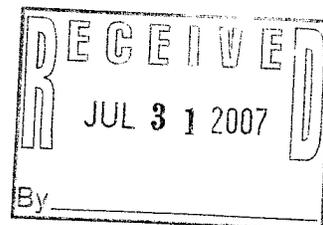
Your critics have much to hide as they may have financial interest in the adoption of these devices but you have stood up to them. Thank you.

In one last thought, I ask you to consider the official adoption of the requirement of all State election machinery to use open source software. As you already know, open source software does not compromise the data (votes) in the machinery; it allows an open, democratized review of the logic used to count the votes. Please help educate the electorate of this important step.

Respectfully yours,



Jay L. Cobb



27 July 2007

Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, CA 95814

Dear Ms. Bowen,

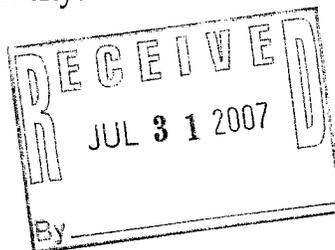
I am one of your many admirers, and I was a bit angered by Stephen Weir, the registrar of voters of Contra Costa County, in his response to your insistence on a paper trail. Mr. Weir also has a history of suppressing votes. I witnessed this myself in the October 2006 election and wrote to Michelle Gabriel about it at that time.

One important way to win an election is to discourage your opponents from voting. I believe there were strong examples of this in West Contra Costa Country in 2007.

In Richmond and El Cerrito polling places were changed in such a way that less people voted. In the heavily Democratic cities of Richmond and El Cerrito voters were sent to new polling locations.

In one case the polling place was set in the heart of what is known as The Iron Triangle. This is where many of the murders occur in Richmond, and voters were frankly afraid of going there. In many, many cases voters did not know how to reach the polling place and had to be given directions over the telephone. There was no public transportation linking voters to the Triangle Community Center. The distance to the Triangle Community Center was too far for most of people to walk. The Community Center can be reached only from the south, and it requires crossing under railroad tracks and in many cases going miles and miles. Voters who did not drive and could not afford taxis were effectively prevented from voting. A very few were contacted by the Democratic Party and offered rides, but they were very few. This same story occurred in another Richmond precinct where people from Hilltop were sent across the railroad tracks through relatively isolated areas to another crime-ridden section of the city, Parchester Village.

In yet another Richmond district voters received postcards from the County telling them to vote in Pleasant Hill, a city miles away from Richmond. When contacted about this error, Contra Costa County election officials promised to correct the error by sending new notification that would tell the voters they could vote in their own city of Richmond. Not all voters received these notifications and were surprised to learn on election night that they really could vote in their own city.



In a fourth precinct voters were told to vote in one place, but the county initially told the local Democratic organization that the polling place was elsewhere. By the time the local Democrats learned of the error hundreds of useless and incorrect doorhangers had been printed!

El Cerrito has no infamous crime district, but telling the voters to go to a school miles away, an unknown school that has no easy public transportation also prevented many people from voting. Madera School is on Madera Court. Now where is Madera Court or Street or Circle or school? Most people do not know its location! Even with a map it is difficult to locate. For people in Precinct 6 it is a trek up a long steep hill from San Pablo Avenue to Arlington Boulevard. It is a long distance away from their home--at least a forty minute walk for some. There are no buses linking them to the school. Many people in the precinct live in retirement homes and could not be expected to drive, much less walk, to the school. Nor could these retired pensioners afford taxis. This school is also at a long distance away from BART riders who could not easily access it either before going to work nor after a day of hard work. No rides were offered by the local Democratic club as the problem had not occurred previously.

I believe it would be worthwhile to check for other cases of voter suppression in Contra Costa County lest this reoccur and we lose future elections. In statewide elections every vote counts, and many people were effectively disenfranchised by the Contra Costa County Registrar of Voters.

Yours truly,


Yvonne M. Steffen

From: Sheila Parks
Sent: Saturday, July 28, 2007 7:38 PM
To: Voting Systems
Subject: ON-SITE OBSERVATIONS OF THE HAND-COUNTING OF PAPER BALLOTS AND RECOMMENDATIONS FOR THE GENERAL ELECTION OF 2008, published on opednews.com and elsewhere
Importance: High

Dear Secretary of State Bowen and Lowell Finley:

I hope you will read this paper I just wrote and had published on opednews.com (and several other places then picked it up) about hand-counting of paper ballots and do the same in CA as they do in Acton, ME, as described in this paper.

http://www.opednews.com/articles/opedne_sheila_p_070718_on_site_observations.htm

It would be very doable.

See also, my article, *Hand-Counted Paper Ballots Now*. A version of this article first appeared in the April 2006 issue of *Tikkun*, <http://www.tikkun.org/magazine/specials/article.2006-04-10.1693298872> . An updated version can be found at <http://electionfraudnews.com/News/HCPBNow.htm>.

Please, contact me if you feel I could be of any service to you in this wonderful work you are doing in CA.

I am also attaching a word doc copy of the ON-SITE OBSERVATIONS paper, for your convenience.

Thanks.

Sheila Parks, Ed.D.

From: Sybertel
Sent: Sunday, July 29, 2007 1:38 PM
To: Voting Systems
Subject: No DRE

Dear Secretary of State, Debra Bowen:

Please decertify all electronic and touch screen voting machines in California. These machines can never provide an accurate verifiable audit trail for any vote recount. As such the integrity of our vote will be seriously compromised as it is humanly impossible for average citizens to verify any electronic election results. Devoid of election credibility, those who would vote are much less likely to vote as they have even less confidence that their vote will make a difference.

Election integrity is the essential hallmark of a democracy and protection of voting is the road upon which it travels. Without election integrity results can and will be subject to manipulation by the unscrupulous acolytes who are more faithful to party agenda than to our constitution. We have seen ample evidence of their election frauds and know that these scoundrels will not be deterred by exposure or prosecutions.

Even in San Diego County, the Board of Supervisors has ignored public protestations and hired the most controversial and suspect individuals that it can find to control our elections. They have employ highly partisan David Haas from Cuyahoga County, Ohio, and Deborah Seiler who has strong ties to Deibold Corp. as Registrar of Voters. These placements have gone forward despite citizen complaints and given their dubious histories one must wonder if "the fix is in".

Our democracy will be imperiled by electronic voting as no one can count electrons. And the early news predictions of "winners" via DRE or Touch Screen machines can be readily manipulated to install unearned claims of election to an elected office. **Thus Californians need to cast their votes on Paper Ballots, not on DRE machines or Touch Screen voting machines! We need verifiable, re-countable, and observable paper ballots which yield hard copy voting records that any citizen can readily examine!!**

Thank you for all your hard work to protect our democracy;

Deborah Mecum

Get a sneak peek of the all-new AOL.com.

07/30/2007

From: Jack McCurdy
Sent: Sunday, July 29, 2007 12:38 PM
To: Voting Systems
Subject: Need response

The following is from an article on July 28, 2007, in the Eureka Times-Standard. Please provide a response to the insinuation that the study may not have taken into account any security measures instituted by McPerson. In any event, be prepared for this kind of defense against the findings of your study.

Jack McCurdy

Humboldt County Registrar of Voters Carolyn Crnich said it's unclear under what conditions the tests were prepared.

"It's my understanding that the red team attacks that were made during the top-to-bottom review did not take into consideration the security efforts or guidelines that had been added by former Secretary of State Bruce McPherson -- so whether or not the systems could be penetrated with those other security guidelines in place, I don't know," Crnich said.

Entire article:

Local election systems may be vulnerable to hackers

James Faulk/The Times-Standard

Article Launched: 07/28/2007 04:21:31 AM PDT

EUREKA -- A team of University of California computer scientists were able to hack into several voting systems used by California counties, including the two systems currently used in Humboldt County, the secretary of state announced Friday.

Matthew Bishop and David Wagner, computer science and cryptography experts, were able to hack into both the Diebold Accuvote system, and the Hart InterCivic system. The main vote counting system in Humboldt County is the Diebold

07/30/2007

Accuvote machine, and the Hart device is used to improve accessibility for people with disabilities.

The hacking test was done as part of a top-to-bottom review conducted by Secretary of State Debra Bowen.

"The top-to-bottom review is designed to look at the security, accuracy, reliability and accessibility of the voting systems certified for use in California in a way that's never been done before on a state or national level," said Bowen, the state's chief elections officer.

"Every voter has the right to have his or her vote counted as it was cast, and voters want to know if the very tools of our democracy are secure, accurate, reliable and accessible," she said.

The independent UC reports are available on the secretary of state's Web site at http://www.sos.ca.gov/elections/elections_vs.htm/.

In addition to the hack tests, the secretary of state will also be holding a public meeting

Advertisement

on Monday and possibly Tuesday to get public input on the situation. A final decision on what this means -- and whether it could lead to a decertification of Humboldt County's voting systems shortly before a string of four closely packed elections -- will likely be announced Friday.

"The UC teams went through a thoughtful, methodical, analytical process in conducting their examinations of these systems," Bowen said. "It is my intent to go through a similarly thoughtful, methodical and analytical process in determining what we do next."

Humboldt County Registrar of Voters Carolyn Crnich said it's unclear under what conditions the tests were prepared.

"It's my understanding that the red team attacks that were made during the top-to-bottom review did not take into consideration the security efforts or guidelines that had been added by former Secretary of State Bruce McPherson -- so whether

or not the systems could be penetrated with those other security guidelines in place, I don't know," Crnich said.

On the Web: The independent UC reports are available at http://www.sos.ca.gov/elections/elections_vs.htm/.

James Faulk

From: Ann
Sent: Monday, July 30, 2007 12:48 PM
To: Voting Systems
Subject: My right as a U.S. citizen to a fair and honest election in 2008

To: California Secretary of State Debra Bowen
From: Ann Zegler, California resident and voter who has no faith in any election conducted by private corporations using secret electronic vote counting machines.

Hand Counted Paper ballots are cheaper and allow us (the public) to conduct our own elections with transparency and public confidence. Since we supposedly have a government of WE THE PEOPLE, it would logically follow that WE THE PEOPLE fully participate in all areas of governing, including elections and vote counting, and participating in the reporting of election results. When our elections are run by Diebold and other private voting machine corporations, WE THE PEOPLE are excluded from our own elections and democracy is silenced and destroyed. Since the passage of HAVA in 2002, with the introduction of electronic voting supposedly for the benefit of the disabled community, fair elections have been stolen from the American public under a false premise. As a disabled person myself, I feel the stated goals of HAVA were false claims, and that the intent all along was primarily to legitimize electronic voting in the eyes of the public. A concise summary of the facts behind my distrust of HAVA and electronic voting in general are at www.bradblog.com/?p=2262.

I'm forwarding some recent thoughts of Paul Lehto, California attorney and voting rights activist. I share these thoughts because they are of tremendous concern to many of us in San Diego. Our new San Diego Registrar of Voters, Deborah Seiler, comes to us having been a sales rep for Diebold from 1999-2004 and before that, a sales rep for Sequoia. Seiler is known as one of the best PR people or apologists for secret vote counting that exists in the nation, Paul Lehto tells us.
www.signonsandiego.com/news/metro/20070512-9999-7m12seiler.html

We also have a new San Diego Assistant Registrar, Michael Vu, who was the director of elections in Cuyahoga County, Ohio during the 2004 and 2006 elections. His handling of problems with Diebold and vote counting in the 2004 presidential election were controversial. In a 2006 election audit, more than 1 in 4 Diebold systems were found to have recorded votes INCORRECTLY in Cuyahoga County under the supervision of Michael Vu. He found nothing wrong with that election, and that is of great concern to many of us in San Diego. For details, see "THE VIEW ON VU" at www.secureelections.org, a local voting rights organization.

We have all learned to follow the money to fine tune the picture, no matter what program we are watching. I'm not implying that any particular person, local Registrar or otherwise, is corrupt but I am concerned that the profit in electronic voting is huge and therefore the chance of fraud increases with the rise in profit at stake. I know that the Electronic voting machine companies involved in California elections will spend large amounts of money and employ many lobbyists to convince you this week to let them continue running our elections in California. I am just a retired California public school teacher with very little money and no lobbyist. I have nothing to bargain or promise you, other than my hope that you can make a bold decision in favor of WE THE PEOPLE and my gratitude for all you have done so far to restore my hope for a better future for democracy.

With the growing number of deaths, both American and Iraqi, sacrificed to bring freedom and democracy to Iraq, I would hope we could restore the very thing our soldiers are giving their lives for, representative democracy, to our own country, and this week, to California.

I look forward to your decision on electronic voting for California. I know the rest of the nation is

watching with me. Below are some thoughts from Paul Lehto, attorney and voting rights proponent, that I would like to pass on to you. He is one of the founders of PSEPHOS. www.psephos-us.org He expresses so well what I have been thinking for some time now.

Thank you again for your willingness to stand up for WE THE PEOPLE in California. I look forward to your decision on Friday, when I will know if my voice has been handed over to Diebold, or if it will be allowed to be heard once again at the ballot box.

From: ca50-bounces@... **In Behalf Of** Paul Lehto
Sent: Sunday, July 29, 2007 11:57 PM
To: annz@nethere.com
Cc: CEPN
Subject: [CA50] Re: [CalifElectionProtection] link to online stopwatch to time your testimony

Key point for testimony (IMHO)

A lot of talk, red team reports included, misleadingly focuses on OUTSIDER attacks. However, there's no serious computer scientist that's honest that won't admit that all bets are off if there is a criminal insider. And there's every reason to believe there will be one because a successful hacker or rigger gets to be the election official or at least to influence election "security" policy for the next election. This means that if you are looking for an election criminal, or the good friend of one, LOOK IN OFFICE.

But even Bowen's red team folks wants to ignore the insider threat in terms of its true level of seriousness.

Instead, the protocols and procedures of local election servants are supposed to "mitigate" or save us to a little extent or to a great extent. We're supposed to now debate just how much said procedures will save our butts from Sequoia, Diebold and company, based on how the reports are structured, this is naturally the kind of debate it leads to....

The fact is, it's not a question of whether local officials mitigate the risk by 10% or by 90% through their vaunted (BS) procedures. The election officials ARE THE CORE PROBLEM. The computers can not possibly be made secure, as against these insiders.

So that means we don't have the power as voters to kick out criminal politicians and criminal election officials. That's totally unacceptable. That's when we need our votes and our power the very most.

Heck, if there were a way to ensure that somebody truly was a saint and worked with all saints, we could use the honor system or something. But the true test of an election system is how it performs when in control of, or penetrated by, people that want to cheat.

Computers in possession of those who want to cheat = hopeless battle. Unacceptable risk, totally unacceptable. And that's the fair test of a system, because as i said if saints are in charge, we don't need security. We need the system to stand up when it is pressured the most

I will not be in Sacramento.

 Paul R Lehto, Juris Doctor

07/30/2007

From: Brad Friedman
Sent: Sunday, July 29, 2007 11:01 AM
To: Voting Systems
Subject: My Only Comment on T2B Review

Thank you all for this landmark analysis.

I suspect you know what I think, so I'll not bother to give details, other than this:

Transparency, transparency, transparency. That's the only thing that allows a *chance* of security and restoring confidence in elections.

DREs need to go. Period. A paper trail does nothing. Even with an audit (as shown by Brennan Center. Call me if you're unfamiliar with their hack that would NOT BE FOUND IN AN AUDIT

So, my MINIMUM recommendation (if you should still allow use of DREs for some reason):

- 1) **Every voter must be asked** whether they prefer to vote on paper or plastic before they are given a ballot.
- 2) Every paper ballot must be **COUNTED BEFORE** any unofficial tabulation results are released to media.
- 3) **Public hand-audits** must be made on the mathematical basis of assuring **99% Scientific certainty that the originally reported results are accurate.** (And proper protocols, remedies must be in place to determine what to do when counts don't match. Not left up to the auditors as in Holt's bill!)

Thank you all, again.

Brad

Brad Friedman
Publisher/Editor, The BRAD BLOG
<http://www.BradBlog.com>

07/30/2007

From: YerEditors
Sent: Sunday, July 29, 2007 11:28 PM
To: Voting Systems
Cc: Elections - El Dorado County
Subject: Message for Secretary Bowen

My Dear Secretary Bowen -

I am so pleased to be able to contact you again, and cheer you on again - I just read that you will be deciding by this Friday how you will decide to proceed on certifying California's electronic voting systems for the 2008 cycle. Victory may come in small, yet crucial spurts these days ... But your courage in the face of daunting odds and a deaf press will never be forgotten by those of us who were so glad to find out about you - no one knows that more than the citizens, both in California and from all over the country, who followed and contributed (as I so proudly did) to your campaign. Imagine a public official willing to stand up and scrap not just for a nomination, but for the citizens' right to vote. How refreshing !

Now, as you press on to take up the mantle you were given, congratulations!!! May I now offer my opinion on the most honest, legal, and cheapest way to make sure that the vote in California will be valid: paper ballots at the precinct level, tallied at the precinct level, and then handed up to the county AND state level simultaneously. The only way for citizens to trust that their votes count again is for that tally to be certified at the precinct level by the judges on site - I know, I worked the polls as a volunteer in 2004. I don't see why ANY poll volunteer would mind counting the ballots by hand (even pairing up "opposing" party member judges to count each ballot cast) - certifying, along with their fellow poll workers, what the tallies are on the spot, then handing up the results. All precinct results would be published the next day on the Internet and in the newspapers, leaving no chance for contradiction. The only thing "wrong" with this approach is that it works - it always has.

I can think of no legitimate argument for computer involvement at this time on the part of any legitimately concerned citizens, just those with vested interests in continued uncertainty, and worse, voting fraud. California now, thanks to your leadership and stewardship, has the chance to lead the nation out of this deliberate morass. You were a lonely voice at a very critical time, but we heard you.

Optical character readers would be fine for a backup JPEG-type file, but I would NOT trust any sort of computerized system, which necessarily would include OCRs, to play any part in tallying any totals - as you know, it is too easy for those totals to change. That's why the chain of evidence needs to be so clear from the ground up, without the daisy-chained machines that somehow need to be networked together.

Secretary Bowen, PLEASE lead the nation in showing how your state can so easily ensure that every vote counts on the crucial day. Of course, making sure voter names aren't erroneously purged is a separate part of the problem ...

Thank you for everything you're doing - keep up the good fight!!!

Sincerely,

Catherine McDermott

Get a sneak peek of the all-new AOL at <http://discover.aol.com/memed/aolcom30tour>

07/30/2007

From: Brina-Rae Schuchman
Sent: Monday, July 30, 2007 1:47 AM
To: Voting Systems; Goldberg, Evan
Subject: GIVE US GOOD VOTING SYSTEMS ONLY please

Dear Secretary of State Bowen,

We know that you are under heavy pressure from greedy election computer vendors and misguided election officials to keep the phony computer election machines.

All we ask is that you think of all the OTHER CITIZENS who are at work or school and not at the Hearing, who want to be able to vote and have their votes accurately counted. That is the earmark of citizenship.

PLEASE--- Retain Democracy in the nation. It is almost all gone.

The VOTE is the VOICE of the People. With phony computer machines it is almost silenced.

Sincerely,

Brina-Rae Schuchman
Chair, TrueVoteSanDiego

From: David Griscom
Sent: Monday, July 30, 2007 8:14 AM
To: Voting Systems
Subject: Fwd: [peoplecount] Here is the Email Address to Send Comments and Suggestions to CA



[peoplecount] Here 330446114-Election
is the Email... Wars in Pim...

FYI I'm attaching a personal account of election theft in Tucson, AZ, in 2004 buttressed by my own original research. This essay is slated to be a chapter in a new book edited by Mark Crispin Miller entitled "How to Steal an Election: The Bush Regime's Subversion of Democracy, 2002-2008," coming out in January.

In short, this fraud required, in addition to hackable voting machines, many insiders to accomplish. So beware of election officials bearing the soothing message that the election server is isolated in a sealed room. The crooked election officials make sure the Trojan horses are in there with them (or pre-planted in the memory cards of the voting machines).

Dave

Note: forwarded message attached.

David L. Griscom

Election Wars in Pima County, Arizona: A Microcosm of Nationwide Election Theft?

David L. Griscom Ph.D.

<http://www.impactglassresearchinternational.com/>

26 July 2007

I. John Brakey, Master Sleuth of Election Fraud

On 2 November 2004, John R. Brakey was Democratic Cluster Captain for four precincts in Arizona Legislative District (LD) 27, a part of the predominately-Hispanic, 80% non-Republican Congressional District (CD) 7. LD 27 encompasses a part of Pima Country including the southwest corner of the city of Tucson. John was new to the job, but he knew that part of his duties – and prerogative – was to pick up “tear sheets,” which are carbon copies of the list of voters who had already cast their ballots hand-printed by the poll workers on a form called the Consecutive Number Register (CNR). Poll workers in three of these precincts greeted him with hostility, and in one case they attempted to conceal the existence of several completed CNR pages for which he was requesting copies.

As Election Day wore on, John became increasingly suspicious that the poll workers in those three precincts were up to something. So, over an hour after the polls had closed, he returned to his home polling place, a school located in Precinct 324, to see what evidence he might pick out of the trash. To the mutual shock of everyone present, he walked in on the poll workers apparently in the act of altering the CNR (which should have been completed at the time of the arrival of the last voter). He also observed the vault of the Diebold optical-scan voting machine to be wide open, instead of being locked shut as it should always be. The poll workers rose to their feet in unison, cursing Brakey and telling him to get back out of the room; (see p. 132 of Mark Crispin Miller’s book “Fooled Again”). He did so quickly after a woman poll worker began to circle behind him brandishing a club-like cane as though a weapon.

From that moment on, getting to the bottom of what was going on became John’s all-consuming passion. He abandoned his bread-winning job and began working unpaid 18-hour days gathering and entering on Excel spreadsheets all available records bearing on the voting at Tucson Precinct 324 on Election Day 2004. I was privileged to be able to aid John in the forensic analysis of these records, the results of which I ended up presenting as PowerPoint lectures at the National Election Reform Conference in Nashville, TN, April 9, 2005, the Election Assessment Hearing in Houston, TX, June 29, 2005, the Election Integrity Workshop held at the quarterly meeting of the Arizona Democratic Committee, Flagstaff, AZ, August 20, 2005, and a session entitled “Are We a Democracy? Vote Counting in the United States” at the 2007 Annual Meeting of the American Association for the Advancement of Science (AAAS), in San Francisco, February 16, 2007.

II. Evidence for Poll-Worker Fraud in Tucson Presented at a National Meeting of the Premier Science Organization in the United States

The following is slightly modified version of my abstract for the 2007 AAAS meeting:

As Cluster Captain on 2 November 2004, John Brakey returned to one of his assigned Tucson polling stations an hour after the polls had closed, surprising poll workers apparently altering the poll books. Brakey began an audit of this precinct (#324) based on copies of all public records: (1) a list of all voters registered in precinct, (2) all Signature Rosters (SRs), (3) the Consecutive Number Register (CNR) with 884 poll-worker-printed voter names, (4) the Official Ballot Report and Certificate of Performance signed by all 7 poll workers, and (5) a list voters who signed affidavits on the envelopes conveying Provisional Ballots (PBs) to the county Recorder. Brakey recovered from the morning-after trash (6) the poll-worker-annotated "Advice to Voter" slips. Records (2) and (6) indicated which voters were required to vote on PBs (which are only accepted by the Recorder if she ascertains that the voter is registered and had not mailed in an Early Ballot). Record (4) could not be reproduced by from the public data without assuming 39 PBs were illegally fed into the optical-scan ballot box on Election Day. The CNR contained 11 fewer unique names than the number of ballots in the ballot box according to (4), implying 11 felony double votes. The poll workers issued 11 extra ballots as alleged spoil replacements, possibly to cover up (but failing to disprove) these double votes. There were also exactly 11 voters who signed a "regular" SR but whose names are not listed on the CNR, 11 voters who signed the PB SR but are not on the CNR, 11 voters who signed both the "regular" and PB SRs, 11 registered voters listed on CNR who failed to sign any roster at all, and 11 phantom voter names appearing on 11 of the signed envelopes of PBs received by the Recorder that do not match any signature on any SR - nor any entry on the CNR! The probability of any one of these irregularities occurring 11 times is much less than 1/11. The odds of all 7 occurring exactly 11 times as independent random accidents (e.g., due to incompetence) are much, much less than one chance in 11 raised to the 7th power = 19.5 million. Three voters had their names inscribed a second time on the CNR exactly 100 places after the first, with one-chance-in-131-million probability. Despite their complete control of the CNR, the poll workers wouldn't have been able to contrive such statistical rarities without a "system." Indeed, (6) revealed a non-standard hand-numbering scheme which would have fit the purpose. We conclude that 22 valid Kerry votes could have been discarded (as 11 allegedly spoiled ballots and the 11 PBs rejected by the Recorder, likely because of 11 forged signatures) and 61 Bush votes could have been forged (as 39 PBs illegally fed into the ballot box on Election Day, 11 double votes, and 11 alleged spoil replacements) – a shift of 9.4%. Still, the inferred "system" would have deposited paper ballots in the ballot box exactly matching the number claimed in (4), and voter choices on these ballots would match the official tally, thus appearing honest in the event of a hand recount – and thereby covering up demonstrably possible hacking the 1.94w memory cards in optical-scanner precincts where the poll workers were honest.

My actual AAAS PowerPoint is available for downloading [1].

I should mention that the estimated vote shift given above (9.4%) differs from that which I erroneously stated in the original abstract as 8% and is based on the assumption that the poll workers had no more blank ballots than the 926 officially issued to them. In fact, extra ballots would have been easy enough to obtain, since in Pima County anyone can request up to two replacement mail-in ballots before the Election *without returning a spoiled one*; (John Brakey's wife actually spoiled hers and was sent another, no questions asked). In my PowerPoint I infer a possible 12.8% shift, which if correct would require the poll workers to have handed out 30 additional ballots and subsequently physically destroyed 30 ballots after voters had marked them.

All AAAS abstracts are forbidden to exceed 500 words, and even by adding 50 more in the above version, much important background is obscured. So let me use a few more words below to fill in some of this background.

As far as I know, John Brakey was the first to discover (by surfing the internet) that the 1.94w memory card used on the Diebold optical-scanners contains "interpreted code" and is thus capable of running programs that could in principle be used to alter the vote totals. This principle was ultimately confirmed in practice by Finnish computer expert Harri Hursti [2,3].

So John had demonstrated poll-worker fraud in Pima County, and had *also* realized that elections could be stolen by hacking of the memory cards. He called the combination of these two attack vectors the "Hack and Stack" [4] (with "Stacking" having the same meaning as ballot-box "stuffing").

III. Evidence for Nationwide Election Fraud

Thanks to Harri Hursti and others, we now know for a fact that elections *can* be electronically stolen by hacking (e.g., by inserting vote-flipping programs the 1.94w memory cards) and John Brakey and I have shown that some poll workers may actually be stuffing ballot boxes.

So the remaining question is: Are entire elections actually *being* stolen by these (and likely other) methods? Based on the national exit poll statistics, the answer is a resounding, *yes*: This was done nationwide in both 2004 and 2006. For anyone in doubt, I list below some reading assignments.

Election 2004:

- (1) "Was the 2004 Presidential Election Stolen?" by Steven F. Freeman and Joel Bleifuss (Seven Stories Press, New York, 2006).
- (2) Robert F. Kennedy's piece in Rolling Stone Magazine [5].

(3) And here's a real "hair raiser"! Actually presented as a kind of ghost story, Michael Collins describes the unbelievable consequences of the practice of "forcing" exit polls to agree with the official ballot tallies – a bizarre "see no fraud" gimmick used for the first time in 2004 but never explained to you by the so-called mainstream media [6].

Election 2006:

"Landslide Denied" by Jonathan Simon and Bruce O'Dell: A short barnburner of a read (even though mathematically correct!), this piece examines some different, but equally bizarre consequences of "forcing" the 2006 exit polls to "see no fraud" [7].

But if for some reason you might be reluctant to believe this statistical evidence (like maybe you don't do math and/or the conclusions of these scholarly studies are way too horrifying to accept), please read Pokey Anderson's trenchant exposition of how and why *all* electronic voting technology is not merely subject to hacking, but presents a clear and present "open door" just begging to be exploited by insiders [8].

IV. Mail-In Ballots: An Invitation to the Perfect Crime

I have been told that only two States in the Union have laws on their books allowing for recounts of mail-in ballots. Obviously, if mail-in votes should be stolen, it would be the perfect crime.

So who witnesses or otherwise assures the integrity of the mail-in ballots we cast? I don't know about other places, but every Election Day for a decade or so prior to 2004, the 8th floor of the Pima County Building, where the Mail-In ballots have been stored, was closed by the police bomb squad at the time of their unwitnessed counting, presumably by Pima County election officials. This old Pima County "tradition" is an eerie precedent for what happened in Warren County, Ohio, on Election Night 2004 [9].

Below is a table of the official Election Day 2004 voting at John Brakey's Arizona LD 27, representing a 74% turnout of some 80,000 registered voters:

Table 1.

Averages of 63 Precincts of AZ LD 27	Kerry/Dem	Bush/Repub	Other
E2004 At-Precinct Voting	61.9%	37.0%	1.0%
E2004 Early/Mail-In Voting	64.6%	34.6%	0.9%
Party Registration	48.8%	20.6%	29.0%

Note that the ever-vulnerable mail-in vote exhibits 2.4% *fewer* Bush votes than was the case for the At-the-Precinct voting. Could this be deliberate, given that those in the know would automatically look for anomalies in the Mail-In totals as possible prima-facie evidence of election theft?

V. New Evidence that They Hacked the *At-the-Precinct* Vote in 2004

After nearly 2 years of assuming I had done all I could by way of exposing Election-2004 fraud in Pima County, I was inspired to return to the Excel spreadsheets of Election 2004 data compiled John Brakey for all 63 precincts of Arizona LD 27, which comprises about 80,000 predominately-Hispanic, 80%-non-Republican registered voters ...who somehow seemed to vote 36% for Bush, even with an amazing 74% turnout!

Since John's data were broken out by precincts, I could do crude statistics on them. (Some of my esteemed colleagues in the EI community who practice full-blown statistics could certainly improve on what I have done by taking into account the variable uncertainties associated with varying precinct sizes.)

My starting premise was this: On average, for voting across a large district (59,752 voters actually voting in the present case), the ratios of At-Precinct to Mail-In to Provisional-Ballot of the vote shares of a major-party presidential candidate should be accurately 1 : 1 : 1.

In fact the data don't obey that rule here. Of the 31,595 voters voting at their respective precincts, 37.0% went for Bush, whereas "just" 34.6% of the 25,886 Mail-In voters went for Bush. This is actually a huge discrepancy, with a low probability of happening by accident.

I will now show you that (at least in AZ LD 27) it appears that someone hacked the *At-the-Precinct* vote but left the Mail-Ins untouched ...mostly.

Recall that John Brakey and I succeeded in proving that at Pct 324 of LD 27, colluding poll workers had stuffed ("Stacked") the ballot box against the possibility that a random recount should have been triggered. In such a case crooked election officials would have been standing by to "randomly" select Pct 324, and other similarly conspirator-infiltrated precincts, for auditing. In this event, we would be back again to the perfect crime.

This was John Brakey's great insight: the "Hack and Stack!"

John also caught the religious right-wing nuts at Pct 324 in the act of "Stacking" the ballot box there. And now thanks to John's compiled data for the entire LD, I was able to take a deeper look at the relative voting patterns of Provisional, At-the-Precinct, and Mail-In voting – which I suppose should occur in the ratios 1:1:1 within 95% statistical confidence for large enough voting units ...*provided* the election was not Hacked in one or two of these categories.

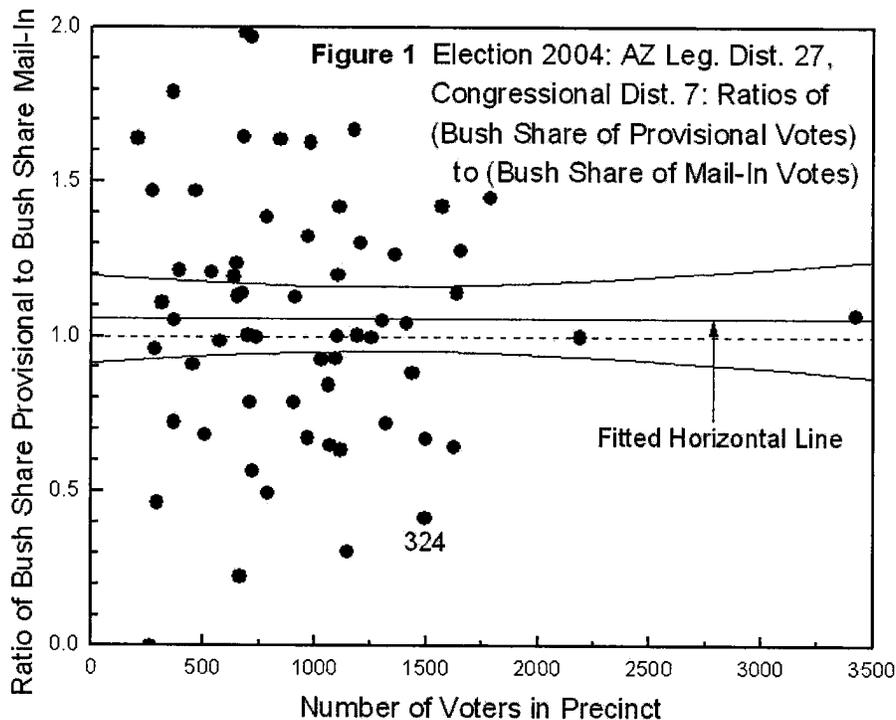
Here is how I approached the problem:

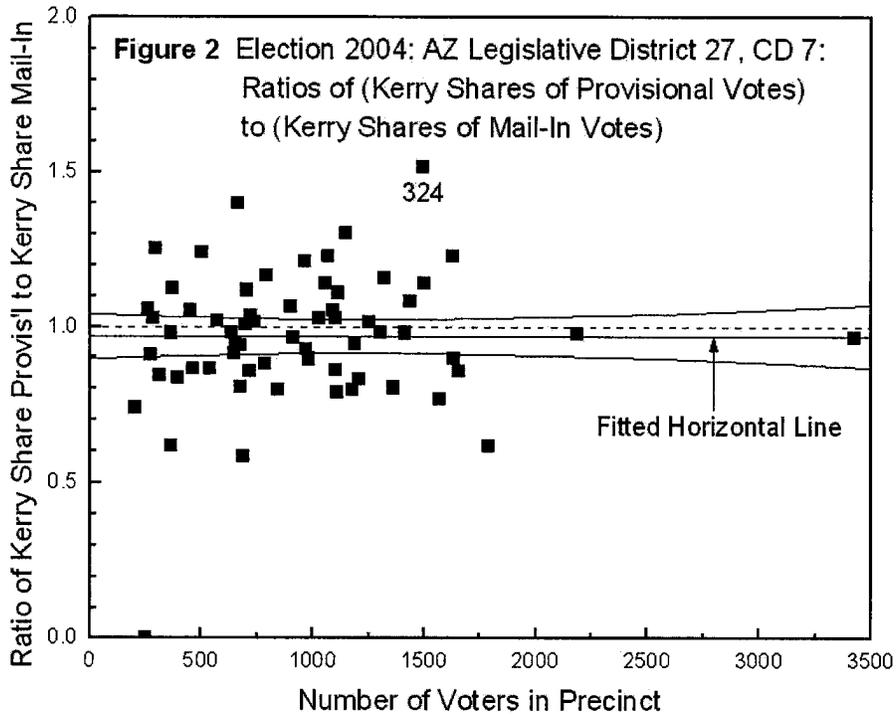
First, I assumed that the Provisional Ballots *actually accepted* by the County Registrar are virtually 100% honest, since each was sealed in an envelope with a voter signature and printed name and address on the affidavit affixed to the outside. For such a ballot to

have been accepted, the Recorder must recognize the signer of the affidavit to have been a voter registered to vote in the correct precinct who had not voted early (or elsewhere on Election Day). *And*, why even try to steal this component of the vote, given that the *accepted* Provisionals accounted for mere 3.8% of the total?

Unfortunately though, forensic analyses the Provisional-Ballot data are subject to large statistical uncertainties owing to the relatively small sample sizes (average 36 Provisional ballots officially *accepted* per precinct in AZ LD 27). Still, when I took the ratios of the Provisional to the Mail-In data, precinct-by-precinct, and used the mathematical curve-fitting software the came with my graph-making program, the continuous horizontal lines that fitted the data in the graphs of Figures 1 and 2 each agreed with the “null hypothesis” that the ratio should equal 1.00 (represented by the horizontal dashed line), within the bounds of the 95% confidence limits concomitantly generated by my software (pair of curved lines above and below the fitted straight line).

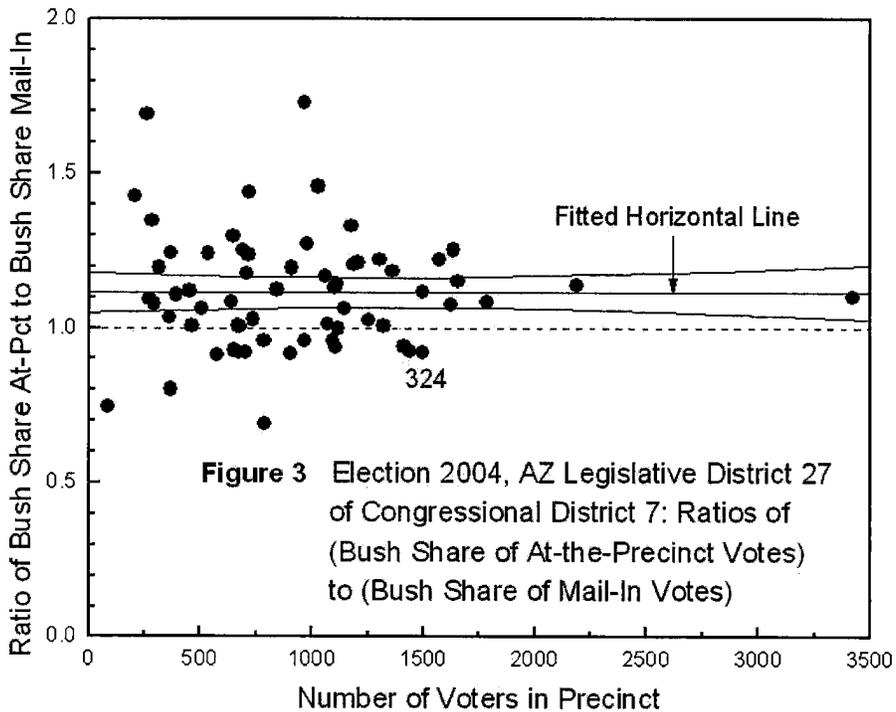
Figure 1 displays the individual-precinct Provisional-Ballot-to-Mail-In ratios of the Bush shares, while Figure 2 shows the corresponding ratios for the Kerry shares. Note that in both cases the black dashed line (the “null hypothesis”) falls between the two 95% confidence curves associated with the fitted horizontal line.

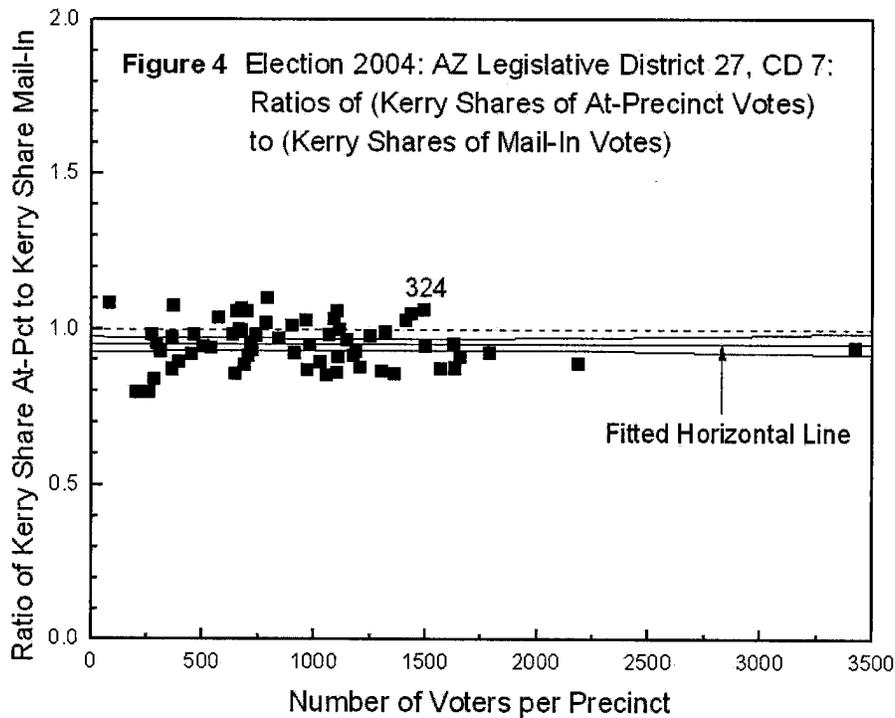




Conclusion: The vast majority of the Mail-Ins are likely *unHacked*.

Next, I took the ratios of the At-the-Precinct data to the (statistically-significant, and now shown to be mostly honest) Mail-In data. And, guess what? We see in Fig. 3 that Bush's ratios of his At-the-Precinct votes to his Mail-Ins are shifted on average 11.5% in his favor, and this shift is well *outside* the 95% confidence limits of the fitted horizontal line!





And in Fig. 4 the ratios of Kerry's At-the-Precinct votes to his Mail-In votes are seen to be shifted an average of 5% against him, again *outside* the 95% confidence limits.

My tentative conclusion is that the *At-the-Precinct* vote at AZ LD 27 was *Hacked!*

The alternates to this interpretation would be that all precincts were operated by poll workers as crooked as Rev. Kahn and his wife at Pct. 324, but far more competent (note that the data points for Pct 324 in Figs. 3 and 4 appear favorable to Kerry) ...or else the voters in Arizona LD 27 inexplicably wanted to keep Bush in office.

VI. Doing the Numbers: Reasons to Doubt that the No-Party-Preference Voters of AZ LD 27 Were Strongly Pro Bush

A critical reader might well ask the question: Couldn't the Pct 324 poll workers have been stealing votes on *Kerry's* behalf, given the positions of the data points in the graphs above? Well, the data points above are *ratios*, so they reveal nothing more than the relative differences between the At-the-Precinct voting and the Mail-In voting. Here is a table of the actual 2004 At-the-Precinct and Mail-In vote shares at Pct 324.

Table 2.

Precinct 324 of AZ LD 27	Kerry/Dem	Bush/Repub	Other
E2004 At-Precinct Voting	56.9%	41.6%	1.6%
E2004 Early/Mail-In Voting	53.6%	45.1%	1.3%
Party Registration	47.1%	21.5%	31.5%

By subtracting the LD-wide-average data shown in Table 1 from Table 2, we see in the resulting Table 3 that Kerry did stunningly *worse* (and Bush correspondingly much better) at Pct 324 than the *average* for the entire Legislative District 27 – *particularly in the case of the Mail-Ins: a net 19.1% shift in Bush’s favor* (after correction for the lower-than-average Democratic party registration)!

Table 3.

Difference (Pct 324) - (LD-27 Average)	Kerry/Dem	Bush/Repub	Other
E2004 At-Precinct Voting	-5.0%	4.5%	0.5%
E2004 Early/Mail-In Voting	-11.0%	10.6%	0.4%
Party Registration	-1.7%	0.8%	2.4%

Let me explain this kind of “vote shift” calculation by using the Pct-324 At-the-Precinct vote shares as the next example. In the first row of Table 3 we see that at Pct 324 Kerry has 5.0% *smaller* (negative) At-the-Precinct vote share than the LD-27-wide average. We also see that Bush has a 4.5% *larger* At-the-Precinct share than the LD-27-wide average. To get the net shift of votes from Kerry to Bush, we subtract the number in the Kerry column from the number on the same row in the Bush column. For the At-the-Precinct voting we get a 9.5% shift. Again, by using the numbers of Table 3, we are measuring this shift *relative to the LD-27-wide average*.

But now if we want to improve our accuracy, we really ought to correct for the fact that there was 1.7% fewer registered Democrats at Pct 324 and 0.8% more registered Republicans *relative to the LD-27-wide average*. For purposes of making any “correction” at all we have no choice but to first make a modest assumption; the simplest *unbiased* assumption we can make is that all registered Dems voted for Kerry and all registered Repubs voted for Bush. Thus, we take the net shift of party registration (in this case in Bush’s favor) at Pct 324 *relative to the LD-wide average* (2.5%) and subtract it from the net At-the-Precinct Kerry-to-Bush vote-share shift *relative to the LD-27-wide average* (9.5%) to get a the part of the shift that might be the result of fraud (“just” 7%). A corollary of our assumption is that 100% of the “corrected red shift” must derive from the votes of third-party or no-party-preference (NOP) voters in the precinct ...if the election was honest.

A few words about my jargon and acronyms. A “red shift” in my short-hand notation is a net shift favoring Bush, and a “blue shift” is one that favors Kerry. Also, from now on I will use the acronym “NOP” to include any third party voters, in addition to those voters who expressed no party preference.

Under the assumption I just described, one may calculate the corresponding percentages of NOP voters who cast their votes for either candidate. Consider Bush’s Pct-324 At-the-Precinct share of 41.6% in Table 2. If we subtract from that the Republican party registration of 21.5%, we get a number, 20.1%, which is the percentage of all voters at Pct 324 on Election Day 2004 who both voted for Bush and but (under our assumption) were neither Republicans nor Democrats. Therefore, this number of voters *must have been registered NOP*. Next we can take the ratio of this number to the percentage of *all voters* (no matter who they voted for) who were registered NOP, seen from Table 2 to be

31.5%. Expressed as a percentage, 20.1% divided by 31.5% is 64% -- an unexpectedly large number in my view.

Still, the devil's advocate (and Karl Rove) would argue that all red shifts resulted from NOP voters at Pct 324 – *and* LD-wide – who simply decided to vote for Bush in large numbers. (Their reasons for this might have been as trivial as having watched a “Swift Boat” attack on Kerry the night before or as visceral as a deep fear that Kerry would defend them less well from “the terrorists” than Bush did on 9/11).

So, *were* the NOPs in John Brakey's predominately-Hispanic precinct rabidly pro-Bush in that moment? Not according to the canvasses that John and I and others carried out just a few days before the election. I recall encountering very few Bush voters among those NOPs and infrequently voting (“turnout”) Dems that I canvassed. Unfortunately, however, our canvass sheets were lost before we totaled them up. So we have no objective pre-polling numbers for that part of Tucson.

Nevertheless, I did retain the results of my own canvass (for MoveOn) of several more-affluent, less-Hispanic, and roughly-50% Republican neighborhoods of Arizona CD 8, in the Catalina foothills 18 miles to the northeast of Pct 324. Of the 115 individual NOPs and “turnout” Democrats I interviewed, 95 were certain of, or leaning toward, voting for Kerry, while only 6 had any intentions of voting for Bush!

Now let me put these numbers in perspective. I conducted what would probably be regarded as a statistically significant poll of a predominately-WASP upper-middle-class Tucson neighborhood and found that **83% of the NOPs and turnout Dems planned to vote for Kerry and only 5% planned to vote for Bush!**

So if you should insist on believing that 64% (At-the-Precinct) and 75% (Mail-In) of the predominately-Hispanic NOP and turnout-Dem voters of less-affluent Pct 324 really voted for Bush (with a 75.9% turnout no less!), I'll sell you the Brooklyn Bridge.

VI. Some Very Odd Numbers

The *huge* discrepancy between the At-Precinct and Mail-In votes at Pct 324 noted above has to be *way* outside normal statistical error. While statisticians will need to demonstrate just how improbable the above numbers are, I conclude that the *Mail-In* votes – at least for Pct 324 – have to have been Hacked. If I am right, the next question is: In how many other precincts could the Mail-In vote have been Hacked? It cannot have been too many, given that Figures 1 and 2 show that the LD-wide *average* Bush and Kerry shares of the Provisional Ballots (presumed honest) are equal to their corresponding *average* shares of the Mail-In ballots with greater than 95% statistical confidence.

I decided that two of the prime candidates for investigation had to be the other two precincts (numbers 271 and 235), where John Brakey encountered poll workers behaving

peculiarly and/or displaying hostility on Election Day 2004. Tables 4 and 5 show the official results for Precincts 271 and 235, respectively, presented in terms of their differences from the LD-wide averages (exactly analogous to Table 3).

Table 4.

Difference (Pct 271) - (LD-27 Average)	Kerry/Dem	Bush/Repub	Other
E2004 At-Precinct Voting	1.9%	-1.2%	-0.7%
E2004 Early/Mail-In Voting	-2.6%	2.8%	-0.2%
Party Registration	5.0%	-2.7%	-0.8%

We see in Table 4 a 3.1% “blue shift” in the At-the-Precinct voting and 5.4% red shift in the Mail-Ins. But when I took into account the net 7.7% party registration advantage enjoyed by the Democrats over the Republicans of Pct 271, I arrived at the following corrected numbers for Pct 271 relative to the average for LD 27: a 4.6% At-the-Precinct red shift (no longer blue) and a hefty **13.1% red shift in the Mail-Ins!**

Now let’s look at Pct 235. In Table 5 we see a 2.3% red shift in the At-the-Precinct voting and whopping **13.8% red shift in the Mail-Ins** (both taking into account the tiny 0.2% correction for party registration).

Table 5.

Difference (Pct 235) - (LD-27 Average)	Kerry/Dem	Bush/Repub	Other
E2004 At-Precinct Voting	-1.5%	0.6%	0.9%
E2004 Early/Mail-In Voting	-7.5%	6.1%	1.4%
Party Registration	0.0%	-0.2%	1.7%

Here is my hypothesis for what went down in LD 27 of Tucson CD 7 on Election Day 2004. There was a conspiracy comprising (1) insiders with access to the 1.94w memory cards in the Diebold AccuVote OS optical scanners (or alternatively to the GEMS central tabulators) and (2) a cadre of colluding poll-worker crews, including the one headed by Rev. Kahn at Pct 324. The overall plan was to *Hack* the At-the-Precinct vote at *all* precincts *except* the ones manned by colluding poll workers, whose job it was to *Stack* (stuff) the ballot boxes at those polling places. However, the evidence shows that someone likely decided to Hack the Mail-In Ballots in these Stacked precincts – perhaps to shield the crooked poll workers there from suspicion, knowing that forensic investigators might compare the Mail-In votes with the At-the-Precinct votes as a possible sign of ballot-box stuffing. (If that was their objective, they badly overdid it, with a **19.1% red shift in the Mail-Ins** vis-à-vis a red shift of “just” 7% managed by the Kahn team.)

Or maybe it was pure greed: Leave no precinct left unHacked.

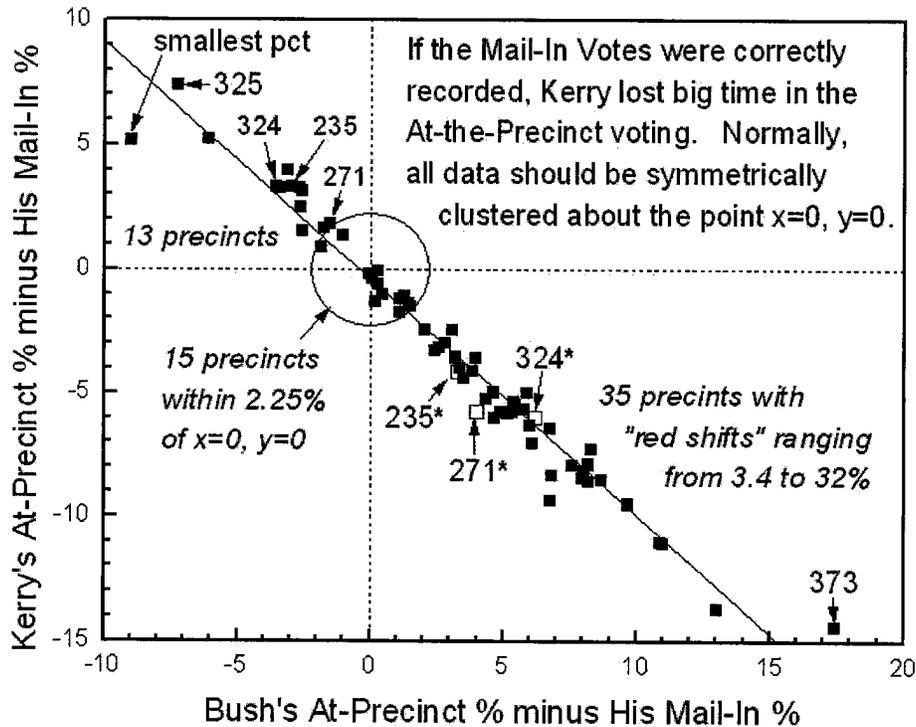
VII. Another Way to the See the Fraud in a Forest of Data

One of the things that I have learned in my 41 years as a research physicist, is that the meaning of one’s data is best comprehended – and explained to others – by finding the most telling way(s) to graph them. So, I tried something else with the AZ LD 27

Election-2004 data. It is a very different way to display the same information, one that affords a more dramatic (if not yet statistically analyzed) visual impression of the Election-Day-2004 shenanigans in Pima County, AZ. In Figure 5 I have plotted Kerry's At-the-Precinct vote shares *minus* his Mail-In shares (in percent) on the y axis versus the corresponding subtraction of data for Bush's shares on the x axis.

Figure 5 Election 2004, 63 Precincts of Arizona LD 27:

At-Precinct Presidential Vote Shares Differ Greatly from Early Vote!



Normally one expects the Mail-In vote share to be very close to the At-the-Precinct share for the same presidential candidate if the precincts are large enough. In AZ LD 27, the two smallest precincts had 87 and 208 voters actually voting and the remainder of the precincts ranged from 265 upward to 3,453. (The 87-voter precinct is indeed an odd fellow, appearing well off the main curve in the upper left quadrant.)

The fitted curve in Figure 5 is a straight line with slope of -0.98, which is close enough to the expected slope of -1.00 that would pertain when 100% of the votes are divided between just two candidates and there are enough total voters that the laws of average are fully expressed. However, this fit doesn't quite pass through the origin ($x=0, y=0$), as I believe it should even when there are third-party candidates. My guess is that when some statistical simulations are done, it will be found that greater than half of all precincts of these sizes will be found fall within an ellipse *centered on the origin* with its major axis extending about 2.5% to both the upper left and lower right along a line of slope -1.00.

For present purposes, I've placed a circle of radius 2.25 about the origin in Figure 5. It encloses 15 precincts that might be considered "normal" ...except for the fact that only 2 of the enclosed ones are blue shifted, while 13 are red shifted. Outside of this circle there are 13 blue-shifted precincts in the upper left quadrant and 35 red-shifted precincts in the lower right quadrant. And, not only are there **2.7 times more red-shifted precincts** than blue-shifted ones outside the circle, but *the average magnitude of these red shifts is roughly double the average magnitude of the blue-shifted ones.*

While it will be necessary to do some "Monte Carlo" computer simulations to estimate just how improbable these numbers are as random happenstance, such a lopsided outcome certainly has to be extremely rare (I would guess less than one chance in a million). And if the lopsided nature of the data of Figure 5 should be the result of fraud, I infer this fraud was committed mostly against the At-the-Precinct balloting, since Figures 1 and 2 have suggested that the Mail-In votes were accurately counted ...with the exceptions that I will now single out.

Notice that the Precincts that I suspect (or know) were Stacked – represented by the hollow squares in the upper left quadrant of Figure 5 – are mildly blue shifted. I wondered what they might look like if I were to subtract the LD-wide *average* Mail-In shares rather than the actual ones for these precincts (which I suspect were influenced by Hacking). When I did that, all three of these data points became moderately *red* shifted. Then, to improve my accuracy, I thought I should correct the LD-wide-average used in these respective subtractions to take into account the differences in party registration in these three precincts with respect to the LD-wide average registration. This correction actually moved these data points deeper into the lower right quadrant ...to the positions indicated in Figure 5 by hollow squares and labeled with the precinct numbers followed by asterisks. This exercise seems to confirm that the Mail-In ballot tabulation for Pct 324 was indeed Hacked ...even as the At-the-Precinct ballot box was being Stacked by Rev. Kahn's crew. Furthermore, it also provides circumstantial evidence that Pcts 271 and 325 may, as John Brakey suspected from day one, also have become victims of the same double-barreled brand of vote theft as was evidently inflicted on Pct 324.

Finally, out of curiosity, I took a closer look at the data for the two extreme outlier precincts on Figure 5, that is, Pct 325 on the extreme upper left and Pct 373 on the extreme lower right. It turns out that they both had interesting stories to tell.

The Pct 325 polling place was the Pascua Yaqui Tribe Tribal Council Chambers, where I would guess that many of the 373 voters were Native Americans. In any event, 65.1% were registered Democratic and *only 3.6% were registered Republican.* The official Provisional and At-the-Precinct tallies were respectively 88.5% and 83.4% for Kerry. It was a veritable landslide, with **58.3% of the NOPS joining the Dems in voting for Kerry at the Precinct.** But wait! The official Mail-In count was just 76.0% for Kerry. This anomalously low value translates into a 10.7% red shift relative to the LD-27-wide Mail-In average. *And we can infer from these numbers that the NOPS who voted by Mail went 63.1% for Bush!* Do you believe that? If you do, I want you to know that I've marked down the Brooklyn Bridge for quick sale...

So they Hacked the Yaquis too. These vote thieves were equal-opportunity stealers of our inalienable rights.

As for Pct 373, with its data point way down in the lower right corner of Figure 5, I calculate from the official 2004 Election returns that fully **72.8% of the NOPS voting by Mail-In cast their ballots for Kerry**. But, get this! **62.8% of the NOPS who voted at the Precinct were recorded as voting for Bush!** This is the diametric opposite of the behavior of the NOPS in Pct 325. This cannot be an accident.

A very large number of electors in AZ LD 27 were denied their constitutional right to have their every vote count.

Factoid: The polling places of three of the five precincts where I have found startling skewing of the votes from normal expectation have been two churches and a church school, while a fourth one at a public school had a reverend and his wife as the head pole workers. This may not be accidental. Both John Brakey and Mark Crispin Miller have done extensive research revealing the involvement of legions of Christian zealots in the campaign to steal Election 2004, and 2006, and 2008...

VIII. The Pima County Democratic Party's Suit against Pima County

One wonders if John Brakey ever sleeps. Last year John decided to teach himself the "geek Greek" of the Diebold GEMS central tabulator. To do this he got the State Democratic Party to bring in one of the best Election Geeks in the Country, Jim March. Jim is an experienced computer tech specialist with 17 years in the IT industry. In 2003 he first heard of Bev Harris' work exposing problems with the Diebold voting systems as used here in Pima County, and he began helping Ms. Harris analyze the 40,000 files she had obtained from a Diebold website lacking any security. Jim was lead plaintiff (along with Ms. Harris) in a California consumer protection suit against Diebold netting that state a \$2.6 million refund, and he now sits on the board of directors of Black Box Voting, a national non-profit. He was brought to Pima by the State Democratic Party to help monitor the primaries and General Elections and is now a tech consultant on the public records lawsuits fought by the county as part of the aftermath.

By Freedom of Information Act (FOIA) requests, John obtained the computer logs of the Pima County tabulators for the past several years. He quickly discovered that ever since the arrival of Brad Nelson as the Pima County Director of Elections, someone at the Elections Department has been printing summary reports of Mail-In ballots counts up to a week or more before the election. This is strictly illegal under Arizona law: "...there shall be no preferential counting of ballots for the purpose of projecting the outcome of the election." And, obviously, anyone in possession of such information would have highly accurate advance information to calibrate any Trojan Horses present in the At-the-Precinct 1.94w memory cards so as to infallibly flip sufficient votes to change the outcome of a race on Election Day without causing undue suspicion by overdoing it.

Although merely printing illegal summary reports of early balloting is not prima-facie evidence of election fraud, on 1 February 2007 the Pima County Democratic Party filed a (civil) public records lawsuit in Pima County Superior Court against the Pima County Board of Supervisors and the County Treasurer seeking the production of summary reports of early ballots that were printed without election observers present and allegedly sealed in the Pima County Treasurer's vault [10].

Then John spotted something else. Back in 2006 there was a ballot initiative to impose a half-cent sales tax to pay for a 20-year, \$2 billion Regional Transportation Authority plan ultimately approved at the same election. After the first day's Mail-In returns, the computer operator had backed up the election and the very next morning backed it up again, whereupon he immediately printed another summary report. John recognized instantly that the operator had it within his power to take home a copy of the first day's voting, alter it using Microsoft Access (for example to flip votes in the event that the RTA tax was being rejected) and then save this altered version the next morning. (Thus, the purpose of the new summary report might have been to assure that the manipulations he had inserted had actually "stuck").

Enter Attorney and Democratic activist William J. (Bill) Risner. As an "officer of the court" bound to report any evidence of possible criminal activity that comes to his attention, Bill immediately filed a criminal complaint with the AZ Attorney General. In response, the Pima County Board of Supervisors went to court asking for a stay on civil case until the civil case is settled. However, the judge recently ruled in favor of Bill Risner's arguments that the civil and criminal cases are not barred by law from proceeding separately. And another piece of good news is that the local media have not shied from reporting this story [11, 12].

Still, John Brakey and Bill Risner, so far as I know, haven't been paid a red cent for their efforts or court costs, even by the Democratic Party.

XI. The Author's Thoughts about All of This

For the most part, in this article I have been clinically dispassionate ...as though I were writing just another scientific paper. On occasion I have been flip and have made a bit of black humor, though this has been just an artifice to hold the reader's attention. In the end, as I reread what I've written, I keep returning to the thought of the nearly 60,000 Americans from all walks of life and ethnic heritages belonging to Arizona Legislative District 27 who turned out on Election Day 2004 to exercise their constitutional right to "throw the bum out." What happened to these Tucsonans that day is surely a microcosm of what was simultaneously happening to Americans all across our country. I reflect on the facts that not only were these good folks' wills – and their inalienable rights – subverted, but they are not even told by the mainstream media what was done to them. So they have no choice but to blame themselves for "the bum" still being at the helm ...still driving Titanic America toward the not-too-distant icebergs, full speed ahead. And all the while, the evil ones who contrived this heinous crime against our Republic go

about consolidating their power and wealth and pursuing their illegal wars at the expense of the good people they stealthily disenfranchise.

“Cry, the Beloved Country!” – Alan Paton

References

- [1] [http://www.drivehq.com/file/df.aspx/publish/dlgriscom/Election Fraud Research/Griscom_AAAS 2007 Annual Mtg.ppt](http://www.drivehq.com/file/df.aspx/publish/dlgriscom/Election_Fraud_Research/Griscom_AAAS_2007_Annual_Mtg.ppt).
- [2] www.bbvforums.org/cgi-bin/forums/board-auth.cgi?file=/1954/15595.html
- [3] www.votetrustusa.org/index.php?option=com_content&task=view&id=798&Itemid=51
- [4] http://www.opednews.com/articles/opedne_michael_070313_the_long_road_to_dem.htm
- [5] http://www.rollingstone.com/news/story/10432334/was_the_2004_election_stolen
- [6] <http://www.scoop.co.nz/stories/HL0706/S00164.htm>
- [7] http://electiondefensealliance.org/landslide_denied_exit_polls_vs_vote_count_2006
- [8] <http://www.votersunite.org/info/PeeringThruChinks.pdf>
- [9] <http://freepress.org/departments/display/19/2004/957>
- [10] <http://www.tucsonweekly.com/gbase/Currents/Content?oid=92557>
- [11] <http://www.azstarnet.com/dailystar/184860>
- [12] <http://www.tucsoncitizen.com/daily/opinion/53903>

ver. 4.4

From: bbcatt
Sent: Monday, July 30, 2007 8:00 AM
To: Voting Systems
Subject: Decertification

Dear Debra Bowen,

I am asking you to please de-certify the current use of voting machines in California. Here in San Diego last election, I was a precinct inspector close to my neighborhood. We were trying to be reassuring to the voters that came in that their vote was safe, but were not convinced ourselves.

There is one incident that continues to haunt me. An elderly gentleman came to me worried that his vote was not counted correctly because the touch screen skipped over a portion of the ballot. This man was very concerned. He was a naturalized citizen after WWII and has voted in every election since that time. I tried to research the possibilities by talking not only to the troubleshooter (who was very nice but had no answers) and the registrars office to no avail. This man held voting sacred as do I, and we could not tell him that his vote was most likely sacrificed to the glitch of the machine because we could NEVER BE SURE! Please de-certify these machines, there are too many uncertainties that cannot be addressed.

Sincerely,

Barb Cattedra

From: John Fillums
Sent: Monday, July 30, 2007 10:37 AM
To: Voting Systems
Subject: question for FAQ

re additional questions for the FAQ:

Is there a subsystem in place whereby team members can report conditions/incidences of external pressures placed on their investigating activities?

(If such system were in place and reports available to the public, voters might have more confidence that the review was fairly conducted.)

Sincerely,
R John Rogers
San Diego, CA

P.S.

I voted for Debra Bowen and am delighted to see that she is following thru on her promise, and that finally this issue is being taken seriously!

Congratulations to all of us who are concerned about voting integrity.

Luggage? GPS? Comic books?
Check out fitting [gifts for grads](#) at Yahoo! Search.

From: Tom Courbat
Sent: Monday, July 30, 2007 3:27 AM
To: Voting Systems
Cc:

Subject: Public Hearing Comments for today, July 30, 2007
Importance: High

7-30-07

From Tom Courbat in Riverside County, CA.

Dear Secretary of State Bowen,

COUNTIES AND VENDORS WON'T COMPLY WITH CERTIFICATION CONDITIONS

Please do not allow continued certification of E-voting machines by adding requirements of actions that counties must take to shore up security of the system or of changes that vendors must make to assure compliance.

As a former high-level executive recruiter, I found one particularly telling truism in our industry. This is, "Past performance is the best indicator of future performance."

Counties track record is to resist direction from Secretary of State

The counties have clearly demonstrated they will ignore both the law and directives from the Secretary of State. In Riverside County, the county refused to post precinct results at the precincts, even after requesting a waiver of that requirement from the SOS and being denied the waiver. Not until media coverage of their transgressions, sparked by continued efforts of election integrity advocates to expose their disregard for the law, did they finally comply.

Indeed, our Board of Supervisors chairman, Mr. John Tavaglione has stated, on film "I think she's nuts, quite frankly, and I don't mind telling that to her face." He was referring to you, Madame Secretary. And Supervisor Jeff Stone has asked the question "Does the Secretary of State have the authority, by herself, to decertify a system based purely on a political decision rather than on a data-backed decision?" You can view this 3minute and 45 second film of our Board of Supervisors in action at <http://tinyurl.com/2cuzpf>.

The President of the California Association of Clerks and Election Officials (CACEO), Steven Weir was quoted as saying, "... **clerks could decide to ignore Bowen's findings and continue to use their systems**, which are already federally qualified." Such a decision which would almost certainly create a legal standoff according to the article in the Contra Costa Times dated July 23, 2007.

Given the above examples, of which there are hundreds more, there is no reason to believe they will suddenly have an epiphany and decide that whatever conditions are imposed by the Secretary of State are righteous and will be implemented without delay.

07/30/2007

Vendors have never exhibited good faith and cannot be trusted to do so now

The review of your team of computer scientists has pointed out numerous instances of electronic voting machine (EVM) companies stating one thing and doing another. Just one of dozens of examples (this one regarding Sequoia): Vendor statement: "The lack of [WinEDS SQL] server access by individual users provides the application with a secure client-server environment." Team findings: "Unfortunately, this is not true. In fact it is possible to connect to the database and completely compromise the MS SQL server host without using the WinEDS application." **"The MS SQL server delivered with the Sequoia system enables users to execute arbitrary commands."** Thus, any election can be compromised at any time by any user. Unbelievable!

Please decertify the Sequoia system, including the central tabulator which can be compromised by arbitrary commands by any user. Our votes are too important to be entrusted to such an unsecure environment. Our Registrar of Voters, Barbara Dunmore, responded to a question from Supervisor Jeff Stone in the affirmative when asked if she would be able to successfully administer a paper-based election in February, 2008 if the machines are decertified. So I guess Riverside is good to go without the Sequoia system. And I suspect that despite all the hoopla, all the other counties can count ballots on paper as well, since we have done it for over 100 years in this state.

Best regards,

Tom Courbat
SAVE R VOTE

P.S. As you know, our BOS appointed a "Blue Ribbon" Elections Review Committee to review our system and make recommendations. Their number one recommendation – get rid of the DREs as quickly as possible. And they studied our situation for six months.

The degree of willingness of a government to open itself up to public scrutiny and public audit foretells the quality and integrity of that government.

Heyes, Jason

From: Washburn, John
Sent: Monday, July 30, 2007 4:07 AM
To: Voting Systems
Subject: Public Comment to the Top-to-Bottom Review

Dear Ms. Secretary:

Please find attached my public comments on the Top-to-Bottom Review of voting systems.

07/30/2007

Public Comments of John Washburn

Top to Bottom Review of Voting Systems used in California.

Secretary Bowen, I thank you for this opportunity to make a public comment on the results of the top to bottom review. My name is John Washburn. I am a resident of Germantown, Wisconsin. I have worked as a software tester and in the field of quality assurance since 1994. I currently am certified by the American Society for Quality as a CSQE; certified software quality engineer. It is a certification I have held continuously and proudly since 1998. I have read the documents found on the website of the California Secretary of State and would like to submit the following comments.

I read with fascination the various attack scenarios. Many are elegant applications to voting systems of well understood attack vectors used against other computerized systems. The results are important, disturbing, and must be addressed. But, as disturbing and import as these technical findings are, I do not believe they are the most disturbing information uncovered by the top to bottom review. The most disturbing findings are:

1. The systems are inaccessible and, in some cases, is an active obstacle to voting accessibility.
2. The revelation that vendor representations may be fraudulent.
3. The continuing evidence the NASED/ITA model for certification has failed and is not worth the paper it is written on.
4. The continuing evidence voting systems are defect-dense.

The Systems are not Accessible

The Accessibility Review by Noel Runyan and Jim Tobias is thorough, detailed, and precise in its findings. None of the three systems reviewed meets the minimum accessibility of the Help America Vote Act (HAVA) or the 2005 Voluntary Voting System Guidelines (2005 VVSG). Direct Recording Electronic (DRE) systems compared to precinct based optical scanning are more expensive to purchase, more expensive to test, more expensive to maintain and, by all indications, are more insecure. The justification for why American elections must endure the addition insecurity and expense of DRE systems is that DRE systems allow disabled voters and voters in language minorities the opportunity to vote privately and independently. This accessibility review refutes this justification in exceptional detail. For the first time, someone has enumerated all of the accessibility requirements of the both HAVA and the 2005 VVSG and objectively tested for conformance. Moreover, under some conditions the DRE system is an active impediment to voting.

If the person is voting in a language other than English and which uses a non-Roman alphabet such as Chinese, the DRE screen does not render characters at all. Even if the translation were well done, it is worthless if the translated text cannot be rendered for display. This is an active impediment to voting by these language minorities.

If the person is has normal vision, normal hearing, and normal upper body strength and dexterity, but is confined to a wheel chair, the DRE system is inaccessible because the forward approach is blocked by the narrow legs of the stand, hard to reach because of the height, and subject to parallax errors. For this class of voters, the DRE either prevents voting or make voting uncomfortably arduous because of the need for a side approach. Since Wisconsin has paper ballots which are tallied by optical scanner or are hand counted, voters who are wheel chair bound can be accommodated with a clip board or a suitably low table. If the polling location has only DRE equipment though, then the DRE equipment **introduces** a barrier to voting which did not exist before.

Representations of the Systems May be Fraudulent

The Red Team Report for Sequoia by Vigna, Kemmerer, et. al. includes several comments where the properties of the Sequoia Voting System were misrepresented to the security testing team by Sequoia. Section 4.4 and 4.8 are two such examples. Section 4.4 of the security assessment report states:

*There is no way to determine which version of the firmware is running on an Edge device. The Sequoia documentation states that the firmware is stored in ROM and that checksum-based mechanisms are used to determine if the firmware has been modified maliciously. However, **in reality there is no secure, hardware based mechanism** to ensure that no corrupted firmware gets loaded and executed. In addition, the Edge firmware is stored on a flash memory card and can be easily overwritten. Hardware support for trusted software execution and the use of non-writable memory would protect the Edge device from a large range of attacks from both insiders and outsiders.*

Section 4.8 of the security assessment reads:

In the documentation ([10], p. 3-1), it is stated that: "WinEDS currently does NOT utilize code outside of MS SQL Server and no connections or permissions are required on the server (besides SQL Client.) The lack of server access by individual users provides the application with a secure client-server environment. The election data stored on the server can only be modified by authorized users only through the application."

Unfortunately, this is not true. In fact, it is possible to connect to the database and completely compromise the MS SQL server host without using the WinEDS application. This is achieved by exploiting two security problems. First of all, the WinEDS access control procedures can be bypassed. Second, the MS SQL server delivered with the Sequoia system enables users to execute arbitrary commands.

The emphasis of the quoted sections above is mine and highlights the diplomatic language of the assessment team. The representations of section 4.8 were made by Sequoia to the Wisconsin State Elections Board during the May 16, 2007 of the Elections board. To me this indicates the representation by Sequoia Voting Systems of the security of WinEDS is a consistent representation.

Another consistent representation is that the firmware of the system is in read-only memory (ROM). Instead the security team found the firmware is stored on EEPROM/Flash memory. Flash memory is the same type of memory used in a portable flash drive or an iPod. Read-only memory is just that; read-only. Once created the contents cannot be re-written, but can only be read. While flash memory retains its contents when the power is off (non-volatile), it can be re-written (mutable). Read-only memory is both non-volatile and immutable. Flash memory is not.

Both of these representations (ROM based firmware and secured SQL architecture) are false. Since, I am not an attorney, I cannot judge whether such false representations constituted fraud. But, the misrepresentations to me are fundamental and hard to classify as anything other than an effort to deceive.

The NASED/ITA Testing Model has Failed

The security reports as a whole present more evidence that the NASED/ITA framework for testing and certification has been an utter failure. This is a significant problem which stretches across the whole country. The NASED/ITA model was used to as the basis for certification of EVERY voting system currently in use in the United States. With the exception of lever machines in New York, only equipment qualified by the NASED/ITA process was used in the most recent Federal election held on November 7, 2006. That this testing and certification model is ineffective and flaw is a concern for the whole country not just the State of California.

The NASED/ITA testing framework failed to find any of the findings of these three reports during repeated rounds of testing conducted over the course of several years. The results of these three reports from the Top-To-Bottom Review on the other hand were all uncovered in less than one month of examination. Each of the findings in the security reports are evidence of the failure of the NASED/ITA process. For illustration I will focus on only two of the findings from the Sequoia security assessment. The NASED/ITA testing and certification system failed to find:

- *There is no way to determine which version of the firmware is running on an Edge device.*
Section 4.4 of the Sequoia Security Assessment Report.
- *The Edge firmware was discovered to include a shell-like scripting language interpreter.*
Section 4.5 of the Sequoia Security Assessment Report.

The inability to identify the system under test is a violation of Section 8.6.d, Volume I, Section 8.7.1, Volume I, and Appendix B.3 Volume II of the 2002 VVSG.

Section 8.6.d Volume I states:

The vendor shall establish such procedures and related conventions, providing a complete description of those used to:

- Perform a first release of the system to an ITA;*
- Perform a subsequent maintenance or upgrade release of the system, or a particular components, to an ITA;*
- Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the qualified system version; and*
- Perform a subsequent maintenance or upgrade release of the system, or a particular component, to a customer, **including confirmation that the installed version of the system matches exactly the qualified system version.***

Section 8.7.1 Volume I states:

8.7.1 Physical Configuration Audit

The PCA is conducted by the ITA to compare the voting system components submitted for qualification to the vendor's technical documentation. For the PCA, a vendor shall provide:

- Identification of all items** that are to be a part of the software release;*

Section B.3 Volume II (System Identification) states:

B.3 System Identification

This section gives information about the tested software and supporting hardware, including:

- System name and major subsystems (or equivalent);*
- System Version;***
- Test Support Hardware; and*
- Specific documentation provided in the vendor's TDP used to support testing.*

Since, “*There is no way to determine which version of the firmware is running on an Edge device*”, it is not possible to meet any of these three requirements of the 2002 VVSG. How was failure to conform this missed by the vendor funded test labs during repeated rounds? Paul Craft, Steven V. Freeman, and Britt Williams of the technical subcommittee of the NASED Voting Systems Board reviewed every report generated by the vendor funded ITA labs. How is it that they failed to notice that the labs were not testing for conformance to the system identification requirements? One possibility is that these three granted a waiver to Sequoia Voting Systems on the matter of conformance to standard. Such waivers to conformance are permitted by Appendix B.5 Volume II of the 2002 and 2005 VVSG. The relevant paragraph of Appendix B.5 of the 2002 VVSG reads:

Of note, any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection. Deficiencies of this type may include failure to fully achieve the levels of performance specified in Volume I, Sections 3 and 4 of the Standards, or failure to fully implement formal programs for qualify[sic] assurance and configuration management described in Volume I, Sections 7 and 8. The nature of the deficiency is described in detail sufficient to support the recommendation either to accept or to reject the system, and the recommendation is based on consideration of the probable effect the deficiency will have on safe and efficient system operation during all phases of election use.

As the security assessment report states interpreters are prohibited by the 2002 VVSG. Again, how is that the vendor funded ITA labs failed to notice the presence of a prohibited interpreter during any of several rounds of testing? The problem for California on this matter is more acute. In December of 2005 it became public knowledge that the voting systems from Diebold Election Systems Inc. used prohibited interpreters and interpreted code. In response, Bruce McDannold, Interim Director of the Office of Voting System Technology Assessment, specifically asked Paul Craft and Steven V. Freeman if there were any other voting systems used in California which also had interpreters and interpreted code. In this [email exchange](#), Mr. McDannold states reveals the State of California is “picking on” Diebold over the interpreted code issue. At the time Mr. Craft and Mr. Freeman stated no other voting system used in California used interpreters or interpreted code. It is ironic that the security assessment team has vindicated Diebold Election Systems. There were two voting systems in California using interpreters, but only Diebold was singled out for investigation.

Paul Craft and Steven V. Freeman are 2 of the 3 people on the technical subcommittee of the NASED Voting Systems Board. How is it they were unaware of the interpreter found in the Edge voting systems from Sequoia? Mr. Craft and Mr. Freeman were hired because of their connection with the NASED process and their expert knowledge of voting systems. The State of California specifically and directly asked both Mr. Craft and Mr. Freeman if about interpreters in California Voting Systems. They stated Diebold was unique. Mr. Craft and Mr. Freeman failed the State of California when they provided this incorrect answer. One may ask what other work product from Mr. Craft and Mr. Freeman may also be defective.

The Systems are Defect-Dense

Over the years, every time a vendor independent team investigates a voting machine the team finds new, significant, and possibly election-altering defects. An incomplete list of these past studies is:

- The 2003 John Hopkins report,
- The 2003 RABA report from Maryland,
- The 2003 Compuware report from Ohio,
- The 2004 follow ups reports by Compuware to the initial 2003 Ohio report,
- The 2005 examinations by Hugh Thompson in Leon County,
- The 2005 examinations of Hari Hursti in Leon County, Florida,
- The 2006 examinations by Hari Hursti in Emery County, Utah,
- The 2006 Princeton report on the TSx,
- The 2007 report from the University of Connecticut on the AccuVote OS, and
- The 2007 report from the University of Connecticut on the AccuVote TSx.

These three security assessments again find new and significant defects which are distinct than those found in these prior reports. In my expert opinion this is a symptom of the software that the software in these systems is defect-dense. A defect-dense system is one where the number of defects per line of code is high. Other measures of software size such as function points may be used to describe defect density. Defect-dense systems are marked by the same properties as exhibited by voting systems:

1. Different testers find different defects. In defect-sparse systems, different testers tend to find the same defects over and over. This is because there are so few defects to find that effective testing by different groups repeatedly find the few defects present.
2. The defects found are generally severe. This is because severe defects are usually found before minor defects. Major defects are easier to detect because the behavior is manifestly incorrect and major defect tend to hide or obscure the presence of more minor defects.

Consider a line of automobiles from the fictional manufacturer Washburn Motors. What if every time a mechanic or engineer not hire by Washburn Motors examines one of my cars and find something new which is wrong and that something found is serious? One mechanic finds the engines stalls at 60 miles per hour. A second discovers the axles tend to break. A third notices the brakes fail intermittently in warm weather. A fourth discovers the lock on the doors can be bypassed by unscrewing the door from its hinges. A fifth discovers the odometer does not sometimes loses 18,000 miles. Would you by a car from Washburn Motors? Most would not. This is because even though they do not use the term defect-dense, most people instinctively recognize the symptoms and would rationally avoid buying a lemon from Washburn Motors.

Voting systems currently exhibit the same behavior as the fictional cars from Washburn Motors. Every time someone not hired by the manufacturer examines the product they find something new which is wrong and that something found is serious.

Conclusion

Secretary Bowen faces some hard choices which must be made in a short time frame. I wish I could offer more than the following suggestions.

1. Do not rely on the results of the NASED/ITA model. It has failed and the certifications issued under the program may not be worth the paper they are written on. I would urge the Secretary to consider creating a multi-state testing consortium. This idea was first presented to the state by Eric Lazarus during the Voting Testing Summit sponsored by the State of California in 2005. His paper is found here:
http://www.sos.ca.gov/elections/vstsummit/presentations/a_vision_for_testing_election_systems_lazarus.ppt. An expansion on the framework proposed by Mr. Lazarus is found here:
http://votetrustusa.org/index.php?option=com_content&task=view&id=870&Itemid=26. I have misgivings that the EAC/NIST/VSTL model currently under construction is little more than the NASED/ITA model with different acronyms.
2. To the extent possible limit the expansion of this unreliable and inaccessible voting technology. Consider technology which actually expands accessibility such as non-tallying ballot marking devices (e.g. Automark or Vote-PAD) or systems which print ballots on demand under the direction of voters. Expanding the franchise to those with disabilities or who are in a language minority is goal which resonates with the deepest aspirations of the American ideal. We should select technology which is both appropriate and effective in realizing this ideal.
3. Sequoia was asked by Bruce McDannold in December of 2005 if there were interpreters or interpreted code found on voting systems from Sequoia. What was the company response to this question? The representations made by Sequoia which have been contradicted by the security assessment team must be assessed to determine if those representations constitute fraud.
4. Where the non-conformances found by the top-to-bottom review also found by the NASED/ITA? Testing results are under the NASED/ITA model are consider trade secrets held by the equipment manufacturer. Thus it is possible the reported non-conformances were discovered by the NASED/ITA process and granted waivers, but the disclosure of such waivers has be blocked by the assertion of trade secrets.

From: TemeculaPaul(
Sent: Sunday, July 29, 2007 1:54 AM
To: 'oting Systems
Cc:
Subject: Public Comment Testimony for 7/30/07 Re Sequoia

Dear Secretary Bowen:

You have my heartfelt respect for finally questioning this machinery we have unquestionably accepted to run the elections that decide the fate and legitimacy of our democracy.

From review of the initial red team reports, it seems that every component of the Sequoia equipment tested was vulnerable to tampering. The report on Sequoia appeared more damning than the reports on Diebold and Hart voting equipment.

In previous correspondence, I have sent you video stills that I personally captured of multiple poll workers handling Results Cartridges in a Sam's Club parking lot in Riverside County that was designated by the ROV as an election collection center in November, 2006. Riverside County introduced the nation to electronic voting in 2000 yet in 6 years of use, rudimentary control of the chain of custody has not been established -- or ever initiated by the Registrar of Voters office. In fact, you will find few counties coming close to being the champions of privatized, computerized voting as you will find in Riverside County .

Your office has been contacted repeatedly by local hound dog Tom Courbat to pressure the ROV to comply with existing election law. Thankfully, your office has prompted our registrar and elected supervisors to take some resistant steps toward election integrity, but the secrecy and resistance this county has taken toward public inquiry of the election system is suffice to determine that Sequoia voting equipment cannot be adequately safeguarded in this or any county in the state.

With all due respect, if Sequoia voting equipment is certified as legitimate, then our democracy is not.

Paul Jacobs

Get a sneak peek of the all-new AOL.com.

From: Mark E. Smith
Sent: Sunday, July 29, 2007 3:23 AM
To: Voting Systems
Subject: Public Comment on Top-To-Bottom Review

To: California Secretary of State Debra Bowen and the panel

From: Mark E. Smith,

I took Mikel Haas, then the San Diego Registrar of Voters, to court prior to the 2006 election due to the fact that he had not been selecting the precincts for recounts randomly as required, there was no proper chain of custody on the voting machines, the so-called "security seals" presented no deterrent to hackers, and other violations. Although the judge appeared convinced that my allegations were well-founded, he did not require the ROV to obey the law or penalize him in any way, and merely suggested that he consider abiding by the laws in the future.

I had been appointed as an official election observer by the San Diego County Green Party and, in what the judge said appeared to be retaliation for my having taken him to court, Mr. Haas had me removed as an observer on the basis that I was not an engineer or computer expert, although the Democratic Party observers were not either, and he did not remove them. To do this, Mr. Haas personally phoned the then co-chair of the S. D. Country Greens, and spent a long time on the phone explaining why I could not be an observer. When the election came, however, Mr. Haas had apparently forgotten all about the observers and did not bother to notify them when the bulk of the votes were counted, so the only people present were Haas, his staff, and the Diebold technician.

Mr. Haas has now been promoted to head S.D. elections, the new Registrar is a former Diebold salesperson, and the Assistant ROV is Michael Vu, two of whose elections officials are in jail for violations of election laws involving rigging the precincts for recounts, and Vu stated publicly that he believes that they did "nothing wrong."

San Diego elected Councilmember Donna Frye to be mayor, but the previous ROV threw out over 5,000 votes (the notorious bubble-ballot scandal), and the next two elections were apparently rigged, the first one being where Jim March was arrested for demanding the right to watch the GEMS screen, and the second where no observers were notified when the bulk of the votes were counted. In the two precincts downstairs from me, the tapes showed Donna winning two to one and three to one, but the official results said that Donna lost.

Because I believe that San Diego elections have been rigged, I donated money to and supported the CA50 lawsuit which was recently dismissed by the CA Supreme Court. We were never allowed to see any proof that Brian Bilbray had been elected, and he was sworn into Congress while more than 68,000 votes remained uncounted.

An electronic vote count is a secret vote count, as no human can observe in real time what goes on inside a computer. I concur with the comments below, which were written by San Diego resident and voting activist Bruce Sims:

!the 'task force' McPherson empaneled in 2006 (that found that the 'Hursti Hack' was reproducible

07/30/2007

(AND AGAIN VERIFIED BY THE 'RED TEAM')) gave 'mitigating actions' to be taken for the Diebold systems.

The very first recommendation from that 'task force' gave was to NEVER allow the machines to be in the possession of a sole individual.

McPherson deleted that recommendation from his procedures -surely because of pressure from election officials- and thus was born the 'sleepover' issue from a 'news' standpoint.

Add to that (from the report) "The results presented in this study should be seen as a "lower bound"; all team members felt that they lacked sufficient time to conduct a thorough examination, and consequently may have missed other serious vulnerabilities."

SHOULD result in the machines being de-certified.
If they are not,well.....

The following points from the Diebold report are particularly significant:

GEMS Server Vulnerabilities

"Primarily, these vulnerabilities existed because the Windows 2000 server (configured by the Diebold technicians) was not properly patched. After noting these vulnerabilities, the Red Team was able to download an exploit from a free public repository of well-known and documented exploits. This exploit gave the Red Team access of a Windows Administrator on the GEMS server."

This -the access of a Windows Administrator- is especially notable because of what the audit log from the June 2006 election indicates. If the 'Connection Everett ' was not to Diebold's Everett, WA location -as the ROV claims- but reflects a ROV employee named Everett Giles -as the ROV claims- he had Windows Administrator capabilities on the GEMS server.

From the Diebold report:

"GEMS Databases

The Red Team used Windows Administrator access on the GEMS server to manipulate and corrupt GEMS databases. These actions could result in manipulated vote totals or in the inability to read previously-generated ballot definitions if no valid database backups were available (whether because the backups were not made or because the backups had also been corrupted)."

"GEMS Audit Logs

The Red Team found methods for executing actions from within the GEMS server that could not be tracked by the GEMS audit logs, allowing malicious GEMS users to conceal actions they had taken while logged in."

(As an aside, I just did another comparison between what was initially provided to me as the GEMS audit log back in June 2006 and what has just been provided me this month (after Seiler's statement about what was being provided me was a 'copied,edited,etc. version, not the original'); what was recently provided to me has had the 'connection Everett' and some other transactions time stamped at the same time deleted from the log; the logs ARE the same size but this latest version given to me has obviously been manipulated.)

Now this is the same election that gave rise to the Busby/Bilbray lawsuit(s) and also ,perhaps, is the reason why the 'pushback' relative to 'other documents' demanded by Gail Jacobson was denied.

"TSx: Physical Security

The Red Team was able to violate the physical security OF EVERY ASPECT of the TSx unit, using only tools that could be found in a typical office. This guaranteed the access necessary to execute physical and electronic attacks."

Also, please keep in mind that the ROV does NO background checking on poll workers so a political party operative could be someone acting as a 'poll worker' who had the machine(s) provided them prior to an election.

What happened in Volusia County, Florida in 2000, and Cuyahoga County Ohio in 2004, is now about to happen in San Diego County, California in 2008. The criminals are running the election bureaucracy and there is no possible oversight. Because the DLC wants Bush and Cheney to be pardoned by the incoming Democratic President (in keeping with the precedent maintained by Bill Clinton with the Iran-Contra felons), and wants the war to continue, they will not allow honest elections or honest candidates.

Many election reform activists told me that they voted for Debra Bowen because they believed that Bowen would decertify the uncertifiable and the previously decertified voting machines. I told them that I did not believe that the Democratic Party would allow Bowen to do so, and that even if the machines were decertified, the SOS would issue waivers to all elections officials who asked for them so that the election could be rigged.

I would like to be proven wrong. I'm 67 years old and have rarely been wrong about anything because I have a tendency not to go on record without first doing a lot of research and giving matters a lot of thought.

Respectfully,

Mark E. Smith

From: Valerie Sanfilippo
Sent: Monday, July 30, 2007 1:52 PM
To: Voting Systems
Subject: Vote Computer Fraud 2000-2007

My vote has been cheated by voting computer companies for the past 7 years, making America a dictatorship. Please see details of vote fraud below. We have proof by virtue of exit polls, and they have no proof they won. This affects my mayor, governor, president and Congress, all stolen from me. Resulting in my brother almost being murdered at 9-11, my job being deleted by tax cuts, and my being disabled from polluted products. Thank you.

VOTES Cheated by neocons

11-06 US DOJ blocked 250,000 brown/black/blue voters with "wrong" ID
11-06 US Reps- exit poll 240 at 11 pm; tally 227 at 7 am; final 233.
11-06 Dems won Congress exit polls by 11%; tally gave win of 7%, 4% cheated
11-06 CA Gov Phil Angelides poll 47 to AS 40; tally 39-56
11-06 CA 145K Dems purged, 43% L.A. Dems purged; Riverside 30% paper uncounted
11-06 CA Rep Busby- polling 46, gained 11 pts; tally 40, exit poll +6 pt
11-06 CA Rep Roth - 75K Absentee uncounted
11-06 CT Sen Lamont - tallied 59, dropped to 43
11-06 FL Rep Jennings - polled 53%; 16% undervote, 18K uncounted, sent to GAO
11-06 FL Rep Clint Curtis - polled leading 45 + 11% Indep.
11-06 FL Reps Russell & Gonzalez protests dismissed by Dem Hse Admin Cte
11-06 GA Gov/Rep McKinney - Defeated after 6 terms/150 yrs Dem with paperless
11-06 LA Rep. Cox, protest dismissed by Dem Hse Admin Cte
11-06 NC Rep Kissell - 1500 paper ballots uncounted, lost by 329 votes
11-06 NM Rep Madrid - 3700 uncounted, lost by 0.4%
11-06 OH State Auditor Sykes polled +10, lost -1, 16% votes lost
11-06 OH Atty Gen Taylor polled ahead, 10% vote lost
11-06 OH Rep Schmidt - paper ballots uncounted
11-06 OH Rep Kilroy - thousands uncounted
11-06 OH Rep Wulsin - 19,000 ballots uncounted
11-06 SD Prop Repro Rights - polled 66%, tallied 10%
11-06 TN Sen Ford - lost by less than 3 percent
11-06 TX Rep Rodriguez -
11-06 Nicaragua - Ortega wins; aid threatened, intimidation/war threat
10-06 13 States suing HAVA e-vote/Diebold:
AK, AZ, CA, CO, FL, IL, NJ, NM, NY, OH, PA, WV.
8-06 GA Rep. Donzella James sues paperless primary
8-06 CT Sen. Ned Lamont polls 54-41, tallies 52-48 primary
7-06 Mexico-Pres Obrador-4 M votes not counted, 10%, exit poll 36-35.
6-06 SD- Supervisor Barrera lost in Democrat-majority primary
6-06 Guerrero, Mexico - PDR polled 359K, tallied 182K, Choice Point data.
6-06 IA - Several Moderate Republican losses reversed by hand count.
6-06 AL- Gov. Siegelman prosecuted to prevent return to office.
6-06 CA - Rep Francine Busby polled/tallied 50, switched to 42.
4-06 NB/IN - Early voters have no paper ballots, not printed by ESS.

07/30/2007

11-05 MI Detroit City Elec Mgr is denied 5% recount by state.
 11-05 OH Absentee vote/campaign finance reform polled 59/61, lost 36/33.
 11-05 CA Mayor Frye polled 50, tallied 46, false polls 52-40, absentee 59-40, city majority Democratic.

8-05 OH Rep. Paul Hackett polled 50, tallied 48, "Breakdown," overvote.
 7-05 CA Mayor Donna Frye- Exit poll showed won by 50.2%, tallied 46.
 2-05 CA SOS Kevin Shelley prosecuted to prevent decertifying touchscreens.

11-04 OH Pres. John Kerry exit poll 51-48, accurate to 0.1%, 300K registrations cancelled, registered 10 M more voters, 5 M purged (reg/challenge/prov/absentee)
 won 11 addtl swing states: AR, AZ, CO, FL, IA, IN, NC, OH, OK, NM, NV.

11-04 IN - 46 machines withheld, long lines.

11-04 AZ - FBI subpoenaed ballots for fraud.

11-04 FL - Vote worker/whistleblower Ray Lemme murdered.

11-04 SD - Sen. Tom Daschle, majority leader, defeated in computer state.

11-04 CA Mayor Donna Frye won by write-ins, 3K disqualified, 2K filled/added.

3-04 CA Props State Budget/Fair Tax, Land Protection, Health Ins and Prison reform polled high 51, lost low, votes added later to defeat.

3-04 OH - Truvote voting systems president Athan Gibbs murdered on highway.

1-04 NH - Gov. Howard Dean frontrunner polled 35, lost 15 with Diebold.

10-03 CA - Gov. Gray Davis/Cruz Bustamente polled 51, lost 36.
 (7-05 Diebold convicted uncertified software in CA recall.)

11-02 (10 SENATORS) - MN Walter Mondale polled 47-39, lost 47-50;

11-02 MN Sen. Paul Wellstone crashed, FBI took black box.

11-02 MO Sen. Carnahan killed/ wife elected.

11-02 GA Sen. Max Cleland polled 49-44, lost 46-53.

11-02 South- 5 Dem Senators polled high, lost low, paperless states, votes added later.

11-02 NH - Sen. Jeanne Shaheen - White House jammed phones.

11-02, 11-04 - FL Reps. Fisher, Wexler, Jacobs, GA Rep Cynthia McKinney,

TX 7 US Reps + probably 30 US Reps won but were cheated by illegal redistricting, paperless votes.

11-02 (7 GOVERNORS) - AL Gov Al Siegleman, MS Gov Mosgrove,
 KY Gov, MD Gov, all polled high, tallied low, votes added later.

11-02 - FL Janet Reno - computer shift.

11-02 GA Gov Roy Barnes polled 48-39, lost 45-52.

11-00 FL - Pres. Al Gore won exit poll by 3%, 2 M votes purged nationwide,
 55K purged fraudulently in FL, Civil Svc Commission sued Jeb Bush, still pending before Supreme Court.

1986 NB Sen. Chuck Hagel owns ESS, wins by 86%, unheard of.

1981 and 1986 - Republicans caught caging voters

CRIMINAL VOTING COMPANIES - Advanced, Danaher, Dominion, Diebold, ESS, Guardian, Hart, Liberty, Microvote, Populex, Sequoia, Triad, Unilect.

HONEST VOTING COMPANIES - Avante (Democratic), Accupoll (bankrupt); TruVote (murdered); Smartmatic (Venezuela Leftist).

REFERENCES - GOVERNMENT OFFICIALS & ATTORNEYS:

Deforest Soaries, Federal Election Action Commission
 GAO (General Accounting Office) report says 2004 election cheated.
 Rep. John Conyers report (ranking Judiciary) says 2004 election cheated.
 Sen. Boxer & 20 Reps. protested 2004 electoral votes and election.
 Civil Service Commission sued over 2000 election, still pending in Sup. Ct.
 Rep. Rush Holt has introduced Voter Verified Paper Trail law in Congress.
 Republican Rep. Jim March is part of Black Box Voting to observe elections.
 Sen. John Kerry introduced bill Count Every Vote Act for registration at polls.
 David Jefferson, CA Secy State office, says scanners also vulnerable.
 Rep. Donna Frye started Election Task Force in San Diego City Council.
 Judges Susan Dlott, James Carr and Alernon Marbley opposed illegal challenges.

REFERENCES - COMPUTER ENGINEERS & UNIV PROFESSORS:

Cal Poly/MIT Voting Technology Project evaluates testing
 Computer Professionals for Social Responsibility
 Prof/Drs David Dill/Stanford, Verified Voting for paper trail laws
 Prof. Avi Rubin/Johns Hopkins, Prof. Rebecca Mercuri/Harvard and
 Prof. Harri Hursti of Finland, computer security experts
 Prof. David Wagner, UC Berkeley; Prof. Ed Felten, Princteon
 Pentagon computer scientists, NJ computer consultant Bruce Schneier
 Prof. Steve Freeman, statitician/Ohio State, book, "Was Pres Elec 04 Stolen?"
 Prof. Ron Baiman, Loyola Math, Natl Elec Data Archive
 Prof. Dan Tokaji, Ohio State Law; election scholar Dr. Allyson Washburn
 Tova Wang, Election expert, opposed misuse of provisional ballots
 Herbert Thompson, Ohio Computer Security expert; Dr. Dan Lopresti
 Prof. David Jones, Univ. Iowa; Dr. David Loo, Cal Poly Pomona;
 Prof. Michael Shamos, Carnegie Mellon; David Jefferson, Livermore Labs;
 Barbara Simons, IBS research; Dr. David Wagner, UC Berkeley
 Princeton Univ computer experts; voting expert Marian Schneider
 Bruce O'Dell, computer security; Victoria Lovegren, Case Western statistician

REFERENCES - JOURNALISTS & ACTIVISTS:

Bev Harris, Black Box Voting; Kim Alexander, Cal Voter
 John Gideon, Vote Trust; Lynn Landes, Ban Voting Machines
 Greg Palast, BBC; Lou Dobbs, CNN; Catherine Crier, Court TV;
 Wayne Madsen; Jrnl Robert Steinbeck, Miami Herald

Ms. Valerie Sanfilippo (Medical-Legal Transcriber)
 (SEIU, Sierra Club, Moveon)

Need a vacation? [Get great deals to amazing places on Yahoo! Travel.](#)

From: Ellen Theisen
Sent: Monday, July 30, 2007 9:14 AM
To: Voting Systems
Subject: Testimony for July 30 Hearing on TTBR

This is my public testimony for the hearing held today, July 30, 2007, regarding the results of the Top to Bottom Review.

In July of 2006, Secretary McPherson's staff conducted certification testing on the Vote-PAD, using the same consulting group he used to test the voting systems that failed so miserably during the Top to Bottom Review. The accessibility testing done on the Vote-PAD was significantly different from the testing done on any other system, before or since. In fact, no other system was tested for accessibility by the California Secretary of State - until now.

After the Vote-PAD testing last summer, we filed a claim against the Secretary's office, Bruce McPherson, Bruce McDannold, and Susan Lapsley for breach of contract, unequal treatment, abuse of discretion in the Secretary's authority to certify voting systems, and other violations.

It arrived in Secretary Bowen's office in February, and we were expecting her to treat our claim seriously and respectfully. **She did not.** She dismissed it in a two page report that failed to address even one of our concerns and appeared to have had much input from Mr. McDannold, one of those named in our claim.

Several counties had been eager to offer the Vote-PAD to their voters with disabilities. Instead they were forced to offer one of the systems recently shown to be inaccessible by Secretary Bowen's own testing.

But Secretary Bowen's testing was also significantly different from the testing conducted on the Vote-PAD. Secretary Bowen used qualified usability testers who designed and administered a professional, thoughtful test. **Secretary McPherson used unqualified testers who designed and administered an inappropriate test - according to testimony written by Noel Runyan, the lead accessibility investigator hired by Secretary Bowen.**

Would Vote-PAD have shown better than the Direct Recording Electronic (DRE) voting systems if the same testing had been applied? We believe so, but there is currently no proof since the testing was so different. (<http://www.vote-pad.us/CA-BOEClaimAttachment.asp>).

Here are a few comparisons of the testing processes and results:

Environment

DREs: A private cubicle was provided for each voter, with three video cameras filming from different angles. A test monitor was on hand to answer questions and give instructions before and after the free form voting.

Vote-PAD: Six tables were set up for voters, with one video camera on each voter. All tables were in the same open room, along with the observers, poll workers, test administrators, and visitors, milling around and talking. A test monitor sat across the table from the voter giving instructions from the script and occasionally engaging in casual conversation, banter, and even criticism of the voter.

Test Scripts

DRE Test Script:

Vote your choices and call out your selections as you make them.

If the review does not start automatically, select and start the review.

If possible, review to the first Senate race and modify your choice. If you have not made a choice in that race, make a choice and then change it.

Go back to the first House of Representatives race and change to write-in "Joe Smith".

VotePAD Test Script:

Begin voting.

Skip the third contest, and continue voting.

Vote the sixth contest as a write-in.

Return to the third contest and vote it.

Resume voting where you left off.

Vote the eighth contest as a write-in.

Vote the eleventh contest as a write-in.

Vote the sixteenth contest as a write-in.

Skip the 23rd and 24th contests, vote the 25th and 26th.

Return to the 23rd contest and vote it.

Resume voting where you left off.

Accuracy

DRE Error Rate: (voluntary write-ins and one scripted write-in) 6.6%

Vote-PAD Error Rate (with voluntary write-ins only): 5.5%
(with voluntary and four scripted write-ins): 10.3%

Positioning for Wheelchair Users

DREs: The VVSG requires a minimum of 30 inches of toe and knee clearance. No machine provided that clearance. This deficit posed a problem to almost every wheelchair-using voter in this study. [Note that the use of the DREs presented an accessibility obstacle for fully-sighted wheelchair users with full manual dexterity, who do not require assistance to mark a paper ballot. This means that the technology itself actually causes some accessibility problems for people who would otherwise be able to vote without assistance.]

Vote-PAD: People in wheelchairs moved up to the table with ease. If the table were too low, they could place the Vote-PAD on their lap. There were no problems accessing the ballot. Positioning for wheelchair users was not mentioned in the staff report.

Adjustability for Standing and Seated Use

DREs: "The systems we tested had little or no height adjustment capability; two were able to adjust the angle at which the screen was presented. This lack of adjustability posed a problem principally for voters who would prefer to sit, but also posed a problem for voters who wanted to stand but were limited in their ability to bend over to read the screen and/or VVPAT."

Vote-PAD: Fully adjustable to any height. This was not mentioned in the staff report.

Physical Controls

DREs: All physical controls pose some degree of difficulty for people with impaired dexterity. Controls are not ergonomic, were confusing, and non-intuitive. Some voters expressed confusion and difficulty using them.

Vote-PAD: The only controls are the pushbuttons on the tape player and the large button on the verification wand. No subjects had difficulty with them, not even the voter with no arms. Physical controls were not mentioned in the staff report.

Touch Screen Controls

DREs: The two touch screen systems pose a reach/range problem for voters with impaired range of motion, and reduced strength near the limits of their range.

Vote-PAD: Those with limited reach were able to adjust the Vote-PAD's position so they could reach all the selections. This convenience was not mentioned in the staff report.

Visual Display Concerns

DREs: Touch screen parallax decreased visibility of the screen for some voters. Screen refresh times were long and could confuse or frustrate voters. "Several voters in our testing found that some of the voting systems require so many repeated button presses or wheel movements that they were feeling exhausted and sore."

Vote-PAD: There are no similar concerns since voters mark a paper ballot.

Speech Rate for Audio

DREs: eSlate is not adjustable. Sequoia is minimally adjustable and does not comply with federal standards. Diebold complies. Sequoia and Diebold present noticeable "chipmunk" speech at faster speeds.

Vote-PAD: Speech rate is nearly double normal speech and can be slowed to less than normal speech rate. No "chipmunk" voice. Speech rate was not mentioned in the staff report.

Voter-Verified Paper Record

DREs: Visually impaired voters were unable to verify the paper record.

Vote-PAD: Visually-impaired voters could verify their selections with the verification wand. Those who used it to verify their own votes did so successfully, even occasionally using it to find their place on the ballot during the scripted voting.

Audio Interface in Complex Tasks

DREs: "Audio interface users found the more complex tasks such as reviewing, making changes, write-in voting, verifying, and casting the ballot very confusing. Although moving from race to race and making selections is somewhat intuitive, the acts of reviewing, modifying, verifying, and casting are not.

Vote-PAD: More complex tasks are more difficult for blind voters using the Vote-PAD, though they are still intuitive. However, the staff did not distinguish between these complex tasks and the simpler task of "moving from race to race and making selections." Thus the standard script called for 10 separate instances of moving from one place on the ballot to another and finding the corresponding place in the audio instructions.

Exhaustion

DREs: "if the voter got too frustrated with the voting task and decided to skip voting on the later portion of the ballot, those undervoted races were not considered to be errors for the accuracy score. Actually, when the voter skipped the final races, that was considered to be the voting system's failure, not a user failure."

Vote-PAD: Only two voters didn't complete the ballot. Both were developmentally disabled. One was a blind man whom the monitor described as falling asleep during the test.

Write-Ins

DREs: Write-ins required many keystrokes for "Joe Smith". 103 keystrokes for the eSlate, 32 for the Diebold, 130 for the Edge. Write-ins were challenging and tedious for most of the voters.

Vote-PAD: Write-ins were difficult for visually-impaired voters, not for others. Two of the eleven pages of the staff's testing results were devoted to discussing the difficulties of write-ins for visually-impaired voters.

Privacy

DREs: "Eavesdropping on the visual display" is a potential problem, especially for those who increase the text size on the screen.

Vote-PAD: The same privacy can be provided as is provided to any voter marking a paper ballot.

Reliability Concerns

DREs: Eight different machine malfunctions occurred, each one multiple times, to interfere with the voter's ability to continue voting.

Vote-PAD: There were no equipment malfunctions. Reliability concerns were not mentioned in the staff report.

Security of the Vote

DREs: Red teams showed that these machines provide no assurance that votes were recorded as cast.

Vote-PAD: Since all voters hand-mark their ballots, votes are always recorded as cast.

Secretary Bowen has now shown that no "accessible" voting system in use in California complies with the law, and it is imperative to find truly accessible systems that can be offered legally in the state. Vote-PAD could be of assistance.

We ask again that the Secretary right the wrong committed by her predecessor and, at the state's expense, test the Vote-PAD using the same test protocol used for the other systems. A fair test is all we have ever asked for.

Ellen Theisen
President, Vote-PAD Inc.

From: AHoiberg _
Sent: Monday, July 30, 2007 9:01 AM
To: Voting Systems
Subject: Support for paper balloting!

Dear Secretary Bowen:

On behalf of the members of the Women's Equity Council of the United Nations Association, I urge you to support the use of paper balloting and to reject the infamous machines.

During the past ten years, I have served as an election observer and supervisor in emerging countries. At all of these elections, paper ballots were used, which we counted at the close of the polling station. Of greatest importance was the fact that at the end of the counting session all of us were confident that there was no fraud--and we enjoyed being a significant part of the democratic system. We all knew that every ballot had been counted and verified; we felt very good about the purity of our work.

Please give paper balloting back to the people!

Sincerely yours,
Anne Hoiberg
Director, Women's Equity Council, UNA of San Diego

Get a sneak peek of the all-new AOL.com.

07/30/2007

From: palmerhouse
Sent: Monday, July 30, 2007 9:20 AM
To: Voting Systems
Subject: System Intergrity

Dear Secretary Bowen:

I was concerned enough about this that I volunteered several years ago and became an election judge. I'm a CPA and I have experience in investigative auditing in the brokerage industry, and I wanted to help.

Since then, I've seen a very partisan Secretary of State fire his own commission and chain the hearing doors shut, then certify electronic systems without resolving serious questions about the system.

Meanwhile, Neil Kelly, our new Orange County Registrar of Voters, gave the names of signers of a petition to recall a local school board to the chief executive of the school district. The school district used the list as a black list for retaliation. Litigation now surrounds that matter.

Voters at my precinct make comments about all this, and I feel like a fool. My precinct workers, all with many years of experience are threatening to quit.

I don't have access to the vote counting process above my precinct post, so I can't help. Those duties are assigned to county bureaucrats who are supervised by partisan political operators.

The system has the appearance of being out of control, and my voters know it. I'm not sure I can stand the embarrassment of being a part of it much longer.

Robert N. Palmer, CPA
Dana Point, CA

07/30/2007

From: Sheri Myers
Sent: Tuesday, July 31, 2007 8:02 AM
To: Voting Systems
Subject: Inkavote Plus Breakdown in Los Angeles county 06

Hello,

We have compiled first hand reports from three teams of camera crews, 51 poll workers, and 200 EIRS reports that indicate

a 32% failure rate in the new PBR machines touted by Conny McCormack for Los Angeles County.

I have the reports and will send a copy at your request.

Thank you.

Sheri Myers

Los Angeles Election Protection Task Force

07/31/2007

From: winogradcoach
Sent: Tuesday, July 31, 2007 6:51 AM
To: Voting Systems
Subject: Progressive Democrats of America Support SOS Bowen's Audit & Findings -- Urge Compliance

Dear Honorable Secretary of State Bowen:

As President of Progressive Democrats of Los Angeles, a chapter of the 80,000-strong national Progressive Democrats of America, I write in support of your valiant efforts to audit the state's electronic voting machinery and urge you to continue your audit to encompass all electronic software and equipment in use in LA County.

Our members have learned that one of our voting vendors, ES & S, was late in submitting its source code, thus avoiding an audit. We hope that, given time, this company's products will also be fully reviewed and tested, and that your office will additionally inspect and scrutinize the electronic software used to scan our Inkavote ballots.

Please note that Progressive Democrats of Los Angeles will be delivering petitions to LA County Supervisors this week, urging our supervisors to fully support your audit, findings, and orders.

Though we understand the enormity of the job facing county registrars, we cannot excuse any registrar recorder who jeopardizes the safety, security, and accuracy of our vote in the name of expediency.

Thank you for conducting this audit, knowing full well that when money and corporate power are involved, you will be challenged at every turn. You and your outstanding staff have our support.

Sincerely,

Marcy Winograd
President, Progressive Democrats of Los Angeles
Executive Board Member, California Democratic Party
Board Member, Palisades Democratic Club

AOL now offers free email to everyone. Find out more about what's free from AOL at AOL.com.

07/31/2007

From: Emily Levy
Sent: Tuesday, July 31, 2007 8:09 AM
To: Voting Systems
Subject: Testimony from yesterday's hearing: Secretary Bowen, please read

July 30, 2007

Secretary Bowen,

Thank you for the strength and courage that has brought you to this moment.

I fear that, even after months of testing, there's still an elephant in the room that has not been tackled. Even if you and your staff could plug every hole in physical and software security and the voting systems were made fully compliant with the accessibility requirements of HAVA, it would still not be safe to use these systems. Why not? Because even if they were absolutely protected from hacking, the systems and therefore our elections could still be rigged. There is no way to provide an absolute safeguard against electronic voting systems being delivered to the counties and presented to the voters already compromised. For this reason alone, these systems and others like them must never again be used in our elections.

The irresponsibility and lack of ethics of the vendors has been amply shown:

The have misrepresented their products.

They have installed uncertified software.

They have cut corners in developing the security of their systems.

Clearly they are not guided by ethics or commitment to the public good. Clearly they have other priorities.

Is it so unbelievable, then, that they might rig an election?

We shouldn't be thinking of how we can make these systems work, we should be thinking of how we can make our elections work.

We have a crisis in voter confidence that can only be solved by creating a true basis for voter confidence. Only transparency and public involvement can save our democracy now.

Perhaps more than any other human being in this country, You, Secretary Bowen, are in a position to take bold, decisive action that will reverberate around this nation and turn it in its tracks. The next step is to decertify these machines, to send these vendors packing and tell them not to come back. Not with another promise, not with another model, and not with another roll of toilet paper.

The people of California, the people of the United States, the people of the world are depending on you.

Emily Levy

07/31/2007

Macias, Ryan

From: John J. Abbene
Sent: Tuesday, July 31, 2007 10:24 AM
To: Voting Systems
Subject: Voting Machines

Dear Secretary Bowen:

I was a touchscreen inspector in San Diego County for the November 2006 election. San Diego County uses the Diebold machines and I was responsible for four machines for the precinct I worked. I thought you would like to know that the integrity of the machines relies exclusively on the integrity of the touchscreen inspector and other poll workers. I had the machines in my possession for over 2 weeks prior to the election. Although other precinct inspectors are supposed to check the machines when they are set up and taken down, due to their other responsibilities, no one else checked whether the seals were intact when the machines were set up and whether all precautions were taken when the election results and memory cards were removed from the machine. I would have been relatively easy to substitute a memory card that had been tampered with. In addition to the other problems with the machines, the integrity of the machines relies solely on the integrity of the poll worker. They should not be recertified.

John J. Abbene

July 29, 2007

Honorable Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, CA 95814

Dear Ms. Bowen,

Re: Lack of Security with Voting Machines

A major article in yesterday's San Francisco Chronicle reported on the failure of most, if not all, of a large number of tested voting machines to be safe from the efforts of hackers to manipulate the counting of votes. Using such machines puts the value of one's vote and the honesty of our elections in very serious jeopardy.

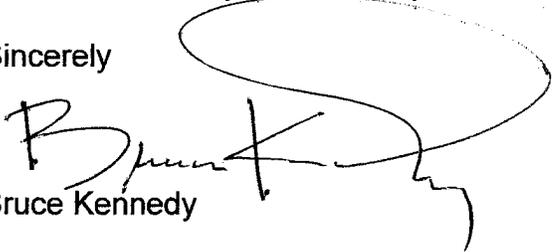
It should be noted that the article said nothing about another substantial risk of using these machines, their potential manipulation by the county officials and employees responsible for the voting process. These people could secretly adjust the machines to give false results and no one would be the wiser.

Our democracy depends on the accuracy, perceived as well as actual, of the vote counting. Every effort must be made to prevent its compromise.

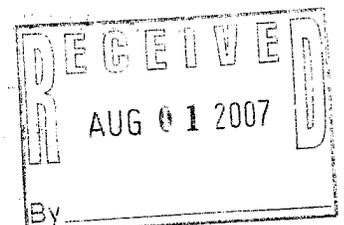
I urge you to ask the Legislature to pass laws making illegal in California the use of any electronic voting machines at any level of government until:

- Such machines have been developed to the point that they cannot be hacked into, and that this level of security is continually reviewed and tested by your office using outside experts; and
- There are procedures enacted in law by which the county officials and employees responsible for these machines are subject to strict oversight so that they cannot compromise the vote from within the system.

Sincerely


Bruce Kennedy

Copies: Governor Arnold Schwarzenegger
State Senator Mike Machado
Assemblymembers Dave Jones, Roger Niello
Chairman and Board, Sacramento County Supervisors



JULY 29, 2007

State of California
Secretary of State
1500 11th Street
Sacramento, CA 95814
ATTN: Ms. Debra Bowen

Dear Ms. Bowen,

I have learned that U.C. Davis was successful in hacking into all electronic voting machines recently. In light of this disclosure (which I suspected from the outset of these machines), please uphold your promise to DECERTIFY ALL ELECTRONIC VOTING MACHINES IMMEDIATELY.

California voters will be much happier to vote on a paper ballot or punchcard system (as we had here in Yuba county) with ballots read by scanners or punchcard readers.

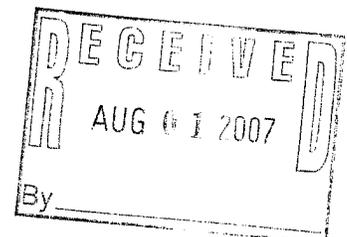
The only way that California should allow electronic voting machines is if:

1. Machine software is not proprietary,
2. Machines should be purchased outright,
3. Machines are programmed by state, county, and/or city officials,
4. Machines produce a printed ballot that would be placed by the voter into ballot boxes at the voting station.

PLEASE DECERTIFY ALL ELECTRONIC VOTING SYSTEMS
NOW !!!!

Sincerely,

William A. Liechti



MISCHELLE TOWNSEND

July 31, 2007

Honorable Debra Bowen
Secretary of State
1500 - 11th Street - Suite 600
Sacramento, California 95814

Subject: SOS' DECISION ON CALIFORNIA'S VOTING SYSTEMS

Dear Secretary Bowen:

Knowing your panel would have a full day of speakers who share your concerns about the future use of voting systems in California, I appreciate the opportunity you have provided by inviting both oral and written comments prior to making your decision as a result of the reports published last Friday by the UC Berkeley-led review teams.

As I listened remotely to the thoughtful testimony provided throughout the day, I was impressed by the common denominator of sustained success: the lessons learned through extensive experience in the conduct of official elections. Clearly, your own experience as an attorney prepared you well for your legislative role as you commenced your deliberative review of the historical evolution of the general laws which govern the State of California and its subdivisions, the 58 counties; and only then worked to introduce change where necessary. Throughout that experience, I'm confident you quickly learned that incremental, well-planned changes based upon the combined experience of those involved in a particular issue generally proved to be successful.

Recognizing that often repeated reality, I was reminded of someone in your own office who had 27 years experience in the SOS' Elections Division and, regrettably, is no longer with us; but he was someone who wrote a "History of Voting Systems in California" which was published just a couple of months prior to our DRE pilot election in Riverside County in August 1999. You may have read it; but if not, it is an extremely informative discussion of the evolution and use of voting systems historically both in America and the State of California.

Key Facts Raised by Ed Arnold's History:

- With hand-counted paper ballots, people can't count accurately; and based on California's largest county's experience (Los Angeles), it was reported then that there was an error rate of approximately 5% in the vote count in each precinct with hand-counted paper ballots;
- He quoted Roy Saltman in a publication on computerized vote tallying for the National Bureau of Standards that multiple vulnerabilities exist in manual tallying

Honorable Debra Bowen
July 31, 2007

Page 2

of paper ballots including inaccurate counting, ballot frauds, and malicious invalidation all of which contributed to the acceptance of vote counting machines;

- On Page 31 of Mr. Arnold's report, he cites an extremely relevant example of the inadvertent errors people make with paper-based systems (overvoting); i.e. ***"An example is the 1984 general election in Ohio. About 137,000 among 4.7 million voters did not cast valid ballots for President, primarily because of overvote, according to the Ohio's Secretary of State."*** With California's growth, particularly in its urban counties, and the fact that DRE voting equipment precludes overvoting, more votes can be counted. Irrespective of the candidate or the high profile of office, this benefit alone can make the difference in who is elected to office.
- From 1897 until 1984, there was a California State Commission on Voting Machines created. During those decades, many voting systems were approved and used throughout the State without the benefit of federal standards or State testing and certification as has been the case in recent years. Yet, Californians accepted the choices made by their local Boards of Supervisors and demonstrated confidence in their voting systems.
- Prior to the November 2000 election in Florida, Ed Arnold included in his study a comparative analysis of the strengths and weaknesses of California's various voting systems including his concerns with "hanging chads" before the term became infamous in the popular culture.
- For more than 50 years, lever machines were the predominant voting machines used in America which had no audit trail whatsoever.
- Perhaps what is reflected most in this document, borne of 27 years of experience, is that the Secretary of State recognized counties' needs were varied because of geography, demographics and other factors that contributed to their respective choices in the acquisition of a voting system that best met their needs. As long as they were approved for purchase by the State, the SOS supported the counties' local decision-making and continued to improve and expand availability of those choices as technology became available in a consistently collaborative environment.

The 21st Century Watershed:

With the 2000 Presidential election and the rapidly-escalating use of the Internet, the political environment quickly turned disappointment in election results into a dangerous blame game in which historically-trusted election officials, pollworkers and voting equipment became the targets of personal crusades for political change without any evidence of fraud, manipulation or inaccurate election results with the new voting technology. "What if" scenarios started to drive public policy away from progress and

Honorable Debra Bowen
July 31, 2007

Page 3

the benefits of technology over the problems associated with paper without any recognition or at least admission in the debate that paper ballots had been tallied by computerized systems for decades, some of which had neither been federally or state certified.

Yet, the decision has already been made by the Secretary of State that these "grandfathered" paper-based systems which have not undergone the rigors of testing nor certification by either the federal or California government will be allowed for use in the 2008 state/federal elections. It would then be more prudent to continue use of the rigorously tested and federally/state-certified DRE systems which are proven to preclude overvotes and, therefore, will count more valid votes because voter intent is clear. We also have an increasingly-aging population in California whose seniors appreciate the larger font type on DRE touchscreens with California's lengthy ballots, whereas on paper, the font size is more difficult to read because of the number of contests which have to be formatted into a smaller size on paper. Or the audio ballots which are not only used by those who are blind or visually impaired, but also by those who have literacy issues.

Voter Confidence:

Ed Arnold concludes his study on p. 45 by pointing out that:

"Given the history of voting systems in California, we as California citizens ought to cherish the precious opportunity to vote, with whatever forms of voting and vote-counting devices."

Words of wisdom, borne of extensive elections experience.

Voter confidence has been expressed in multiple ways since the Secretary of State's office certified and approved for purchase DRE voting systems:

- In March 2002, Californians approved an unprecedented \$200 million in taxpayer funds to purchase new voting technology. The electorate's support far surpasses the activists' voices who do not represent the majority of voters.
- Every county which has implemented a DRE system has accumulated multiple voter surveys which consistently reflect more than 90% approval ratings whether in small, suburban or urban counties.
- Wherever DRE's have been employed, pollworkers (many of whom are seniors) have enthusiastically welcomed their use because it has significantly eased their burden of handling the time-consuming complexities of paper, particularly recognizing the length of California's ballots, multiple languages in many counties and the difficulties encountered by voters with special needs.

SUMMARY:

The SOS' review has demonstrated your commitment to continuous improvement in the use of California's certified voting systems. DRE voting technology, in particular, has positioned this

Honorable Secretary Bowen
July 31, 2007

Page 4

State to address the rapidly-growing populations in our urban counties with benefits in improved accuracy, reliability and accessibility that surpass the limitations of paper-based systems.

The history and evolution of California's voting systems, as documented, in part, by Ed Arnold and the Secretary of State's office demonstrated that:

- California's diversity, size and range of our counties' needs have benefited from the competition among voting manufacturers, availability of a variety of voting solutions and expanding flexibility for any Californian to choose to vote either a paper ballot or electronically at the polls, recognizing that even those paper ballots will be tallied electronically.
- California's rigorous testing, certification and best election practices have served to lead the nation (e.g. provisional voting, no-excuse absentee voting, implementation of DRE touchscreens, etc.). Building upon many successful elections with this voting technology and in collaboration with experienced California election officials, these voting systems will continue to be strengthened through evolving administrative procedures and security protocols which will honor the voters' wishes with their passage of Proposition 41 and years of effort by the Voting Modernization Board to distribute those funds for these systems in good faith.
- There is far more redundancy in audit trails with the DRE voting systems (on the memory in each unit, the cartridges and the VVPAT) than can be offered with the traditional paper-based system which far exceeds what had previously been available historically in this State or the Nation. Yet, even without any audit trail for decades (e.g. lever machines), the electorate did not express widespread dissatisfaction with their voting systems; nor does the vast majority of voters today.
- If non federally or state-certified paper systems will be allowed for use in the 2008 federal/state elections, it would be disparate treatment not to permit continued use of more accurate and accessible DRE voting systems that have been both federally and California certified for use.
- There has not been a scintilla of evidence in which fraud or manipulation has occurred with any DRE voting system in the more than 25 years they have been used in the Nation or over the past eight years in California. This fact has been further validated in multiple audits, recounts, the SOS' parallel testing and adjudicated court cases challenging their continued use.
- California voters overwhelmingly expressed their support for new voting technology with the passage of Proposition 41. The Voting Modernization Board, elected Boards of Supervisors and the Secretary of State have honored the expressed preference of the people by utilizing proceeds of this \$200 million in the deployment of these more accurate voting systems. California issued bonds to fund this voter-approved proposition which have not yet been amortized; and there is no factual basis in these DRE systems' sustained performance to negate the will of California's electorate. Nor to negate expenditure of HAVA federal funding which was approved through bipartisan support of the United States Congress for improved voting technology which will continue to be used throughout the Nation in the 2008 elections.

Honorable Debra Bowen
July 31, 2007

Page 5

CONCLUSION:

Every constitutional officer in California assumes a huge leadership responsibility, as does the Secretary of State with her multi-faceted duties. With that oath of office is wisdom borne of collective experience which is shared with the elected representatives in each of the 58 counties that inherently includes a fiduciary responsibility.

The Secretary of State's Office has a longstanding tradition of working collaboratively with California's election officials and their respective Boards of Supervisors in the choice of voting systems to conduct municipal, state and federal elections. All of whom share a mutual goal in conducting them fairly, accurately and promoting voter confidence and participation. The Secretary of State is at a critical crossroads with this decision.

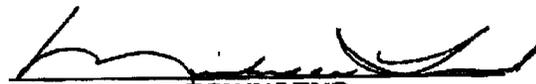
RECOMMENDATION:

Based upon facts, (rather than theoretical "what-if" scenarios), the extensive history in the use of voting systems in California, and the cumulative experience of its election officials, it is respectfully recommended that California's certified DRE voting systems continue to be used for these imminent elections; and that on-going opportunities be provided between the SOS' staff and the counties to incrementally improve procedures and security protocols, as well as, encourage further research and development in using technology to address the exponentially increasing growth demands in California.

Equally compelling priorities of pollworker recruitment, training, voter education and participation, as well as, preparing for implementation of a new statewide voter registration database can then be addressed - without incurring potential chaos by hastily mandating major changes and their inevitable unintended consequences so close to the November 2007 and multiple 2008 elections.

Thank you for your willingness to listen and your consideration of the concerns of our 58 counties, their election officials and elected representatives who pledge their willingness to work with you on these critical issues.

Respectfully submitted,



MISCHELLE TOWNSEND
Registrar of Voters (Retired)
Riverside County

From: Sharon B.Ross
Sent: Tuesday, July 31, 2007 11:27 PM
To: Voting Systems
Subject: Please de-certify vote machines & restore our election integrity

Dear Secretary of State Debra Bowen and staff,

Please de-certify the voting machines used in California, and require paper ballots in time for the February 2008 primary. 'The shocking results obtained by the hacking and security challenges conducted by US Davis and UC Santa Barbara showed us clearly that our elections are in severe danger. By clearly and decisively responding to the findings of your recent top to bottom review on the vulnerability of these voting machines. your leadership will initiate the restoration of election integrity in our state and the return to re-countable paper ballots.

ROV procedures and protocol are simply insufficient to combat the vast vulnerabilities of these suspect voting machines, and they will never be sufficient to ensure the security needed for voting. While your insisting on this basic voting protection may anger the county registrars, the voters will appreciate that you are serious about election integrity. I found their cozy relationships with vendors more than disturbing, and wish that their loyalty would be with the voters, not the vendors. The registrar from Yolo County has won my respect.

Ideally, Diebold, Hart, Sesquioia and the rest should be forced to take their machines back and absorb the financial loss, due to their smokescreen sales of faulty software, unproven firmware amidst the widespread public fleecing that urged their purchase. Short of that, please de-certify these machines.

I greatly admire and appreciate your courage and national leadership at this crucial time in our state and our nation.

Thank you for your time and consideration,

Kelsey Ramage

Please note that I am writing this letter from the computer and email address of my friend Sharon Ross in Paradise California.

From: Stuart Schy '
Sent: Tuesday, July 31, 2007 3:43 PM
To: Voting Systems
Subject: Additional Comments



BowenHearing.rtf

I was one of the speakers (public) at the hearing July 30. I took a different tack than most of the other speakers who strongly advocate getting rid of electronic counting.

All of the vendors, of course, were very much for the status quo. The speaker from Sequoia pointed out that many of the problems noted by your team would be solved if only Registrars would buy their new, improved, systems. One e-mail comment I received from Jackie Riskin of the California Election Protection Network (CEPN) asked "If you were taking an expensive medication and found that it was making you sicker, would you buy more?" Nearly all were careful to point out that your tests were done in a "laboratory environment" and therefore didn't apply to the real world. They said that, in the "real world" safeguard and procedures were in place to prevent outsider hacking. No one asked about hacking (software updating) by the vendors. Even assuming all election personnel are above reproach, the total reliance placed on the vendors for maintaining their electronic systems makes the whole system vulnerable to partisan machinations.

As a member of the L&A panel in my county I am quite aware of the problems of the election staff in carrying out the complex operations of a typical overstuffed California election.

My first vote was in 1948 in Los Angeles County. The population was about 4,000,000. We didn't have computers other than ENIAC and a couple of others and they weren't used for vote counting. We did fine with hand counted paper ballots.

My recommendations for the panel to consider are:

1. De-certify all systems which have been proven hackable and non-accessible per HAVA requirements.
2. Mandate hand-counted paper ballots for the State.
3. As an interim step, allow present electronic systems to be used ONLY by people with disabilities - all others to be hand counted paper ballots.
4. In the future, investigate the use of non-conditional counting and tabulating equipment. Those "If-Then-Else" loops allow all sorts of mischief.
5. Also investigate non-electronic methods which can assist a person with a disability to prepare a PAPER ballot.
6. Forget about "paper trails" they are a semantic trap.

Thank you for your incredible hard work. There are a lot of us out here who appreciate it.

Stuart Schy

From: Lillian Laskin
Sent: Tuesday, July 31, 2007 3:48 PM
To: Voting Systems
Subject: Thanks!!

Dear Honorable Secretary of State Bowen:

As founding member and executive board member of the Democratic Club of Westside Progressives of Los Angeles, I write in support of your valiant efforts to audit the state's electronic voting machinery and urge you to continue your audit to encompass all electronic software and equipment in use in LA County.

We know that one of the voting vendors, ES & S, was late in submitting its source code, and avoided an audit. This company's products must also be fully reviewed and tested. We urge that your office additionally inspect and scrutinize the electronic software used to scan our Inkavote ballots.

We understand the enormity of the job facing county registrars, and we cannot excuse any registrar recorder who jeopardizes the safety, security, and accuracy of our vote in the name of expediency.

Thank you for conducting this audit, knowing full well that when money and corporate power are involved, you will be challenged at every turn. You and your outstanding staff have our support.

Sincerely,

Lillian Laskin

From: Mark Carlson
Sent: Tuesday, July 31, 2007 4:00 PM
To: Voting Systems
Cc: Connie Soucy; Valerie Arita
Subject: Letter to Secretary of State Debra Bown, RE: Voting Machines

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 30, 2007

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

07/31/2007

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,

**Mark Carlson, CTM
Assistive Technology Advocate
Access to Independence**

From: Jan Shriner _
Sent: Tuesday, July 31, 2007 4:46 PM
To: Voting Systems
Subject: Voting Machines

I have been involved in several political campaigns as a volunteer and have spent some time at polling places working for the "get out the vote" portion of the campaigns. One in particular made me realize that some very strange circumstances could easily be set up from the inside, that was the City of Marina Mayoral contest of 2004.

Based on these previous experiences and observations, I have completely switched to permanent absentee ballot so that I can ensure my vote by paper. I trust paper ballots, particularly if either count or re-count are done by hand.

I do not trust the electronic machines or the computers that suddenly go down in the night, please review the election of Monterey County in November 2004. Monterey Herald reported computer glitches in the night.

It is already too easy to manipulate our democracy.

If your priority is to improve the integrity of our democratic system, please get rid of the computerized voting machines including the scanners.

Don't make it any easier to damage the process with some strategically placed insiders.

I trust most of the voters, but there are people who are working the polls that are sketchy, please review the behavior of Monterey County Elections Official Tony Anchundo around the election of November 2004. No recount was requested by a candidate who lost by 69 votes in a population of nearly 8000 voters because the candidate felt sympathy for Anchundo's reported grieving for his sister when it turns out in 2006 Anchundo was indicted for living it up in a hotel room with a girlfriend on a County credit card during November 2004 elections.

Please, protect democracy. Get rid of the electronic voting machines. Insiders are only human.

Janet Shriner

07/31/2007

Helen Bliven

July 27, 2007

Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, CA 95814

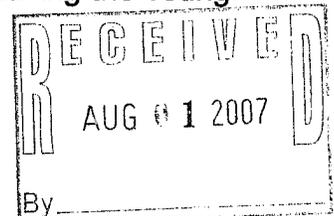
The Honorable Debra Bowen:

Re: Voting Machines & Saving Millions of Taxpayer Dollars

I have three years experience working in the Registrar's office including every election in Santa Clara County as a Field Inspector from the inception of the Sequoia voting machines, and one year serving as a Precinct Coordinator in Alameda County. My duties included election day field (polling place) support for 10-18 precincts each election.

I initially had a very open and positive attitude about the voting machines, but personal experience and observations have changed my opinions. Enumerated are the reasons:

1. Every election it is difficult to recruit poll workers. Most are retired folks and students. The voting machines require substantially more extra training. Many seniors find them too confusing. They do not want to spend the extra time or sessions attending training. Therefore, they refuse to serve as poll workers.
2. Sequoia's Edge machines weigh 40+ pounds each. Many precincts are staffed with seniors only. The voting machines are too heavy for many of them and others with physical restrictions, even with two people sharing the work. Back problems and weight lifting limitations precluded a substantial number from participating in polling place set-up and tear-down. This also could adversely affect curbside voting under HAVA (Help America Vote Act).
3. It is also difficult to secure polling places according to the guidelines. Many venues will no longer serve as polling places because either they can't or won't be responsible for the security of the voting machines from the time of delivery to the time of pick-up. Some places are now too small. My precincts typically experienced having the voting machines on the premises for two weeks.



4. Drayage costs. Drayage must be paid both directions to have the machines delivered and picked up. The poll star system allowed poll workers to pick up the voting machines and "pizza box" booths, thus eliminating additional election expense.

5. Unit cost. My understanding is the cost of each machine runs around \$5,000. The cost of the poll stars - maybe \$5?

6. VVPAT paper trails will add to election costs.

7. When the voting machine malfunctions, it takes high priced technicians to fix them. The poll stars can simply be replaced.

There are many safety issues.

A. Again weight for seniors and disabled or physically challenged folks becomes a problem.

B. Cords must be attached to both the voting machines and card activators for them to be used an entire day. These cords present ample opportunity for someone to trip. The dictates of the polling place set-up and electrical outlets frequently don't allow avoidance of walking over the cords. Even with tape and mats there is an uneven surface where it is easy to trip.

8. Storage of the voting machines and card activators takes considerably more space as it entails larger and more extensive equipment. Now add paper trail equipment.

9. Security and cost of same becomes another issue to consider. Specially built locked cages must be provided. There was no way someone could tamper with the poll stars that would "throw" an election.

10. Unprepared voters, who've not previously marked their sample ballots, tie up the machines and cause other voters to wait unnecessarily. This has happened many times when polling places get busy. With poll stars one could ask these voters to step away to finish the decision process and then resume voting. Once an activated card is in process the voter must finish before the machine is again available.

11. Voter confidence has been a problem from the start. The VVPAT paper trails, now being instituted, add yet another layer of complexity to a system that is already too difficult for many.

12. Santa Clara County never had a problem with its poll stars. After the Florida debacle employees tried to produce pregnant and hanging chads. They were unable to do so. The poll stars were cleaned and maintained. Whoever die cut the ballots did an outstanding job.

13. Problems with minor machine malfunctions were, I believe, much more prevalent than may have been reported. They did, however, many times negatively impact a

voting experience. These would include: activator card stuck in machine, cords not properly connected causing machines to go yellow/red line.

14. Although Sequoia's screens can be placed in a horizontal position, a substantial number of voters and poll workers were not aware of this, and the question of privacy arose. Voters felt poll workers or other voters walking by could see how they were voting. They felt their voting privacy was being compromised.

15. In one election the voting screens appeared in a different order than the races and measures appeared on the sample ballot. This caused no end of confusion for voters, poll workers and field support staff.

I'm a fan of technology, but I don't think elections should be a part of it yet. Sometimes it's better to keep things SIMPLE. Elections and the voting process should be such at this juncture. People KNOW how they vote a paper ballot. There is no question of tampering.

What if the public has to wait an extra hour or two to get the election results? It really won't hurt anybody.

There is a great deal at stake for both the voting public as well as jobs for those providing voting equipment and technical support. It is hoped this perspective from one with over 35 years practical election experience will provide valuable input in the decision making process.

Sincerely yours,



Helen Bliven

Enc.: Oakland Tribune article, *California ballots - paper or not?* dated December 7, 2006

THURSDAY, December 7, 2006

OP-ED

California ballots — paper or not?

DEBRA Bowen, California's next secretary of state, was accused during the recently ended campaign of hanging too closely with opponents of electronic voting who believe the boxes can be tampered with to rig the results of an election.

Bowen posted items about voting security on her own Web log. She ran an ad showing make-believe thieves stealing an electronic voting machine. Internet sites where "black-box" voting critics gather to exchange conspiracy theories buzzed about her candidacy.

Now, with her victory over incumbent Bruce McPherson secured (and undisputed, as far we know), Bowen will be California's chief elections officer in January and instantly become perhaps the nation's most prominent and influential skeptic of the technology. Or will she?

I spoke with Bowen as she was preparing to leave the state Senate for a month's hiatus from government before she is sworn in as secretary of state. She said she has not made any decisions yet about how to approach the issue of electronic voting. But she did say she doesn't intend to push to return California to a more paper-oriented system, or to encourage the universal use of optical scan technology, which allows voters to make their choices on paper ballots that are then counted by computers.

Instead, Bowen said she will likely focus on making the new



Daniel WEINTRAUB

voting technology more user-friendly.

"It's not just a matter of the hacking and all of the things people are concerned about," she said. "There have been a lot of usability issues. . . . There are a variety of practical problems that deserve some attention."

She is concerned about the training of poll workers, many of whom are retirees with little familiarity with computers. And she is troubled by what happens when the electronic systems fail.

"We have a lot of places where the vendors will say it's not a machine problem, it's a user problem," Bowen said. "But machines don't run themselves. So problems with set-up or use or bugs have to be considered problems with the machines."

Bowen, however, said she does not believe that electronic voting can be scrapped because it has brought important advances that need to be preserved. Among them: access for the disabled, for whom touch-screen voting is usually far easier, and early voting in public places, which in most

counties is not viable without touch-screen voting because there are so many different versions of the local ballot, depending on a voter's exact address and precinct.

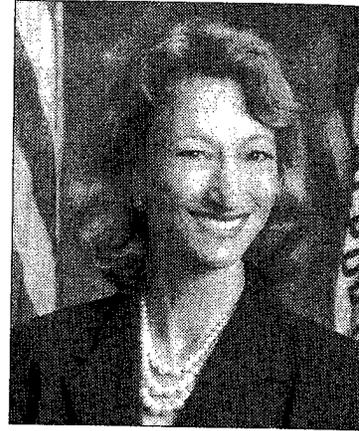
Despite Bowen's alliance with the black-box voting skeptics, then, she may one day become an evangelist for California's voting laws and regulations because the state is one of relatively few that already require a voter-verifiable paper trail and random audits of the results.

As it happened, we spoke the same day that a national standards board released a draft report concluding that computer voting systems that do not include an independent paper trail cannot be made secure. If any security audit relies on information that exists only in the guts of the machine, the report said, there is no way to know that the entire system is not faulty.

The losing side in any election is thus prone to question the result.

We're seeing just that kind of situation unfolding in Sarasota County, Fla., where 18,000 voters failed to vote in the congressional race even though many of them voted in races above and below it on their electronic ballot. The machines used in Sarasota County warned voters if they skipped a particular race, they were provided no paper trail that can be used to verify the outcome.

Democrats are questioning the Republican victory, and some are even calling for Congress to seat the Democratic



DEBRA BOWEN, newly elected California secretary of state, will have to contend with voting machines.

candidate who lost the race on Election Day.

"If the balance of power in Congress were dependent on the outcome of that race, it would be front-page news every day," Bowen said.

California Sen. Dianne Feinstein, meanwhile, is introducing legislation that would require every state to use voting machines with a paper trail that can be viewed by the voter and checked later against the electronic results.

"It is crucial that there be an independent record that can be reviewed by election officials," Feinstein said.

It sounds as if Feinstein is talking about making California's systems a model for the nation. It will be interesting to see whether Bowen, once she takes office, supports or opposes that notion.

Daniel Weintraub writes for the Sacramento Bee.

From: Ty Meissner
Sent: Tuesday, July 31, 2007 5:32 PM
To: Secretary of State Bowen; Elections - El Dorado County; Voting Systems
Subject: Mapped: voter caging and US Attorney firings; voting machine vulnerabilities

Dear Secretary of State Bowen,

In the article below, Kim Grant addresses the correlation between US Attorney firings and vote suppression in the 2004 election. I find it particularly alarming that

"days before the election, state officials have learned that California's most widely used electronic voting machines feature a button in back that can allow someone to vote multiple times. Several computer scientists said Wednesday that the vulnerability found in all touch-screen machines sold by Oakland-based Sequoia Voting Systems was not especially great because using the yellow button for vote fraud would require reaching far behind the voting machine twice and triggering two beeps."

July 31, 2007

MAPPED: Voter Caging, US Attorneys

By Kim Grant

During November 2006, I created a map of voting irregularities reported from across the country. During the weeks before and after the election my small staff and I created [an incident-by-incident map of voter fraud](#), voter suppression, and cases that were taken to court in the weeks after the election. (Red map marker points represent cases that were being argued in court during the time period of October 20 - Nov. 20)

Last night, I created [a map of 7 of the 8 attorneys fired by President Bush](#).

I noticed a pattern: In the western states where the attorneys were dismissed, none of the election irregularities reported in the media were prosecuted.

Keep in mind that November 15-17th was the "call the Bush-leads and let them know these people are being fired" target date.

Also, after doing more research, I noticed that many of the attorneys fired were appointed by President Bush himself.

This is how I believe that the Bush Administration felt they could get away with what they'd done. The Bush Administration line that has been parroted to everyone is this, "They serve at the discretion of the President. If the President could hire them, then, the President has the power to fire them as well." The fact that all but one of the attorneys fired were appointed by Bush leads me to believe that this chain of events was premeditated, planned intricately, and executed with utmost disrespect for our Constitution.

The eVoting relationship

Take a closer look at [this map here](#). (For you Firefox users, this is the time to start opening links in new tabs.) This is a map of eVoting irregularities, machine malfunctions, and other related problems.

Each of these incidents should have immediately been addressed by the courts and/or local elections officials. Many of them were not, despite lots of evidence that fraud had, in fact, occurred. Take a look at Florida and Ohio, in particular.

This was organized voter suppression on a national scale.

Look at the dates the attorneys were being fired and the Senators/ "Bush-Leads" were being notified. **November 15- 17th, 2006. Just days after the election.**

No US Attorney to bring suit = no nasty corruption cases in court = no justice for America. Even if any of those attorneys wanted to prosecute, they would not have had time to do so,

because most were preparing to lose their jobs. It's hard to bring a case when a prosecutor is going to be fired, is fired, or there is no US Attorney in the district to bring charges. For this, I strongly assert that Bush MUST be indicted for treason, fraud, corruption, obstruction of justice, perjury, conspiracy and collusion. The pattern is all too clear. It needs to stop. It disgusts me at the most visceral level, as I'm sure it does for you. IMPEACH BUSH!!!
Kim Grant, Founder www.NetrootsNetwork.com

Ty (Titus) Meissner, proud "Kucinich Democrat for John Edwards" Napa Valley wine country, California, USA

"We have met the enemy and he is us." - Pogo (by Walt Kelly)

"Its not who votes that counts. Its who counts the votes." Josef Stalin

WARNING: In accordance with the USA Patriot Act and Presidential Directives and Executive Orders, this and all other electronic communications in all probability are screened by the FBI, NSA or other US government agencies. Any statements that could be construed as critical of any corporation, any Republican Party member or employee of the US administration may be regarded as an action in support of terrorism.

From: Deborah S. Hench
Sent: Tuesday, July 31, 2007 6:14 PM
To: Voting Systems
Subject: Top to Bottom Review

Dear Secretary of State Bowen,

It is unfortunate that you have again take away voter confidence in our voting systems by using tests outside of Election Day and Election Officials security measures that all counties institute whether by election law and by their own procedures. No system could pass when given access to every part of the voting process. Paper ballots would also fail if you handed hackers those ballots and the access to those ballot counting servers.

Your selection of Lowell Findley as the Deputy Secretary of State in charge of Voting Systems Testing is a major problem as he was the Attorney of Record for lawsuits filed against counties that use electronic voting as well as the Secretary of State. He is still involved in lawsuits in other states. This shows a bias against electronic voting before the top to bottom review began. It should also be noted that on your own website during your campaign and after, was a video on how to break into a locked garage and destroy electronic voting equipment a felony if convicted. Is this the act of a non biased Secretary of State?

As a former election official, I ran many elections in the 6 years I was in charge of the office and both parties won elections. I have 24 years in elections and have participated in paper ballots both punch card and optical scan, as well as electronic voting systems. Election Officials do everything in all elections to ensure voters votes count.

This top to bottom review is bias and conducted as the anti electronic voting activist environment instead of as the election process. I submit that you should allow the Counties to continue using their voting systems with the procedures for security that are already in place.

Remember you were elected in an election that many counties used electronic voting systems. Does this review imply that you should not have won the election?

The Secretary of State should motivate voters to vote not discourage voter participation.

Sincerely,
Deborah Hench
Retired San Joaquin County
Registrar of Voters

From: Chrisner, Bill
Sent: Tuesday, July 31, 2007 3:29 PM
To: Voting Systems
Cc:

Subject: Voting independently

Dear Secretary Bowen,

As the Executive Director of the Dayle McIntosh Center (the Center for Independent Living serving Orange County), as a resident and registered voter in Orange County, and as an individual who has a visual disability (total blindness), I am writing to demand that you follow Federal Law to ensure my right to cast my vote privately and independently on election day. I moved to California in the summer of 2004. Since I have been living here in Orange County, I have been voting in every election using the accessible voting machines that Office of the Registrar purchased and made available at my polling site starting with the 2004 Fall election. Prior to this for the past 30 years plus, I always had to depend on a family member, an election official, or an acquaintance I met at the poles to assist me. The accessible machines that are in place in Orange County enable me and other individuals with various types of disabilities to cast their ballots on the day of the election at their designated polling sites just like everyone else in the voting district. I will not allow you to take away my right to cast a private and independent vote by decertifying these machines. I will not allow you to violate Federal law in the process. We have Federal Courts for a reason.

Thank you for considering this input and for understanding that for every action there is a corresponding reaction.

--Bill

"Together we can and do make a difference."

W. D. Chrisner III, C.R.C./L.P.C.
Executive Director

Our Mission is to advance the empowerment, equality, integration and full participation of people with disabilities in the community.

From: John Washburn
Sent: Tuesday, July 31, 2007 7:46 PM
To: Voting Systems
Subject: Updated Public comments of John Washburn

Dear Secretary Bowen:

Please find attached an updated copy of the public comment I submitted yesterday. It primarily contains corrections to grammar and spelling.

The only content change is the last paragraph of the conclusion. I hope I have not been too presumptuous in this last paragraph.

Public Comments of John Washburn

Top to Bottom Review of Voting Systems used in California.

Dear Madam Secretary Bowen:

I thank you for this opportunity to make a public comment on the results of the top to bottom review. My name is John Washburn. I am a resident of Germantown, Wisconsin. I have worked as a software tester and in the field of quality assurance since 1994. I currently am certified by the American Society for Quality as a CSQE; certified software quality engineer. It is a certification I have held continuously and proudly since 1998. I have read the documents¹ found on the website of the California Secretary of State and would like to submit the following comments.

I read with fascination the various attack scenarios. Many are elegant applications to voting systems of well understood attack vectors used against other computerized systems. The results are important, disturbing, and must be addressed. But, as disturbing and import as these technical findings are, I do not believe they are the most disturbing information uncovered by the top to bottom review. The most disturbing findings are:

1. The revelation that the systems are inaccessible and, in some cases, present an active obstacle to voting accessibility.
2. The revelation that vendor representations may be fraudulent.
3. The continuing evidence the NASED/ITA model for certification has failed and is not worth the paper it is written on.
4. The continuing evidence that voting systems are defect-dense.

¹ http://www.sos.ca.gov/elections/elections_vsr.htm

The Systems are not Accessible

The Accessibility Review² by Noel Runyan and Jim Tobias is thorough, detailed, and precise in its findings. None of the three systems reviewed meets the minimum accessibility requirements of the Help America Vote Act (HAVA) or the 2005 Voluntary Voting System Guidelines³ (2005 VVSG). Direct Recording Electronic (DRE) systems compared to precinct based optical scanning are more expensive to purchase, more expensive to test, more expensive to maintain and, by all indications, are more insecure. The justification for why American elections must endure the addition insecurity and expense of DRE systems has been that DRE systems allow disabled voters and voters in language minorities the opportunity to vote privately and independently. This accessibility review refutes this justification in exceptional detail. For the first time, someone has enumerated all of the accessibility requirements of the both HAVA and the 2005 VVSG and objectively tested for conformance. Moreover, under some conditions the DRE system is an active impediment to voting.

If the person is voting in a language other than English and which uses a non-Roman alphabet such as Chinese, the DRE screen does not render characters at all. Even if the translation were well done, it is worthless if the translated text cannot be rendered for display. This is an active impediment to voting by voters in these language minorities, an impediment they would not encounter with a paper ballot which has no trouble displaying non-Roman characters.

If the person has normal vision, normal hearing, and normal upper body strength and dexterity, but is confined to a wheel chair, the DRE system is inaccessible because the forward approach is blocked by the narrow legs of the stand, hard to reach because of the height, and subject to parallax errors. For this class of voters, the DRE either prevents voting or make voting uncomfortably arduous because of the need for a side approach. Since Wisconsin has paper ballots which are tallied by optical scanner or are hand counted, voters who are wheel chair bound can be accommodated with a clip board or a suitably low table. If the polling location has only DRE equipment though, then the DRE equipment **introduces** a barrier to voting which did not exist before.

2

http://www.sos.ca.gov/elections/voting_systems/ttbr/accessibility_review_report_california_ttb_absolute_final_version16.pdf

³ http://www.eac.gov/vvsg_intro.htm

Representations of the Systems May be Fraudulent

The Red Team Report for Sequoia⁴ by Vigna, Kemmerer, et. al. includes several comments where the properties of the Sequoia Voting System were misrepresented to the security testing team by Sequoia. Section 4.4 and 4.8 are two such examples. Section 4.4 of the security assessment report states:

*There is no way to determine which version of the firmware is running on an Edge device. The Sequoia documentation states that the firmware is stored in ROM and that checksum-based mechanisms are used to determine if the firmware has been modified maliciously. However, **in reality there is no secure, hardware based mechanism** to ensure that no corrupted firmware gets loaded and executed. In addition, the Edge firmware is stored on a flash memory card and can be easily overwritten. Hardware support for trusted software execution and the use of non-writable memory would protect the Edge device from a large range of attacks from both insiders and outsiders.*

Section 4.8 of the security assessment reads:

*In the documentation ([10], p. 3-1), it is stated that: "WinEDS currently does NOT utilize code outside of MS SQL Server and no connections or permissions are required on the server (besides SQL Client.) The lack of server access by individual users provides the application with a secure client-server environment. The election data stored on the server can only be modified by authorized users only through the application." **Unfortunately, this is not true.** In fact, it is possible to connect to the database and completely compromise the MS SQL server host without using the WinEDS application. This is achieved by exploiting two security problems. First of all, the WinEDS access control procedures can be bypassed. Second, the MS SQL server delivered with the Sequoia system enables users to execute arbitrary commands.*

The emphasis of the quoted sections above is mine and highlights the diplomatic language of the assessment team. The representations of section 4.8 were made by Sequoia to the Wisconsin State Elections Board during the May 16, 2007 of the Elections board. This indicates the misrepresentation by Sequoia Voting Systems on the security of WinEDS is consistent.

Another consistent misrepresentation is that the firmware of the system is in read-only memory (ROM). Instead the security team found the firmware is stored on EEPROM/Flash memory. Flash memory is the same type of memory used in a portable flash drive or an iPod. Read-only memory is just that; read-only. Once created the contents cannot be re-written, but can only be read. While flash memory retains its contents when the power is off (non-volatile), it can be re-written (mutable). Read-only memory is both non-volatile and immutable. Flash memory is easily changed and therefore highly insecure.

Both of these representations (ROM based firmware and secured SQL architecture) are false. Since, I am not an attorney, I cannot judge whether such false representations constituted fraud. But, the misrepresentations are fundamental and hard to classify as anything other than an effort to deceive.

⁴ http://www.sos.ca.gov/elections/voting_systems/ttbr/red_sequoia.pdf

The NASED/ITA Testing Model has Failed

The security reports as a whole present more evidence that the NASED/ITA framework for testing and certification has been an utter failure. This is a significant problem which impacts the whole country. The NASED/ITA model was used to as the basis for the certification of EVERY voting system currently in use in the United States. With the exception of lever machines in New York, only equipment qualified by the NASED/ITA process was used in the most recent Federal election held on November 7, 2006. That this testing and certification model is ineffective and flawed is a concern for the State of California and every other state where NASED certification is a requirement to state certification

The NASED/ITA testing framework failed to find any of the findings of these three reports during repeated rounds of testing conducted over the course of several years. The results of these three reports from the Top-To-Bottom Review on the other hand were all uncovered in less than one month of examination. Each finding in the security reports is evidence of the failure of the NASED/ITA process. For illustration I will focus on only two of the findings from the Sequoia security assessment. The NASED/ITA testing and certification system failed to find:

- *There is no way to determine which version of the firmware is running on an Edge device.* Section 4.4 of the Sequoia Security Assessment Report.
- *The Edge firmware was discovered to include a shell-like scripting language interpreter.* Section 4.5 of the Sequoia Security Assessment Report.

The inability to identify the system under test is a violation of Section 8.6.d, Volume I, Section 8.7.1, Volume I, and Appendix B.3 Volume II of the 2002 VVSG.

Section 8.6.d Volume I states:

The vendor shall establish such procedures and related conventions, providing a complete description of those used to:

- Perform a first release of the system to an ITA;*
- Perform a subsequent maintenance or upgrade release of the system, or a particular components, to an ITA;*
- Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the qualified system version; and*
- Perform a subsequent maintenance or upgrade release of the system, or a particular component, to a customer, **including confirmation that the installed version of the system matches exactly the qualified system version.***

Section 8.7.1 Volume I states:

Physical Configuration Audit

The PCA is conducted by the ITA to compare the voting system components submitted for qualification to the vendor's technical documentation. For the PCA, a vendor shall provide:

- Identification of all items** that are to be a part of the software release;*

Section B.3 Volume II (System Identification) states:

System Identification

This section gives information about the tested software and supporting hardware, including:

- a. System name and major subsystems (or equivalent);*
- b. **System Version;***
- c. Test Support Hardware; and*
- d. Specific documentation provided in the vendor's TDP used to support testing.*

Since, "There is no way to determine which version of the firmware is running on an Edge device", it is not possible to meet any of these three requirements of the 2002 VVSG. How was this failure to conform missed by the vendor funded test labs during repeated rounds of testing? Paul Craft, Steven V. Freeman, and Britt Williams of the technical subcommittee of the NASED Voting Systems Board reviewed every report generated by the vendor funded ITA labs. How is it that they failed to notice that the labs were not testing for conformance to the system identification requirements? One possibility is that these three granted a waiver to Sequoia Voting Systems on the matter of conformance to standard. Such waivers to conformance are permitted by Appendix B.5 Volume II of both the 2002 and 2005 VVSG. The relevant paragraph of Appendix B.5 of the 2002 VVSG reads:

Of note, any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection. Deficiencies of this type may include failure to fully achieve the levels of performance specified in Volume I, Sections 3 and 4 of the Standards, or failure to fully implement formal programs for qualify[sic] assurance and configuration management described in Volume I, Sections 7 and 8. The nature of the deficiency is described in detail sufficient to support the recommendation either to accept or to reject the system, and the recommendation is based on consideration of the probable effect the deficiency will have on safe and efficient system operation during all phases of election use.

As the security assessment report states, interpreters are prohibited by the 2002 VVSG. Again, how is that the vendor funded ITA labs failed to notice the presence of a prohibited interpreter during any of several rounds of testing? The problem for California on this matter is more acute. In December of 2005 it became public knowledge that the voting systems from Diebold Election Systems Inc. used prohibited interpreters and interpreted code. In response, Bruce McDannold, Interim Director of the Office of Voting System Technology Assessment, specifically asked Paul Craft and Steven V. Freeman if there were any other voting systems used in California which also had interpreters and interpreted code. In this [email exchange](#)⁵, Mr. McDannold states that some think the State of California is "picking on" Diebold over the interpreted code issue. At the time Mr. Craft and Mr. Freeman stated no other voting system used in California used interpreters or interpreted code. It is ironic that the security assessment team has vindicated Diebold Election Systems. There were two voting systems in California using interpreters, but only Diebold was singled out for investigation.

Paul Craft and Steven V. Freeman are 2 of the 3 people on the technical subcommittee of the NASED Voting Systems Board. How is it they were unaware of the interpreter found in the Edge voting systems from Sequoia? Mr. Craft and Mr. Freeman were hired because of their connection with the NASED process and their expert knowledge of voting systems. The State of California specifically and directly asked both Mr. Craft and Mr. Freeman about interpreters in California Voting Systems. They stated Diebold was unique. Mr. Craft and Mr. Freeman failed the State of California when they provided this incorrect answer. One may ask what other work product from Mr. Craft and Mr. Freeman may also be defective.

⁵ <http://www.washburnresearch.org/archive/FCMGroup/CraftFreeman02.pdf>

The Systems are Defect-Dense

Over the years, every time a vendor-independent team investigates a voting machine the team finds new, significant, and possibly election-altering defects. An incomplete list of these past studies is:

- The 2003 John Hopkins report,
- The 2003 RABA report from Maryland,
- The 2003 Compuware report from Ohio,
- The 2004 follow ups reports by Compuware to the initial 2003 Ohio report,
- The 2005 examinations by Hugh Thompson in Leon County,
- The 2005 examinations of Hari Hursti in Leon County, Florida,
- The 2006 examinations by Hari Hursti in Emery County, Utah,
- The 2006 Princeton report on the TSx,
- The 2007 report from the University of Connecticut on the AccuVote OS, and
- The 2007 report from the University of Connecticut on the AccuVote TSx.

California's three new security assessments again find new and significant defects which are distinct from those found in prior reports. In my expert opinion this indicates that the software in these systems is defect-dense. A defect-dense system has a high number of defects per thousand lines of code. Defect-dense systems are marked by the same properties as exhibited by voting systems:

1. Different testers find different defects. In defect-sparse systems, different testers tend to find the same defects over and over. This is because there are so few defects to find that effective testing by different groups repeatedly finds the few defects present.
2. The defects found are generally severe. This is because severe defects are usually found before minor defects. Major defects are easier to detect because the behavior is manifestly incorrect and major defects tend to hide or obscure the presence of more minor defects.

Consider a line of automobiles from the fictional manufacturer Washburn Motors. What if every time a mechanic or engineer not hired by Washburn Motors examines one of my cars, they find a new, serious problem? One mechanic finds the engines stalls at 60 miles per hour. A second discovers the axles tend to break. A third notices the brakes fail intermittently in warm weather. A fourth discovers the odometer sometimes loses 18,000 miles. Would you buy a car from Washburn Motors? Most would not. This is because even though they do not use the term defect-dense, most people instinctively recognize the symptoms and would avoid buying a lemon from Washburn Motors.

Voting systems currently exhibit the same behavior as the fictional cars from Washburn Motors. Every time someone not hired by the manufacturer examines the product, they find new, serious problems.

Conclusion

Secretary Bowen you face some hard choices which must be made in a short time frame. I wish I could offer more than the following suggestions.

1. Do not rely on the results of the NASED/ITA model. It has failed and the certifications issued under the program is not be worth the paper they are written on. I would urge the Secretary to consider creating a multi-state testing consortium. This idea was first presented to the state by Eric Lazarus during the Voting Testing Summit sponsored by the State of California in 2005. His paper is found [here](#)⁶ is entitled: "[A Vision for the Testing of Election Systems in a HAVA World](#)". An expansion on the framework proposed by Mr. Lazarus is found [here](#)⁷ and is entitled: "[Testing Election Software Effectively](#)". I have misgivings that the EAC/NIST/VSTL model currently under construction is little more than the NASED/ITA model with different acronyms.
2. To the extent possible limit the expansion of this unreliable and inaccessible voting technology. Consider technology which actually expands accessibility such as non-tallying ballot marking devices (e.g. Automark or Vote-PAD) or systems which print ballots on demand under the direction of voters. Expanding the franchise to those with disabilities or who are in a language minority is goal which resonates with the deepest aspirations of the American ideal. We should select technology which is both appropriate and effective in realizing this ideal.
3. Sequoia was asked by Bruce McDannold in December of 2005 if there were interpreters or interpreted code found on voting systems from Sequoia. What was the company response to this question? The representations made by Sequoia which have been contradicted by the security assessment team must be assessed to determine if those representations constitute fraud.
4. Determine, if possible, whether the non-conformances found by the top-to-bottom review were also found by the NASED/ITA. Testing results are under the NASED/ITA model are consider trade secrets held by the equipment manufacturer. Thus it is possible the reported non-conformances were discovered by the NASED/ITA process and granted waivers, but the disclosure of such waivers has been blocked by the assertion of trade secrets and the enforcement of non-disclosure agreements.

Even if you ultimately decide to use the currently certified systems, continue to vigorously test these systems beyond this Friday. Information acquired late is better than no information. You will need all the evidence and information possible in order to make an informed and prudent decision. I fear any decision you make on these voting systems (keep the certifications as is, decertify all, decertify some, mandate specific procedures, etc.) will deeply anger some segment of the people you have chosen to serve. On this matter I can only offer this advice: It is better to squarely face the uncomfortable truth than accept the comforting lie. Postponement should be avoided. As hard as it is in the immediate good things flow from following the truth and bad things will drown as you hide the refuge of the lie.

⁶ http://www.sos.ca.gov/elections/vstsummit/presentations/a_vision_for_testing_election_systems_lazarus.ppt

⁷ http://votetrustusa.org/index.php?option=com_content&task=view&id=870&Itemid=26

From: Sharon B. Ross
Sent: Tuesday, July 31, 2007 11:53 PM
To: Voting Systems
Subject: Review of voting systems

Secretary Bowen and Staff-

It was indeed an honor and privilege for me to attend the public hearing of July 30, regarding

the top-to-bottom review of the currently certified voting systems currently used in California.

I commend you for your courage to challenge the use of these systems in view of the apparently misdirected unity of the County Registrars who were in attendance and perhaps those not attending.

It appears that even though hackers may or may not have made their appearance into the currently used systems evidence has now been presented to California by way of your office that these systems are susceptible and vulnerable to electronic manipulation.

This now means that you and you alone have the deciding decision to be courageous and to say

to the voters of California that you are upholding our right to have a vote that counts. Perhaps your

courage will give momentum to other States to follow suit and perhaps we citizens of the United

States can once again have the knowledge and faith to know that our votes count and that we

have returned to a Nation which not only boasts democracy but actually have a democratic election process.

I know this is a challenge for you and your staff----We the citizens who support an honest

vote are here to help you when you put forth the call for help----It can be done-It can be done-.

Decertify and let's move forward-we have a full 6 months...

NOTHING IS MORE IMPORTANT THAT A VOTE THAT COUNTS

I send you courage-

Respectfully,
Sharon B. Ross

From: David Griscom
Sent: Wednesday, August 01, 2007 4:51 PM
To: Voting Systems
Subject: Beware Insiders.



444392631-Election
Wars in Pim...

A few days ago I sent you an earlier draft of the attached chapter slated for Mark Crispin Miller's new book entitled "How to Steal an Election: The Bush Regime's Subversion of Democracy, 2002-2008," coming out in January.

The moral of my Arizona tale, as well as the tales of other chapters in this book, is that the primary attack vectors in computerized elections come from insiders. And one never knows who the insiders are (although one gets an idea that election officials who oppose audits likely do so because they don't want to get caught).

Beware insiders, whatever else you do by the way of election reform. Putting seals on voting machines and their memory cards is a palliative. Only well-designed and well-carried-out audits can prevent election theft by insiders.

Dave

Election Wars in Pima County, Arizona: A Microcosm of Nationwide Election Theft?

David L. Griscom Ph.D.

<http://www.impactglassresearchinternational.com/>

1 August 2007

I. John Brakey, Master Sleuth of Election Fraud

On 2 November 2004, John R. Brakey was Democratic Cluster Captain for four precincts in Arizona Legislative District (LD) 27, a part of the predominately-Hispanic, 80% non-Republican Congressional District (CD) 7. LD 27 encompasses a part of Pima County including the southwest corner of the city of Tucson. John was new to the job, but he knew that part of his duties – and prerogative – was to pick up “tear sheets,” which are carbon copies of the list of voters who had already cast their ballots hand-printed by the poll workers on a form called the Consecutive Number Register (CNR). Poll workers in three of these precincts greeted him with hostility, and in one case they attempted to conceal the existence of several completed CNR pages for which he was requesting copies.

As Election Day wore on, John became increasingly suspicious that the poll workers in those three precincts were up to something. So, over an hour after the polls had closed, he returned to his home polling place, a school located in Precinct 324, to see what evidence he might pick out of the trash. To the mutual shock of everyone present, he walked in on the poll workers apparently in the act of altering the CNR (which should have been completed at the time of the arrival of the last voter). He also observed the vault of the Diebold optical-scan voting machine to be wide open, instead of being locked shut as it should always be. The poll workers rose to their feet in unison, cursing Brakey and telling him to get back out of the room; (see p. 132 of Mark Crispin Miller’s book “Fooled Again”). He did so quickly after a woman poll worker began to circle behind him brandishing a club-like cane as though a weapon.

From that moment on, getting to the bottom of what was going on became John’s all-consuming passion. He abandoned his bread-winning job and began working unpaid 18-hour days gathering and entering on Excel spreadsheets all available records bearing on the voting at Tucson Precinct 324 on Election Day 2004. I was privileged to be able to aid John in the forensic analysis of these records, the results of which I ended up presenting as PowerPoint lectures at the National Election Reform Conference in Nashville, TN, April 9, 2005, the Election Assessment Hearing in Houston, TX, June 29, 2005, the Election Integrity Workshop held at the quarterly meeting of the Arizona Democratic Committee, Flagstaff, AZ, August 20, 2005, and a session entitled “Are We a Democracy? Vote Counting in the United States” at the 2007 Annual Meeting of the American Association for the Advancement of Science (AAAS), in San Francisco, February 16, 2007.

II. Evidence for Poll-Worker Fraud in Tucson Presented at a National Meeting of the Premier Science Organization in the United States

The following is slightly modified version of my abstract for the 2007 AAAS meeting:

As Cluster Captain on 2 November 2004, John Brakey returned to one of his assigned Tucson polling stations an hour after the polls had closed, surprising poll workers apparently altering the poll books. Brakey began an audit of this precinct (#324) based on copies of all public records: (1) a list of all voters registered in precinct, (2) all Signature Rosters (SRs), (3) the Consecutive Number Register (CNR) with 884 poll-worker-printed voter names, (4) the Official Ballot Report and Certificate of Performance signed by all 7 poll workers, and (5) a list voters who signed affidavits on the envelopes conveying Provisional Ballots (PBs) to the county Recorder. Brakey recovered from the morning-after trash (6) the poll-worker-annotated "Advice to Voter" slips. Records (2) and (6) indicated which voters were required to vote on PBs (which are only accepted by the Recorder if she ascertains that the voter is registered and had not mailed in an Early Ballot). Record (4) could not be reproduced by from the public data without assuming 39 PBs were illegally fed into the optical-scan ballot box on Election Day. The CNR contained 11 fewer unique names than the number of ballots in the ballot box according to (4), implying 11 felony double votes. The poll workers issued 11 extra ballots as alleged spoil replacements, possibly to cover up (but failing to disprove) these double votes. There were also exactly 11 voters who signed a "regular" SR but whose names are not listed on the CNR, 11 voters who signed the PB SR but are not on the CNR, 11 voters who signed both the "regular" and PB SRs, 11 registered voters listed on CNR who failed to sign any roster at all, and 11 phantom voter names appearing on 11 of the signed envelopes of PBs received by the Recorder that do not match any signature on any SR - nor any entry on the CNR! The probability of any one of these irregularities occurring 11 times is much less than 1/11. The odds of all 7 occurring exactly 11 times as independent random accidents (e.g., due to incompetence) are much, much less than one chance in 11 raised to the 7th power = 19.5 million. Three voters had their names inscribed a second time on the CNR exactly 100 places after the first, with one-chance-in-131-million probability. Despite their complete control of the CNR, the poll workers wouldn't have been able to contrive such statistical rarities without a "system." Indeed, (6) revealed a non-standard hand-numbering scheme which would have fit the purpose. We conclude that 22 valid Kerry votes could have been discarded (as 11 allegedly spoiled ballots and the 11 PBs rejected by the Recorder, likely because of 11 forged signatures) and 61 Bush votes could have been forged (as 39 PBs illegally fed into the ballot box on Election Day, 11 double votes, and 11 alleged spoil replacements) – a shift of 9.4%. Still, the inferred "system" would have deposited paper ballots in the ballot box exactly matching the number claimed in (4), and voter choices on these ballots would match the official tally, thus appearing honest in the event of a hand recount – and thereby covering up demonstrably possible hacking the 1.94w memory cards in optical-scanner precincts where the poll workers were honest.

My actual AAAS PowerPoint is available for downloading [1].

I should mention that the estimated vote shift given above (9.4%) differs from that which I erroneously stated in the original abstract as 8% and is based on the assumption that the poll workers had no more blank ballots than the 926 officially issued to them. In fact, extra ballots would have been easy enough to obtain, since in Pima County anyone can request up to two replacement mail-in ballots before the Election *without returning a spoiled one*; (John Brakey's wife actually spoiled hers and was sent another, no questions asked). In my PowerPoint I infer a possible 12.8% shift, which if correct would require the poll workers to have handed out 30 additional ballots and subsequently physically destroyed 30 ballots after voters had marked them.

All AAAS abstracts are forbidden to exceed 500 words, and even by adding 50 more in the above version, much important background is obscured. So let me use a few more words below to fill in some of this background.

As far as I know, John Brakey was the first to discover (by surfing the internet) that the 1.94w memory card used on the Diebold optical-scanners contains "interpreted code" and is thus capable of running programs that could in principle be used to alter the vote totals. This principle was ultimately confirmed in practice by Finnish computer expert Harri Hursti [2,3].

So John had demonstrated poll-worker fraud in Pima County, and had *also* realized that elections could be stolen by hacking of the memory cards. He called the combination of these two attack vectors the "Hack and Stack" [4] (with "Stacking" having the same meaning as ballot-box "stuffing").

III. Evidence for Nationwide Election Fraud

Thanks to Harri Hursti and others, we now know for a fact that elections *can* be electronically stolen by hacking (e.g., by inserting vote-flipping programs the 1.94w memory cards) and John Brakey and I have shown that some poll workers may actually be stuffing ballot boxes.

So the remaining question is: Are entire elections actually *being* stolen by these (and likely other) methods? Based on the national exit poll statistics, the answer is a resounding, *yes*: This was done nationwide in both 2004 and 2006. For anyone in doubt, I list below some reading assignments.

Election 2004:

- (1) "Was the 2004 Presidential Election Stolen?" by Steven F. Freeman and Joel Bleifuss (Seven Stories Press, New York, 2006).
- (2) Robert F. Kennedy's piece in Rolling Stone Magazine [5].

(3) And here's a real "hair raiser"! Actually presented as a kind of ghost story, Michael Collins describes the unbelievable consequences of the practice of "forcing" exit polls to agree with the official ballot tallies – a bizarre "see no fraud" gimmick used for the first time in 2004 but never explained to you by the so-called mainstream media [6].

Election 2006:

"Landslide Denied" by Jonathan Simon and Bruce O'Dell: A short barnburner of a read (even though mathematically correct!), this piece examines some different, but equally bizarre consequences of "forcing" the 2006 exit polls to "see no fraud" [7].

But if for some reason you might be reluctant to believe this statistical evidence (like maybe you don't do math and/or the conclusions of these scholarly studies are way too horrifying to accept), please read Pokey Anderson's trenchant exposition of how and why *all* electronic voting technology is not merely subject to hacking, but presents a clear and present "open door" just begging to be exploited by insiders [8].

IV. Mail-In Ballots: An Invitation to the Perfect Crime

I have been told that only two States in the Union have laws on their books allowing for recounts of mail-in ballots. Obviously, if mail-in votes should be stolen, it would be the perfect crime.

So who witnesses or otherwise assures the integrity of the mail-in ballots we cast? I don't know about other places, but every Election Day for a decade or so prior to 2004, the 8th floor of the Pima County Building, where the Mail-In ballots have been stored, was closed by the police bomb squad at the time of their unwitnessed counting, presumably by Pima County election officials. This old Pima County "tradition" is an eerie precedent for what happened in Warren County, Ohio, on Election Night 2004 [9].

Below is a table of the official Election Day 2004 voting at John Brakey's Arizona LD 27, representing a 74% turnout of some 80,000 registered voters:

Table 1.

Averages of 63 Precincts of AZ LD 27	Kerry/Dem	Bush/Repub	Other/NOP
E2004 At-Precinct Voting	61.9%	37.0%	1.0%
E2004 Early/Mail-In Voting	64.6%	34.6%	0.9%
Party Registration	48.8%	20.6%	29.0%

Note that the ever-vulnerable mail-in vote exhibits 2.4% *fewer* Bush votes than was the case for the At-the-Precinct voting. Could this be deliberate, given that those in the know would automatically look for anomalies in the Mail-In totals as possible prima-facie evidence of election theft?

V. New Evidence that They Hacked the *At-the-Precinct* Vote in 2004

After nearly 2 years of assuming I had done all I could by way of exposing Election-2004 fraud in Pima County, I was inspired to return to the Excel spreadsheets of Election 2004 data compiled John Brakey for all 63 precincts of Arizona LD 27, which comprises very close to 80,000 predominately-Hispanic, 80%-non-Republican registered voters ...who somehow seemed to vote 36% for Bush, even with an amazing 74% turnout!

Since John's data were broken out by precincts, I could do crude statistics on them. (Some of my esteemed colleagues in the EI community who practice full-blown statistics could certainly improve on what I have done by taking into account the variable uncertainties associated with varying precinct sizes.)

My starting premise was this: On average, for voting across a large district (59,752 voters actually voting in the present case), the ratios of At-Precinct to Mail-In to Provisional-Ballot of the vote shares of a major-party presidential candidate should be accurately 1 : 1 : 1.

In fact the data don't obey that rule here. Of the 31,595 voters voting at their respective precincts, 37.0% went for Bush, whereas "just" 34.6% of the 25,886 Mail-In voters went for Bush. This is actually a huge discrepancy, likely to have a low probability of happening by accident.

I will now show you that (at least in AZ LD 27) it appears that someone hacked the *At-the-Precinct* vote but left the Mail-Ins untouched ...mostly.

Recall that John Brakey and I succeeded in proving that at Pct 324 of LD 27, colluding poll workers had stuffed ("Stacked") the ballot box against the possibility that a random recount should have been triggered. In such a case crooked election officials would have been standing by to "randomly" select Pct 324, and other similarly conspirator-infiltrated precincts, for auditing. In this event, we would be back again to the perfect crime.

This was John Brakey's great insight: the "Hack and Stack!"

John also caught the pious poll workers at Pct 324 in the act of "Stacking" the ballot box there. And now thanks to John's compiled data for the entire LD, I was able to take a deeper look at the relative voting patterns of Provisional, At-the-Precinct, and Mail-In voting – which I suppose should occur in the ratios very close to 1:1:1 within 95% statistical confidence for large enough voting units ...*provided* the election was not Hacked in one or two of these categories.

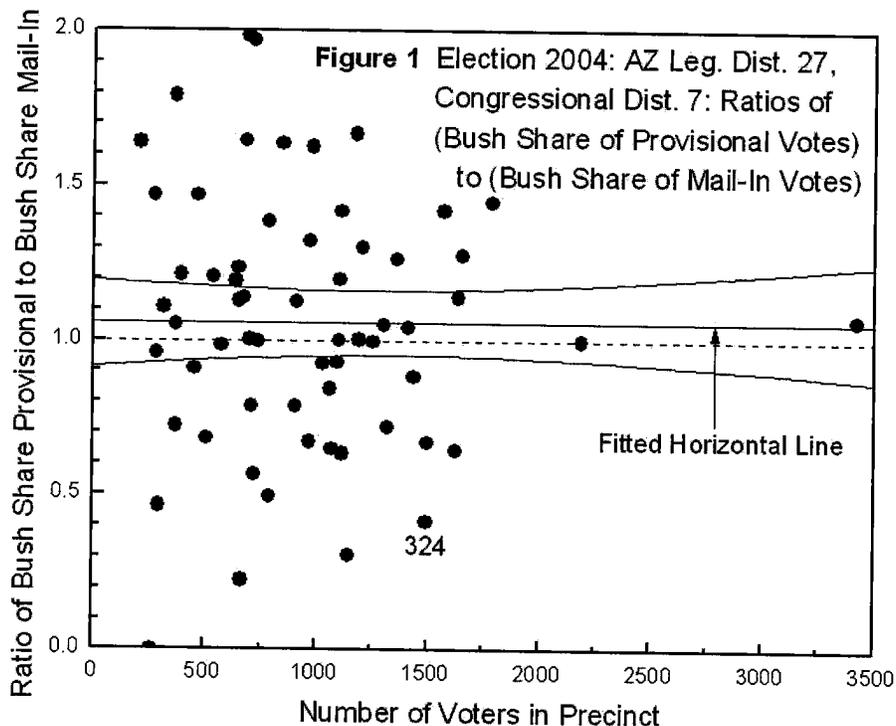
Here is how I approached the problem:

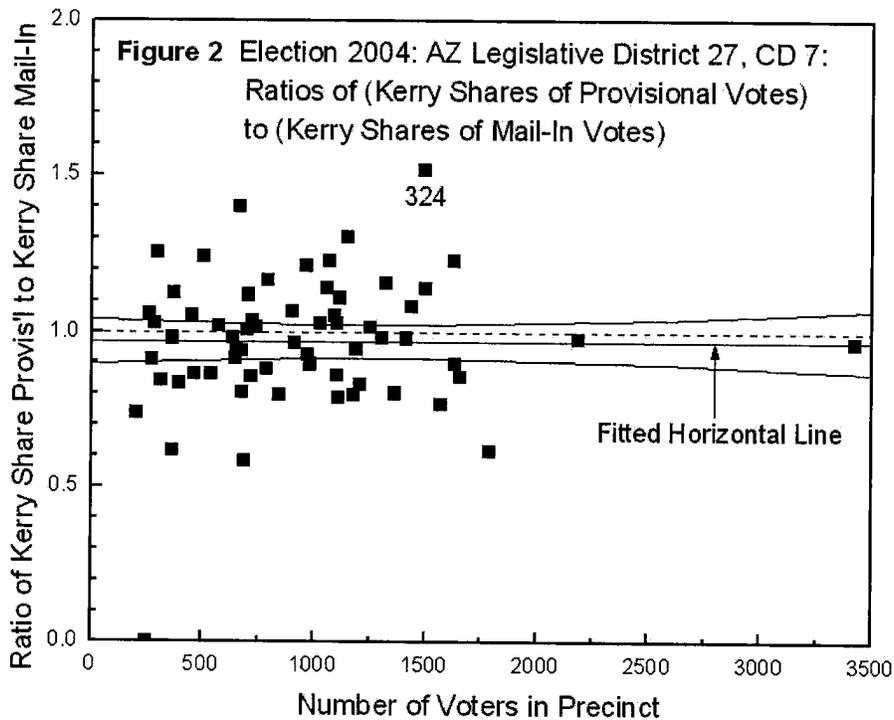
First, I assumed that the Provisional Ballots *actually accepted* by the County Registrar are virtually 100% honest, since each was sealed in an envelope with a voter signature and printed name and address on the affidavit affixed to the outside. For such a ballot to

have been accepted, the Recorder must recognize the signer of the affidavit to have been a voter registered to vote in the correct precinct who had not voted early (or elsewhere on Election Day). *And*, why even try to steal this component of the vote, given that the *accepted* Provisionals accounted for mere 3.8% of the total?

Unfortunately though, forensic analyses the Provisional-Ballot data are subject to large statistically uncertainties owing to the relatively small sample sizes (average 36 Provisional ballots officially *accepted* per precinct in AZ LD 27). Still, when I took the ratios of the Provisional to the Mail-In data, precinct-by-precinct, and used the mathematical curve-fitting software the came with my graph-making program, the continuous horizontal lines that fitted the data in the graphs of Figures 1 and 2 each agreed with the “null hypothesis” that the ratio should equal 1.00 (represented by the horizontal dashed line), within the bounds of the 95% confidence limits concomitantly generated by my software (pair of curved lines above and below the fitted straight line).

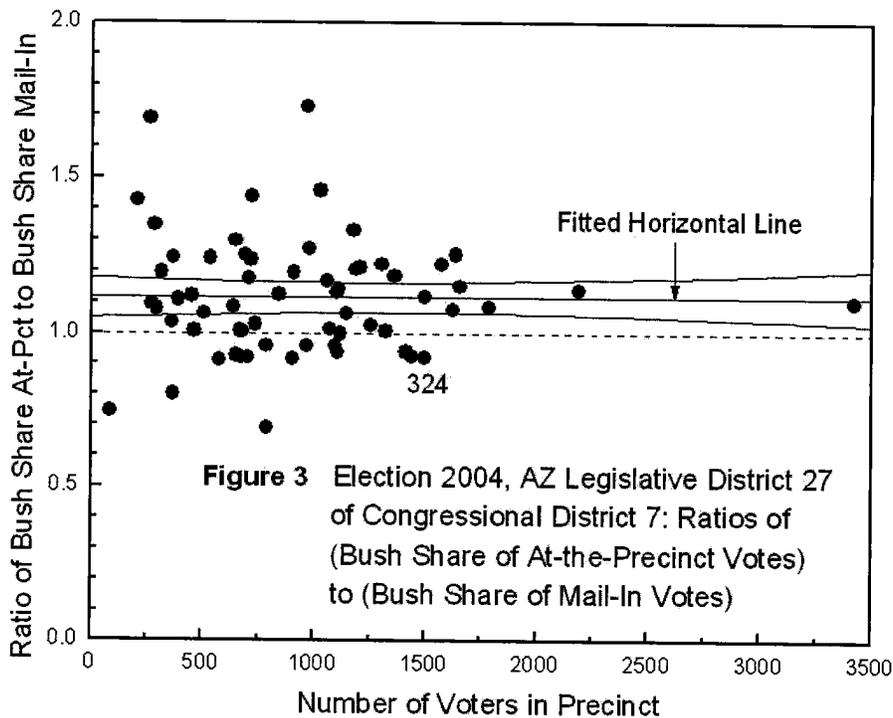
Figure 1 displays the individual-precinct Provisional-Ballot-to-Mail-In ratios of the Bush shares, while Figure 2 shows the corresponding ratios for the Kerry shares. Note that in both cases the black dashed line (the “null hypothesis”) falls between the two 95% confidence curves associated with the fitted horizontal line.

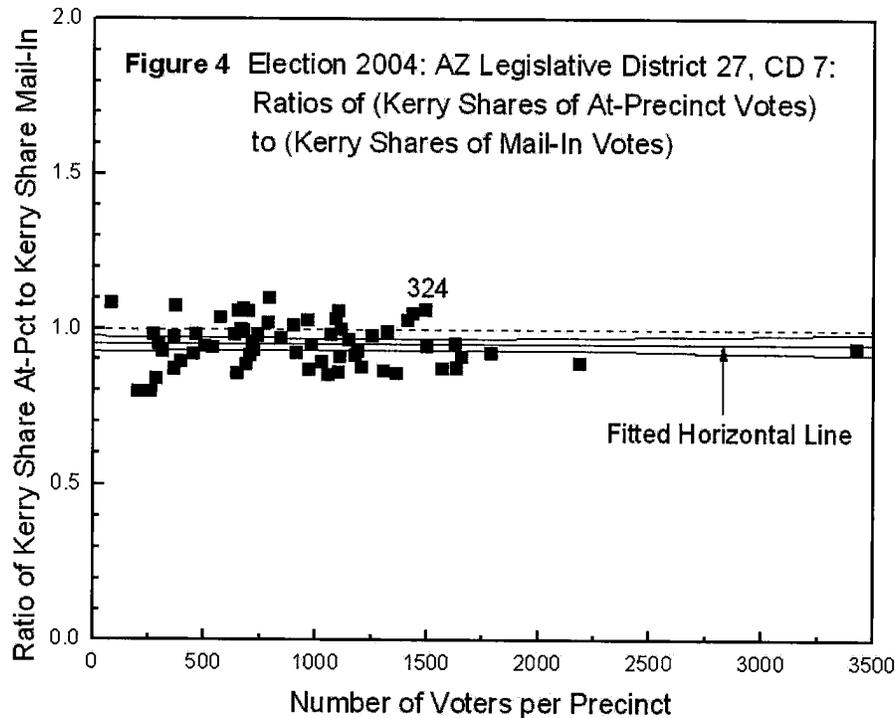




Conclusion: The vast majority of the Mail-Ins are likely *unHacked*.

Next, I took the ratios of the At-the-Precinct data to the (statistically-significant, and now shown to be mostly honest) Mail-In data. And, guess what? We see in Fig. 3 that Bush's ratios of his At-the-Precinct votes to his Mail-Ins are shifted on average 11.5% in his favor, and this shift is well *outside* the 95% confidence limits of the fitted horizontal line!





And in Fig. 4 the ratios of Kerry's At-the-Precinct votes to his Mail-In votes are seen to be shifted an average of 5% against him, again *outside* the 95% confidence limits.

My tentative conclusion is that the *At-the-Precinct* vote at AZ LD 27 was *Hacked!*

The alternates to this interpretation would be that all precincts were operated by poll workers as crooked as Rev. Kahn and his wife at Pct. 324, but far more competent (note that the data points for Pct 324 in Figs. 3 and 4 appear favorable to Kerry) ...or else the voters in Arizona LD 27 inexplicably wanted to keep Bush in office.

VI. Doing the Numbers: Reasons to Doubt that the No-Party-Preference Voters of AZ LD 27 Were Strongly Pro Bush

A critical reader might well ask the question: Couldn't the Pct 324 poll workers have been stealing votes on *Kerry's* behalf, given the positions of the data points in the graphs above? Well, the data points above are *ratios*, so they reveal nothing more than the relative differences between the At-the-Precinct voting and the Mail-In voting. Here is a table of the actual 2004 At-the-Precinct and Mail-In vote shares at Pct 324.

Table 2.

Precinct 324 of AZ LD 27	Kerry/Dem	Bush/Repub	Other/NOP
E2004 At-Precinct Voting	56.9%	41.6%	1.6%
E2004 Early/Mail-In Voting	53.6%	45.1%	1.3%
Party Registration	47.1%	21.5%	31.5%

By subtracting the LD-wide-average data shown in Table 1 from Table 2, we see in the resulting Table 3 that Kerry did stunningly *worse* (and Bush correspondingly much better) at Pct 324 than the *average* for the entire Legislative District 27 – *particularly in the case of the Mail-Ins: a net 19.1% shift in Bush’s favor* (after correction for the lower-than-average Democratic party registration)!

Table 3.

Difference (Pct 324) - (LD-27 Average)	Kerry/Dem	Bush/Repub	Other/NOP
E2004 At-Precinct Voting	-5.0%	4.5%	0.5%
E2004 Early/Mail-In Voting	-11.0%	10.6%	0.4%
Party Registration	-1.7%	0.8%	2.4%

Let me explain this kind of “vote shift” calculation by using the Pct-324 At-the-Precinct vote shares as the next example. In the first row of Table 3 we see that at Pct 324 Kerry has 5.0% *smaller* (negative) At-the-Precinct vote share than the LD-27-wide average. We also see that Bush has a 4.5% *larger* At-the-Precinct share than the LD-27-wide average. To get the net shift of votes from Kerry to Bush, we subtract the number in the Kerry column from the number on the same row in the Bush column. Thus, for the At-the-Precinct voting we get a 9.5% shift. Again, because we are using the numbers of Table 3, we are measuring all shifts *relative to the LD-27-wide average*.

But now if we wish to improve our accuracy, we really ought to correct for the fact that there were 1.7% fewer registered Democrats at Pct 324 and 0.8% more registered Republicans *relative to the LD-27-wide average*. For purposes of making any “correction” based on party registration we have no choice but to first make a modest assumption, namely, that all registered Democrats voted for Kerry and all registered Republicans voted for Bush. Thus, we take the net shift of party registration (in this case in Bush’s favor) at Pct 324 *relative to the LD-wide average* (2.5%) and subtract it from the net At-the-Precinct Kerry-to-Bush vote-share shift *relative to the LD-27-wide average* (9.5%) to get a the part of the shift that might be the result of fraud (“just” 7%).

In the discussion below I will use the jargon “red shift” and the acronym “NOP.” By a “red shift” I mean a net shift favoring Bush (that is, a Kerry loss plus a Bush gain added as positive numbers), and by a “blue shift” I mean one that favors Kerry (a Kerry gain plus a Bush loss). Also, from now on I will use the acronym “NOP” to include all third-party registered voters in addition to the *far more numerous* voters who registered as “No Party Preference.”

Under the assumption I just described, one may calculate the corresponding percentages of NOP voters who cast their votes for either candidate. Consider Bush’s Pct-324 At-the-Precinct share of 41.6% in Table 2. If we subtract from this the Republican party registration of 21.5%, we get a number, 20.1%, which (under our assumption) is the percentage of all voters at Pct 324 on Election Day 2004 who both voted for Bush but were neither Republicans nor Democrats. Therefore, under our assumption this number of voters *must have been registered NOP*. Next we can take the ratio of this number to the percentage of *all voters* (no matter who they voted for) who were registered NOP,

seen from Table 2 to be 31.5%. Expressed as a percentage, 20.1% divided by 31.5% is 64% – an unexpectedly large number in my view.

Still, the devil's advocate (and Karl Rove) would argue that all red shifts resulted from NOP voters at Pct 324 – *and* LD-wide – who simply decided to vote for Bush in large numbers. (Their reasons for this might have been as trivial as having watched a “Swift Boat” attack on Kerry the night before or as visceral as a deep fear that Kerry would defend them less well from “the terrorists” than Bush did on 9/11).

So, *were* the NOPs in John Brakey's predominately-Hispanic precinct rabidly pro-Bush in that moment? Not according to the canvasses that John and I and others carried out just a few days before the election. I recall encountering very few Bush voters among those NOPs and infrequently voting (“turnout”) Dems that I canvassed. Unfortunately, however, our canvass sheets were lost before we totaled them up. So we have no objective pre-polling numbers for that part of Tucson.

Nevertheless, I did retain the results of my own canvass (for MoveOn) of several more-affluent, less-Hispanic, and more-Republican neighborhoods of Arizona CD 8, in the Catalina foothills 18 miles to the northeast of Pct 324. Of the 115 individual NOPs and “turnout” Democrats I interviewed, 95 were certain of, or leaning toward, voting for Kerry, while only 6 had any intentions of voting for Bush!

Now let me put these numbers in perspective. I conducted what would probably be regarded as a statistically significant poll of a predominately-WASP upper-middle-class Tucson neighborhood and found that **83% of the NOPs and turnout Dems planned to vote for Kerry and only 5% planned to vote for Bush!**

So if you should insist on believing that 64% (At-the-Precinct) and 75% (Mail-In) of the predominately-Hispanic NOP voters of less-affluent Pct 324 really voted for Bush (with a 75.9% turnout, no less!), I'll sell you the Brooklyn Bridge.

VI. Some Very Odd Numbers

The *huge* discrepancy between the At-Precinct and Mail-In votes at Pct 324 noted above has to be *way* outside normal statistical error. While statisticians will need to demonstrate just how improbable the above numbers are, I conclude that the *Mail-In* votes – at least for Pct 324 – have to have been Hacked. If I am right, the next question is: In how many other precincts could the Mail-In vote have been Hacked? It cannot have been too many, given that Figures 1 and 2 show that the LD-wide *average* Bush and Kerry shares of the Provisional Ballots (presumed honest) are equal to their corresponding *average* shares of the Mail-In ballots with greater than 95% statistical confidence.

I decided that two of the prime candidates for investigation had to be the other two precincts (numbers 271 and 235), where John Brakey encountered poll workers behaving

peculiarly and/or displaying hostility on Election Day 2004. Tables 4 and 5 show the official results for Precincts 271 and 235, respectively, *presented in terms of their differences from the LD-wide averages* (exactly analogous to Table 3).

Table 4.

Difference (Pct 271) - (LD-27 Average)	Kerry/Dem	Bush/Repub	Other/NOP
E2004 At-Precinct Voting	1.9%	-1.2%	-0.7%
E2004 Early/Mail-In Voting	-2.6%	2.8%	-0.2%
Party Registration	5.0%	-2.7%	-0.8%

We see in Table 4 a 3.1% “blue shift” in the At-the-Precinct voting and 5.4% red shift in the Mail-Ins. But when I took into account the net 7.7% party registration advantage enjoyed by the Democrats over the Republicans of Pct 271, I arrived at the following corrected numbers for Pct 271 relative to the average for LD 27: a 4.6% At-the-Precinct red shift (no longer blue) and a hefty **13.1% red shift in the Mail-Ins** with respect to the LD-wide average.

Now let’s look at Pct 235. In Table 5 we see a 2.3% red shift in the At-the-Precinct voting and whopping **13.8% red shift in the Mail-Ins** (both taking into account the tiny 0.2% correction for party registration).

Table 5.

Difference (Pct 235) - (LD-27 Average)	Kerry/Dem	Bush/Repub	Other/NOP
E2004 At-Precinct Voting	-1.5%	0.6%	0.9%
E2004 Early/Mail-In Voting	-7.5%	6.1%	1.4%
Party Registration	0.0%	-0.2%	1.7%

Here is my hypothesis for what went down in LD 27 of Tucson CD 7 on Election Day 2004. There was a conspiracy comprising (1) insiders with access to the 1.94w memory cards in the Diebold AccuVote OS optical scanners (or alternatively to the GEMS central tabulators) and (2) a cadre of colluding poll-worker crews, including the one headed by Rev. Kahn at Pct 324. The overall plan was to Hack the At-the-Precinct vote at *all* precincts *except* the ones manned by colluding poll workers, whose job it was to “Stack” (stuff) the ballot boxes at those polling places. However, the evidence shows that the Mail-In vote was Hacked in these Stacked precincts – perhaps to shield the crooked poll workers there from suspicion, knowing that forensic investigators might compare the Mail-In votes with the At-the-Precinct votes as a possible sign of ballot-box stuffing. If that was their objective, they badly overdid it, amassing a **19.1% red shift in the Mail-Ins** at Pct 324 vis-à-vis a red shift in the At-the-Precinct votes of “just” 7% contrived by the Kahn team. (Bear in mind that all of these red shifts are *with respect to the LD-wide average* and also that the LD-wide average At-the-Precinct vote is itself red shifted with respect to the LD-wide average Mail-In vote; refer to Figures 3 and 4.)

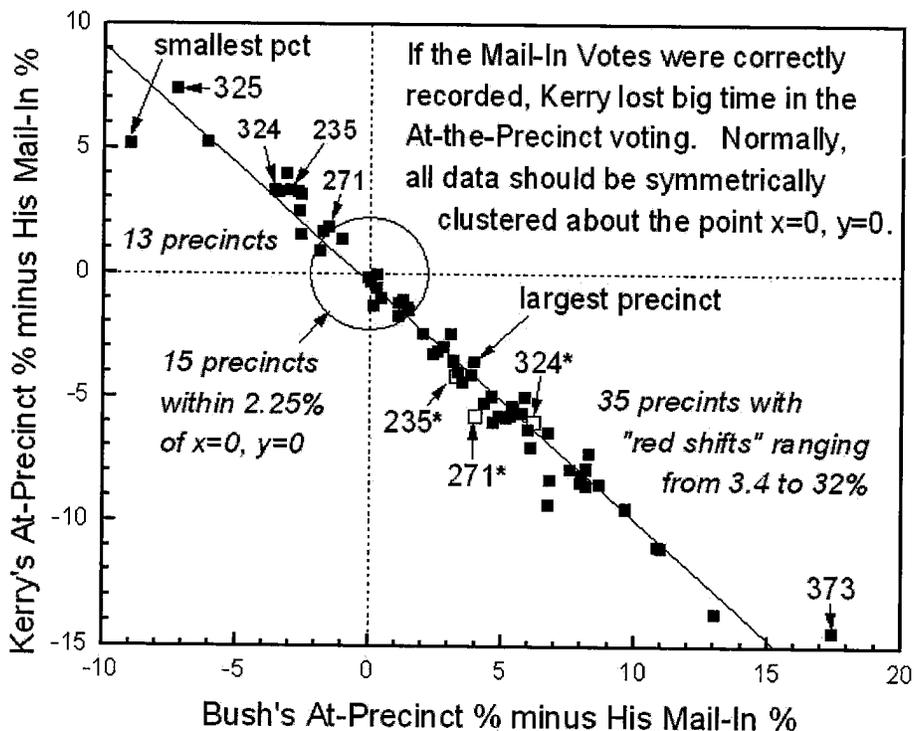
Maybe the motive for hacking the Mail-In votes at Precincts 324, 271, and 325 was pure greed. In the few precincts where they were not Hacking the At-the-Precinct vote (because they were Stacking them), why not hack the Mail-Ins?

No precinct left unHacked.

VII. Another Way to See the Fraud in a Forest of Data

One of the things that I have learned in my 41 years as a research physicist, is that the meaning of one's data is best comprehended – and explained to others – by finding the most telling way(s) to graph them. So, I tried something else with the AZ LD 27 Election-2004 data. It is a very different way to display the same information, one that affords a more dramatic (if not yet statistically analyzed) visual impression of the Election-Day-2004 shenanigans in Pima County, AZ. In Figure 5 I have plotted Kerry's At-the-Precinct vote shares *minus* his Mail-In shares (in percent) on the y axis versus the corresponding subtraction of data for Bush's shares on the x axis.

Figure 5 Election 2004, 63 Precincts of Arizona LD 27:
At-Precinct Presidential Vote Shares Differ Greatly from Early Vote!



Normally one expects the Mail-In vote share to be very close to the At-the-Precinct share for the same presidential candidate, if the precincts are large enough. In AZ LD 27, the two smallest precincts had 87 and 208 voters actually voting and the remainder of the precincts ranged upward from 265 and averaging 952. The 87-voter precinct is indeed an odd fellow, appearing well off the main curve in the upper left quadrant. However, the largest precinct, Pct 185, with 3,453 voters casting ballots, which statistically speaking should have fallen closest to the origin ($x=0$, $y=0$), displays a substantial shift to the lower right – totally unexpected as a random accident.

The fitted curve in Figure 5 is a straight line with slope of -0.98, which is close enough to the expected slope of -1.00 that would pertain when nearly 100% of the votes are divided

between two candidates and there are enough total voters that the laws of average are fully expressed. However, this fit doesn't quite pass through the origin. The magnitude of this displacement to the lower left of the origin could be explained if 0.5% more votes were cast for third-party candidates at the Precinct than was the case for the Mail-Ins. But this explanation is contradicted by Table 1, which shows that *as an LD-wide average* there was only 0.1% more votes for third-party candidates At-the-Precinct than was the case for the Mail-Ins. Even in the absence of statistical calculations, I venture the guess that this discrepancy is yet another indication of the tampering I have already inferred in Section VI.

I believe that when some statistical simulations are finally performed, it will be found that half or more of all LD-27 precincts will fall within an ellipse centered about 0.1% to the lower left of the origin with the semi-major axes of this ellipse extending about 3% to the upper left and lower right along a straight line of slope -1.00. The semi-minor axes of this ellipse would be something like 0.2%.

For purposes of the present discussion, I've placed a circle of radius 2.25 about the origin in Figure 5. It encloses 15 precincts that might be considered "normal" ...except for the fact that only 2 of the enclosed ones are blue shifted, while 13 are red shifted. Outside of this circle there are 13 blue-shifted precincts in the upper left quadrant and 35 red-shifted precincts in the lower right quadrant. And, not only are there **2.7 times more red-shifted precincts** than blue-shifted ones outside the circle, but *the average magnitude of these red shifts is roughly double the average magnitude of the blue-shifted ones.*

While it will be necessary to do some "Monte Carlo" computer simulations to estimate just how improbable these numbers are as random happenstance, such a lopsided outcome certainly has to be extremely rare (I would guess less than one chance in a million). And if the lopsided nature of the data of Figure 5 should be the result of fraud, I infer this fraud was committed mostly against the At-the-Precinct balloting, since Figures 1 and 2 have suggested that the Mail-In votes were accurately counted ...with the exceptions that I will now single out.

Notice that the Precincts that I suspect (or know) were Stacked – numbers 235, 271, and (324) – are mildly blue shifted in Figure 5. I wondered what they might look like if I were to subtract the LD-wide *average* Mail-In shares rather than the actual ones for these precincts (which I suspect were influenced by Hacking). When I did that, all three of these data points became moderately *red* shifted. Then, to improve my accuracy, I corrected the LD-wide-average used in these respective subtractions to take into account the differences in party registration in these three precincts with respect to the LD-wide average registration. This correction actually moved these data points deeper into the lower right quadrant ...to the positions indicated in Figure 5 by hollow squares and labeled with the same precinct numbers followed by asterisks. This exercise seems to confirm that the Mail-In ballot tabulation for Pct 324 was indeed Hacked ...even as the At-the-Precinct ballot box was being Stacked by Rev. Kahn's crew. Furthermore, it also provides an independent form of evidence that Pcts 271 and 325 may also have become

victims of the same double-barreled brand of vote theft as was evidently inflicted on Pct 324.

Finally, out of curiosity, I took a closer look at the data for the two extreme outlier precincts on Figure 5, that is, Pct 325 on the extreme upper left and Pct 373 on the extreme lower right. It turns out that they both had interesting stories to tell.

The Pct 325 polling place was the Pascua Yaqui Tribe Tribal Council Chambers, where I would suppose that many of the 373 voters were Native Americans. In any event, 65.1% were registered Democratic and *only 3.6% were registered Republican*. The official Provisional and At-the-Precinct tallies were respectively 88.5% and 83.4% for Kerry. It was a veritable landslide, with **58.3% of the NOPs joining the Dems in voting for Kerry at the Precinct**. But wait! The official Mail-In count at Pct 325 was just 76.0% for Kerry. This anomalously low value translates into a 10.7% red shift relative to the LD-wide Mail-In average. *And we can infer from these numbers that the NOPs who voted by Mail went 63.1% for Bush!* Do you believe that? If you do, I want you to know that I've marked down the Brooklyn Bridge for quick sale...

As for Pct 373, with its data point way down in the lower right corner of Figure 5, I calculate from the official 2004 Election returns that fully **72.8% of the NOPs voting by Mail-In cast their ballots for Kerry**. But, get this! **62.8% of the NOPs who voted at the Precinct were recorded as voting for Bush!** This is the diametric opposite of the NOP behavior in Pct 325.

Here is a table recapping what I just told you happened on Election Day 2004 at Precincts 325 and 373 (for visual impact, I show only presidential vote shares greater than 50%):

Precinct (polling place)	% NOPs Voting for Candidate	Kerry	Bush
Pct 325 (Yaqui Tribal Council Chambers)	By Mail-In		63.1%
	At the Precinct	58.4%	
Pct 373 (Tucson Independent Church Turning Point School)	By Mail-In	72.8%	
	At the Precinct		62.8%

Was there some difference between the DNA of the Native Americans NOPs at Pct 325 that caused them to go big for Kerry only at the Precinct and the Hispanics NOPs at Pct 373 that caused them to go big for Kerry only by Mail-Ins? (The scientific answer is, no, it would have taken millennia of optional Mail-In voting for natural selection to come into play, and Mail-In voting has only been around for a couple of generations.) No, a far more likely explanation is that the election thieves were unable to gain a foothold in the Yaqui Tribal Council Chambers, so they resorted to stealing only the Mail-Ins at Pct 325. By contrast, down in Pct 373, the "Christian soldiers" of the Tucson Independent Church are likely to have captured most or all of the poll-worker positions at the Precinct, so they Stacked (or Hacked) the At-the-Precinct ballot box and left the Mail-Ins alone.

It is a fact that the polling places of three of the five precincts where I have found startling skewing of the votes from normal expectation have been two churches and a church school, while a fourth one (at a public school) had a reverend and his wife as the

head pole workers. This may not be accidental. Both John Brakey and Mark Crispin Miller have done extensive research revealing the involvement of legions of Christian zealots in the campaign to steal Elections 2004, and 2006, and 2008...

VIII. The Pima County Democratic Party's Suit against Pima County

One wonders if John Brakey ever sleeps. Last year John decided to teach himself the "geek Greek" of the Diebold GEMS central tabulator. To do this he got the State Democratic Party to bring in one of the best election geeks in the Country, Jim March. Jim is an experienced computer tech specialist with 17 years in the IT industry. In 2003 he first heard of Bev Harris' work exposing problems with the Diebold voting systems as used in Pima County, and he began helping Ms. Harris analyze the 40,000 files she had obtained from a Diebold website lacking any security. Jim was lead plaintiff (along with Ms. Harris) in a California consumer protection suit against Diebold netting that state a \$2.6 million refund, and he now sits on the board of directors of Black Box Voting, a national non-profit. He was brought to Pima by the State Democratic Party to help monitor the primaries and General Elections and is currently a tech consultant on the public records lawsuits fought by the county as part of the aftermath.

By Freedom of Information Act (FOIA) requests, John obtained the computer logs of the Pima County tabulators for the past several years. He quickly discovered that ever since the arrival of Brad Nelson as the Pima County Director of Elections, someone at the Elections Department has been printing summary reports of Mail-In ballots counts up to a week or more before the election. This is strictly illegal under Arizona law: "...there shall be no preferential counting of ballots for the purpose of projecting the outcome of the election." And, obviously, anyone in possession of such information would have highly accurate advance information to calibrate any Trojan Horses present in the At-the-Precinct 1.94w memory cards so as to infallibly flip sufficient votes to change the outcome of a race on Election Day without causing undue suspicion by overdoing it.

Although merely printing illegal summary reports of early balloting is not prima-facie evidence of election fraud, on 1 February 2007 the Pima County Democratic Party filed a (civil) public records lawsuit in Pima County Superior Court against the Pima County Board of Supervisors and the County Treasurer seeking the production of summary reports of early ballots that were printed without election observers present and allegedly sealed in the Pima County Treasurer's vault [10].

Then John spotted something else. Back in 2006 there was a ballot initiative to impose a half-cent sales tax to pay for a 20-year, \$2 *billion* Regional Transportation Authority plan ultimately approved at the same election. After the first day's Mail-In returns, the computer operator had backed up the election and the very next morning backed it up again, whereupon he immediately printed another summary report. John recognized instantly that the operator had it within his power to take home a copy of the first day's voting, alter it using Microsoft Access (for example to flip votes in the event that the RTA tax was being rejected) and then save this altered version the next morning. (Thus,

the purpose of the new summary report might have been to assure that the manipulations he had inserted had actually “stuck”).

Enter Attorney and Democratic activist William J. (Bill) Risner. As an “officer of the court” bound to report any evidence of possible criminal activity that comes to his attention, Bill immediately filed a criminal complaint with the AZ Attorney General. In response, the Pima County Board of Supervisors immediately went to court asking for a stay on civil case until the civil case is settled. However, a judge recently ruled in favor of Bill Risner’s arguments that the civil and criminal cases are not barred by law from proceeding separately. And another piece of good news is that the local media have not shied from reporting this story [11, 12].

Still, John Brakey and Bill Risner, so far as I know, haven’t been paid a red cent for their efforts or court costs, even by the Democratic Party.

XI. The Author’s Thoughts about All of This

For the most part, in this article I have been clinically dispassionate ...as though I were writing just another scientific paper. On occasion I have been flip and have made a bit of black humor, though this has been just an artifice to hold the reader’s attention. In the end, as I reread what I’ve written, I keep returning to the thought of the 60,000 Americans from all walks of life and ethnic heritages belonging to Arizona Legislative District 27 who turned out on Election Day 2004 to exercise their constitutional right to “throw the bum out.” What happened to these Tucsonans that day is surely a microcosm of what was simultaneously happening to Americans all across our country. I reflect on the facts that not only were these good folks’ wills – and their inalienable rights – subverted, but they are not even told by the mainstream media what was done to them. So they have no choice but to blame themselves for “the bum” still being at the helm ...still driving Titanic America toward the not-too-distant icebergs, full speed ahead. And all the while, the evil ones who contrived this heinous crime against our Republic go about consolidating their power and wealth and pursuing their illegal wars at the expense of the good people they stealthily disenfranchise.

The words that best describe my feelings leapt from the title of a book by Alan Paton:

“Cry, the Beloved Country.”

References

[1] [http://www.drivehq.com/file/df.aspx/publish/dlgriscom/Election Fraud Research/Griscom_AAAS 2007 Annual Mtg.ppt](http://www.drivehq.com/file/df.aspx/publish/dlgriscom/Election%20Fraud%20Research/Griscom_AAAS%202007%20Annual%20Mtg.ppt).

[2] www.bbvforums.org/cgi-bin/forums/board-auth.cgi?file=/1954/15595.html

[3]

www.votetrustusa.org/index.php?option=com_content&task=view&id=798&Itemid=51

- [4] http://www.opednews.com/articles/opedne_michael_070313_the_long_road_to_dem.htm
- [5] http://www.rollingstone.com/news/story/10432334/was_the_2004_election_stolen
- [6] <http://www.scoop.co.nz/stories/HL0706/S00164.htm>
- [7] http://electiondefensealliance.org/landslide_denied_exit_polls_vs_vote_count_2006
- [8] <http://www.votersunite.org/info/PeeringThruChinks.pdf>
- [9] <http://freepress.org/departments/display/19/2004/957>
- [10] <http://www.tucsonweekly.com/gbase/Currents/Content?oid=92557>
- [11] <http://www.azstarnet.com/dailystar/184860>
- [12] <http://www.tucsoncitizen.com/daily/opinion/53903>

ver. 4.5

From: Julie Penny
Sent: Thursday, August 02, 2007 10:33 AM
To: Voting Systems
Subject: Top to Bottom Review of Voting Systems

Julie Penny

August 2, 2007
RE: Top to Bottom Review of Voting Systems

Debra Bowen, Secretary of State
State of California

Dear Ms. Bowen,

As someone who used to live in California, and who will retire there (our grown children are there and I urged them to vote for you to guarantee we would have clean elections) I want to thank you for conducting this review which was long overdue. We are grateful for you having conducted this review as the voting issue is the bedrock of our democracy.

I have cut and pasted here the NYC Council's Res. 961 which they introduced last week **calling upon the NY State Board of Elections to develop their own optical scan system like Oklahoma did, or to accept a free 100% open-source optical scan system from citizens who have developed it.**

Apparently, Oklahoma has not had any problems like the rest of the country has had with their own system.

Time to throw out the vendors with their secret proprietary software and save taxpayers with California's own State-owned and run system that's transparent and cheap.

As the old 60's motto went: "Power to the People:"

New York City Council's

Res. No. 961

Resolution urging the New York State Board of Elections to promptly commission the development of a Precinct Based Optical Scan voting system that would comply with New York State voting system standards, which would be owned entirely by the State of New York and would be certified for use by the county Boards of Elections and by the Board of Elections in the City of New York.

08/02/2007

By Council Members Mealy, Jackson, James, Foster, Gerson, White Jr., Monserrate, Addabbo Jr., Avella, Gentile, Koppell, Liu, Mark-Viverito, Mendez, Palma, Reyna, Sanders Jr., Seabrook, Vann, Martinez and Vacca

Whereas, Public confidence in the outcome of elections depends, in part, on the use of voting equipment that is under full public control and not under the control of private corporations, which have no responsibility or accountability to the public; and

Whereas, In 2005, the New York State Legislature enacted the Election Reform and Modernization Act (ERMA) in order to comply with the Federal Help America Vote Act of 2002 (HAVA), ERMA requires county boards of election to select new voting technology to replace the currently used mechanical lever machines; and

Whereas, Many computer technologists urge that all software in any voting or vote-tabulating system be Open Source Software; and

Whereas, Open Source Software is software that: (i) is freely available for any member of the public to read and evaluate, free of charge; (ii) is easy to obtain, (iii) can be copied, used, modified, and distributed but not sold; and (iv) the open source voting system is currently in development by citizens eager to provide an alternative to commercially produced voting systems; and

Whereas, The use of Open Source Software has not been possible to date in New York State because all of the private manufacturers and vendors of the computerized voting equipment that may ultimately be certified for purchase by New York counties require certain protections for their software in their contracts of sale that prevent the public from being able to freely read and critique the software; and

Whereas, In addition, these private manufacturers and vendors require on-going payment for the use of their equipment, which in some cases can double the purchase cost of equipment within a few years of purchase; and

Whereas, These private manufacturers and vendors have had multiple problems, including delivery of non-working equipment, a history of high equipment failure rates, and legal disputes with jurisdictions in which the vendors have claimed ownership of voting data after the jurisdictions purchased and used their equipment; and

Whereas, New York has two alternatives to the purchase of Precinct Based Optical Scan (“PBOS”) voting systems with “secret” software from private manufacturers and vendors: (1) New York could commission the development of a PBOS system to be used throughout the state, or (2) New York could accept a free, completely Open Source system that runs on Commercial-off-the-Shelf (“COTS”) laptops, scanners, and printers; and

Whereas, New York State could follow a model similar to that of Oklahoma, which in the early 1990’s purchased hardware and full ownership and control of the software source code for an optical scanner voting system; Oklahoma freely revised and modified the software to develop a statewide optical scanner system perfectly tailored for Oklahoma’s needs, and now has an optical scanner system completely under Oklahoma’s control; and

Whereas, Certain American companies and individual machine-vision system consultants are very experienced in developing custom machine-vision and document processing systems similar to what New York State would need to commission in order to develop an open source PBOS voting system; and

Whereas, Some of the advantages to New York State of commissioning the development of an optical scanner voting system include: (1) the programming code could be designed and implemented using currently-accepted professional standards, thereby enabling New York to avoid the use of equipment with programming that has been criticized for poor design and security flaws, (2) there would be substantial initial and continuing cost savings because there would be no annual recurring payments to vendors for use of equipment or software already delivered, (3) the system could be customized specifically for New York State’s requirements by using COTS hardware programmed to provide all necessary functions and customized to omit functions that are not wanted, and (4) the people of the State

of New York would have complete control over the voting process and the State would be free of dependence on any manufacturer and/or vendor; and

Whereas, An open source optical scanning system already exists and according to Richard C. Johnson, CEO of Open Voting Solutions, a final completed system could be prepared and submitted for testing at an estimated cost of under \$200,000, which would enable the New York State Board of Elections to evaluate the system when the State resumes testing of other voting systems under consideration for certification; and

Whereas, Due to various delays, New York State may not begin to use new voting equipment until the 2009 elections, which would allow sufficient time for the completion of testing and certification of New York State's PBOS voting system; now therefore, be it

Resolved, That the Council of the City of New York urges the New York State Board of Elections to promptly commission the development of a Precinct Based Optical Scan voting system that would comply with New York State voting system standards, which would be owned entirely by the State of New York and would be certified for use by the county Boards of Elections and by the Board of Elections in the City of New York.

Sincerely,

Julie Penny

From: Kathleen Wynne
Sent: Thursday, August 02, 2007 9:49 AM
To: Voting Systems
Subject: TEXANS SUPPORT YOU AND THANK YOU!

Dear Secretary Bowen,

My name is Kathleen Wynne and I am the former Associate Director of Black Box Voting.org. As you recall, Black Box Voting has been an avid supporter of your efforts in election reform when you were State Senator and now in your role as Secretary of State of California.

I presently live in Austin, Texas and have continued working in election reform with Black Box Voting and with VoteRescue of Austin.

The reason I am writing to you is to add my voice to all the other grateful citizens, who have also sent e-mails of praise and support for your recent "Top to Bottom Review of E-Voting Systems Certified in California". Your courage in taking on the election industry on behalf of the American people is not only laudable, it will be remembered in the history books.

In order to continue moving forward in protecting the integrity of our elections and setting a precedent for the rest of the country to follow, I strongly urge you to defy the critics, who serve the vendors's best interest, and not the citizens', and immediately "decertify" these machines and send a message that will resonate across the country that all of these machines should be recalled and we must return to "citizen-controlled" elections.

You may be the SOS of California, but you represent the best interests of citizens in all the other states by your courageous actions. The "Texans For Real Elections Coalition" stand ready to support you in any way we can. Stay the course and change the course of history.

My sincere thanks to you for what you are doing on behalf of fair and honest elections and the very survival of our republic.

God speed, Secretary Bowen!

Sincerely,

Kathleen Wynne
Former Associate Director - Black Box Voting.org
Founder HCPBnow.org
Member VoteRescue.org - Austin, Texas
Member - VoteRes

Be a better Globetrotter. [Get better travel answers](#) from someone who knows.
Yahoo! Answers - Check it out.

08/02/2007

From: Tom Courbat
Sent: Wednesday, August 01, 2007 11:51 PM
To: Voting Systems
Cc:

Subject: Riverside County "Blue Ribbon Committee" Report/Testimony
Importance: High

Dear Honorable Madam Secretary,

It just occurred to me that perhaps the official report of the Elections Review Committee (aka "Blue Ribbon Committee"), submitted to the Riverside County Board of Supervisors on July 17, 2007 may not have been submitted as a testimony document for your consideration. I understand that documents submitted by August 1, 2007 will be considered in your final decision regarding e-voting systems' certification status.

The Blue Ribbon Committee (BRC) was appointed by the Riverside County Chairman of the Board, Bob Buster in December 2006 to address a wide-ranging array of issues related to election administration in Riverside County. The committee consisted of two retired judges, a retired 16-year member of the Board of Supervisors and former president of CSAC, the former editor/publisher of the Press Enterprise (the largest circulation newspaper in Riverside County) and the president of a local chamber of commerce.

I have attached the executive summary and their 17 recommendations. The full report is 3.8 MB and will be emailed to you under separate cover, to ensure that the "meat" of the report is received by your office prior to the end of this day.

The #1 recommendation of the BRC is: "Move as quickly as possible to a hybrid voting system whereby able-bodied voters mark their preferences on paper ballots which are then counted by optical scanners." In other words, do not use DRE touchscreens except possibly for non-able-bodied individuals.

One of the key reasons the BRC stated for moving to a paper-based balloting system was this statement:

"As one expert put it, a paper ballot is "macroscopic." The voter can see it. The voter doesn't need a machine to read it. This provides true transparency. The voter knows the vote he/she marked is the vote that was cast and is the vote that will be used in an audit or recount. This promotes public confidence."

You have repeatedly emphasized the importance of transparency in government. The DRE touchscreens do NOT provide for transparency, in fact, just the opposite. Secrecy and opportunities for manipulation abound.

Thank you for considering the findings and recommendations of the BRC. This highly-respected committee spent over six months researching and taking public testimony, including expert testimony from Mr. Harri Hursti and Mr. David Jefferson, among others.

Best regards,

Tom Courbat
SAVE R VOTE

08/02/2007

951-677-6451

Full report to follow via email.

The degree of willingness of a government to open itself up to public scrutiny and public audit foretells the quality and integrity of that government.

**SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**



FROM: Elections Review Committee

SUBMITTAL DATE:
July 11, 2007

SUBJECT: Report on the November 2006 Election

RECOMMENDED MOTION: That the Board of Supervisors receive and file the attached report, and schedule discussion of this and other election issues at a September Board workshop.

BACKGROUND: On December 12, 2006, Chairman Bob Buster directed formation of an ad hoc Blue-Ribbon panel to review issues arising from the November election. . . Five county residents – Lynn Baldi, Kay Cenicerros, Marcia McQuern, Rob Taylor and Jim Ward – were appointed to the panel. They met several times, and issued an interim report to the Board on April 24.

Since that time, the committee has held several study sessions, and consulted with the office of the Secretary of State. The Secretary of State is currently testing the electronic voting system used in Riverside and is expected to issue an opinion early next month. The attached report recommends that the county “transition away from the current voting system as soon as practical and move to a hybrid voting system...” subject to the Secretary of State’s review.

A Board workshop with the Registrar of Voters has been tentatively scheduled for ^{Monday} September 17th

Kathryn Field
Kathryn Field, Principal Management Analyst

FINANCIAL DATA	Current F.Y. Total Cost:	\$ 0	In Current Year Budget:	n/a
	Current F.Y. Net County Cost:	\$ 0	Budget Adjustment:	n/a
	Annual Net County Cost:	\$ 0	For Fiscal Year:	n/a

SOURCE OF FUNDS: n/a	Positions To Be Deleted Per A-30	<input type="checkbox"/>
	Requires 4/5 Vote	<input type="checkbox"/>

C.E.O. RECOMMENDATION: APPROVE
BY: *Kenneth M. Mohr*
Kenneth M. Mohr
County Executive Office Signature

Dep't Recomm.: Consent Policy
Per Exec. Ofc.: Consent Policy

Prev. Agn. Ref.: 3.11 of 4/24/07 | **District:** all | **Agenda Number:**

3.25

July 7, 2007

Chairman John Tavaglione
Supervisor Bob Buster
Supervisor Jeff Stone
Supervisor Roy Wilson
Supervisor Marion Ashley

Re: Election Review Committee

Dear Chairman Tavaglione and
Members of the Board,

Our Election Review Committee (ERC) has met fifteen times including an organizational meeting on January 31. Since our formation we have held three noticed formal public hearings (totaling almost nine hours); four meetings with the Registrar of Voters, including a presentation by Sequoia Services; one meeting to update the Board of Supervisors on our progress, and three group study and writing meetings.

Our committee has spent many hours of research into the benefits and problems with electronic voting. Our committee has also researched the experience of several California counties, notably Alameda County, which has created a hybrid system which allows voters to vote using paper ballots using optical scanners to create a record.

It is not possible to accurately assign motives to the public for casting paper ballots at polling places; through absentee votes, or through electronic record. We do know that 40-43% of voters in Riverside County cast paper ballots. The increasingly large minority vote for paper ballots does suggest, however, an ongoing trend. We certainly recognize the influence of long commutes which shorten the opportunity to vote on Election Day, as noted by long lines of voters at some election sites in Riverside County.

The Election Review Committee has also studied the benefits of Riverside County's Sequoia System as a major election tool. Widely used and lauded just a few years ago, concerns with electronic voting, including its 3% error rate, have led to extensive discussion. These issues are of concern to our committee and to county voters, many of whom are concerned.

A summary of recommendations will be readied by July 9 for your packet for the July 17 meeting of the Board of Supervisors.

Sincerely,


Kay Cenicerros, Chairman

Election Review Committee
Corrected Report
to the
Riverside County Board of Supervisors
July 17, 2007

The Charge

In the wake of complaints about the conduct of the November 2006 elections, the chairman of the Riverside County Board of Supervisors appointed an Election Review Committee to study “problems arising from the recent election.”

Committee members are Lynn Bogh Baldi, board member and former president of the Beaumont Chamber of Commerce and of The Community Foundation; Kay Cenicerros, retired Riverside County Supervisor and retired dean of Mt. San Jacinto College; Marcia McQuern, former editor and publisher of The Press-Enterprise; Robert Gregory Taylor, retired Superior Court judge; James Ward, retired state appellate court justice; Mrs. Cenicerros was selected chairman of the committee.

Their charge was to “broadly review the election” including voting and counting efficiency; security; delays for voters at the polls; problems with voting machines; training and deployment of poll workers; timely mailing of absentee ballots; other factors impeding the count of absentee, paper and provisional ballots; the official posting of results at polling places; and appropriate election observer access.

Executive Summary

The committee concludes that while there were many problems and frustrations with the November 2006 election, Riverside County voters’ intentions were not compromised.

The Registrar of Voters already has addressed many of the security and transparency problems noted during the committee’s review.

The committee unanimously makes the following additional recommendations:

1. Move as quickly as possible to a hybrid voting system whereby able-bodied voters mark their preferences on paper ballots which are then counted by optical scanners. *See explanation below.*
2. Place a prominent sign at every voting site letting voters know they are entitled to cast a paper ballot if they would rather not use an electronic voting machine.
3. Do not provide extraordinary absentee ballot pickup measures for some voters or communities that are not provided for all.
4. Reduce as much as possible the time lag between removal of voting machines from the Registrar of Voters’ warehouse and their Election Day use. Secure voting machines delivered to voting locations behind locked doors until Election Day.
5. Better educate the public on the process for casting absentee ballots, particularly when they must be mailed back and on the permissibility of polling place delivery on Election Day.

6. Implement the Secretary of State's requirements for an Election Observer Panel in a timely manner. Appointers should be encouraged to rotate members at least biennially to broadly acquaint the public with the election process.
7. Designate at least one private voting booth at every voting site for casting of paper ballots.
8. Severely restrict physical access to the tabulating room, as allowed by Election Code 15204.
9. Provide a more transparent and secure post-election one-percent manual count by making public the process for randomly selecting the precincts to be checked (including perhaps posting on the web), giving proper notice of the selection time and reducing as much as possible the length of time between the selection of precincts for the manual count and the start of the audit.
10. Install video cameras to record activity in all areas of the central tabulating room with displays of each camera's view in a public room.
11. Verify that election results are posted at every voting location.
12. Recruit Election Day workers aggressively and train them well ahead of elections. Public advertisements including in utility bills, fliers, and invitations at senior centers should be considered, as well as public recognition for workers' service.
13. Take advantage of the city clerks' willingness to help find polling places, recruit poll workers and even be trained to change voting machine paper.
14. Consider formal agreements between the county and each city on election services that the county will provide, including how the charges for such services are calculated.
15. Hold quarterly meetings between the Registrar of Voters and city clerks, including a post-mortem meeting after every election.
16. Provide a forum for public input on election issues hosted by the Registrar of Voters at least annually.
17. Consider hiring a consultant to review the Registrar of Voters security procedures.

Secretary Bowen, Deputy Secretary Finley,

I am Jerry Berkman, a retired computer programmer at U.C. Berkeley, with an interest in and a certification in computer security earned from the SANS Institute [sans] in 2003.

Thanks you very much for performing the Top-To-Bottom Review of Voting Systems. It was much overdue.

1. Beliefs vs. Reality

The registrars, vendors, and supporters of the DRE election systems have beliefs which seem to me to not be based on reality. Part of the problem is that the supporters seem to feel we need only to defend against amateur attacks. If someone wants to fix a Gubernatorial race, or U.S. Senate race, they will probably have millions to spend, and be able to hire real talent, not amateurs.

1.a. They believe that you can depend on elections officials and elections workers.

But:

- Two election workers in Cleveland are now in jail for altering a recount; [Vu]

- Their supervisor, Michael Vu, is now Assistant Registrar of Voters in San Diego County. He either must have been complicit or clueless. Either way, would you want him in charge of counting your vote? [Vu]

- The former ROV of Monterey County, Tony Anchundo, is now in jail for 43 charges of forgery, misapplication of funds, embezzlement, falsification of accounts, and grand theft of nearly \$80,000 of County money. [Anchundo]

- San Diego Registrar Deborah Seiler gave misleading testimony yesterday in the public hearing, claiming the Top-To-Bottom review was a patch work picking only a few of the systems to test and if a system failed the tests, the County may use an untested less secure system. [Seiler] In fact, all current systems which will be used in the future in California by any but the smallest counties are being tested. [ttbrinc] Why is she misleading us?

- Los Angeles Registrar Connie McCormack said to the Los Angeles Times:

"All of us have made changes to our software - even major changes - and none of us have gone back to the secretary of state. But it was no secret we've been doing this all along." [connie]

1.b. The illusion that you can depend on vendors.

But:

- Diebold was decertified in 2004 due to installing unauthorized patches without notifying the Secretary of State,
- the reports mention many things which do not work as documented,
- security vulnerabilities such as hard coded passwords and vulnerabilities to election databases have been

documented for years and not been fixed [cert],
 - using Windows as a base platform calls into question the vendors committment to security.
 - the reports mention undisclosed logins without passwords on the systems,

1.c. The supporters claim the red-team testing was unreasonable because hackers wouldn't have access to systems for that long a time.

But:

- Researchers have been able to buy Diebold and Sequoia machines on Ebay.
 [ebay]

- Machines can and have been stolen, e.g. six Diebold tabulation machines and a touch-screen voting terminal were stolen from a Ramada Inn in Macon Georgia in June, 2002. It took Kathy Rogers, head of the Georgia election division, two years until Sep. 2004 before she would acknowledge the theft. Kathy Rogers is now a division head, and wrote the Diebold statement presented at the public hearing Monday.
 [macon]

- Machines are lost; e.g. there are reports of machines turning up in strange places after elections.
 [strange]

Does anyone really think that organized crime could not get a few DREs and tabulators?

1.d. The supporters claim the red-team testing was unreasonable because hackers and others can't get the source code.

- The Diebold source code was found unprotected on the Web.
 - It is quite possible someone could hack the vendors network and get the source code.
 - Social engineering, bribing a vendor programmer, or bribing someone for a copy of the daily backup tapes may work.

If Los Alamos can't control it's classified computer programs, why do we believe Diebold, Sequoia, and Hart InterCivic can?

1.e. The supporters claim these are well tested systems.

But:

- The ITAs test functionality, not security[summit].
 - Each report commissioned to look at the security of the systems has found more and more vulnerabilities [reports]
 - The ITA testing system has been found to be lacking with Ciber, a major ITA, being denied initial accreditation by the EAC.
 - Many parts of the source code which were supposed to be examined by the ITAs were withheld by the vendors, e.g. Windows CE being called COTS.

1.f. The supporters believe if a system hasn't been proven to be hacked, then it is secure.

This has proven false with:

- Kryptonite locks for bicycles; once regarded as the ultimate in security, but easily opened with a bic pen.
- Door locks: easily opened with "bump" keys available on the Internet.
- RFID keys for cars: these can be bypassed by a series of pulls on the emergency brake.

2. The Current Situation

Currently, the systems:

- The systems are not secure.
 - The systems are not HAVA compliant.
 - The systems are not California Elections Code compliant.
 - The vendor resist any attempts at oversight.
 - The vendors act in a half hearted manner to address these issues, e.g.:
 - Diebold building voting terminal stands which are too narrow, only 19" wide, when the VVSG calls for 30" wide. Even without the VVSG, 19" is obviously too narrow.
 - None of the vendors show evidence of using modern security practices such as designing in security from the beginning, never using hardcoded passwords, always validating input, etc.
 - The systems keep changing, forcing ROVs to keep upgrading their systems.
 - The systems are very expensive compared to optical scan systems.
 - Each election, there are new problems, e.g. Sarasota's 18% undervote, Charlotte County, Florida's 25% undervote, minority undervotes, etc. The system needs simplifying.
- another Florida's

A big problem is that there is not enough money in the election systems market to cause the vendors to react and fix the problems, or for new vendors to emerge.

Another big problem is the vendors development timetables.

According to the Elections Technology Council, [etcouncil] the timeline for a minor software change to a voting system is 18 months,

- for a minor hardware change to a voting system: 24 months,
- for a major software change to a voting system: 36 months,
- for a major hardware change to a voting system: 42 months,
- for a new product to a voting system: 54 months.

These are too long. In fact, it has taken Diebold 1 and 1/2 years to fix the problems found in the previous Secretary's term, and the new system is still not certified.

3. Conclusions

To keep doing what we are doing, and expect better results has been called the definition of insanity.

Decertify immediately any system not reviewed.

Decertify all the systems with DREs. Recertify with stringent conditions the DREs for 2008 only to be used primarily for accessibility, with a maximum of one DRE per polling place.

Other states, such as New Mexico, have made this switch quickly. And, in fact, the undervotes for minority communities plummeted after the switch in New Mexico!

The optical scanners also have many problems; recertify them

or switch to hand counting. The February, 2008 primary could easily be counted via hand, as there will be only one partisan race plus, possibly, a few initiatives.

The HART system should be recertified only if they provide the withheld software components.

Require as part of the recertification, unfettered observation by the public. SOVCs should be posted in usable formats on the web. All central servers should have their event logs posted on the web.

4. Miscellaneous

Many of the Registrars are trying to count votes as the voters intended. However, that is not in the Elections Code. It should be amended to fix that.

The Elections Code allows a maximum of 5 minutes time in the booth with a DRE, 10 minutes otherwise. The accessibility report showed about 10 minutes average for visual usage, 20-40 for audio usage. The Elections Code should be amended.

The accessibility report stated there is a need for better privacy. This is true for all voters. There should be curtains around the booths.

[sans]

<http://www.sans.org>

[Vu]

http://www.nctimes.com/articles/2007/04/12/news/sandiego/5_02_564_11_07.txt

[Anchundo]

<http://www.bradblog.com/?p=3937>

BradBlog: "Monterey County, CA, Registrar Tony Anchundo Pleads 'No Contest' To 43 Criminal Charges"

[Seiler] Testimony during TTBR Public Hearing, July 30, 2007

[ttbrinc]

"Frequently Asked Questions"

Top-To-Bottom Review FAQ, July 2, 2007

http://www.sos.ca.gov/elections/voting_systems/ttbr/ttbr_faq_final070207.pdf

[connie]The McCormack quote is cited on several web pages, including:

Kim Alexander:

<http://www.calvoter.org/issues/votingtech/pub/0707KACOMremarks.html>

Doug Jones:

<http://www.cs.uiowa.edu/~jones/voting/nist2003.html>

ACM Risks:

<http://catless.ncl.ac.uk/Risks/23.03.html>

LA City Beat:

<http://www.lacitybeat.com/article.php?id=863&IssueNum=47>

[cert]

Gems Central Tabulator 1.17.7, 1.18, August 31, 2004

<http://www.us-cert.gov/cas/bulletins/SB04-252.html#diebold>

[ebay]

<http://www.bbvforums.org/cgi-bin/forums/board-auth.cgi?file=/8/46561.html>,

Lou Dobs: http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1673

Sequoia: <http://earc.berkeley.edu/news/2007/June/KeepingAnEye.php>

[macon] "Steal This Vote", Andrew Gumbel, 2005, pages 235-236.

[strange] USA Today, "Mysterious touchscreen voting machine found", 9/29/04,
<http://www.usatoday.com/tech/news/techpolicy/evoting/2004-09-29-abandoned-diebold-ma>

[summit]

Remarks of ITA testers and other panelists at the Secretary of State's Voting Systems Testing Summit, November 28-29, 2005, Sacramento, CA.

[reports]

These include the SAIC, RABA, CompuWare, and Berkeley reports. A major exception is the Alameda County report; but the report was done without examining the source code and without testing the machines.

[etcouncil]

Elections Technology Comments on HAVA Amendments, page 10.
<http://www.electiontech.org/news/HelpAmericaVoteActAmendmentsFINAL.pdf>

E-VOTING TOP TO BOTTOM REVIEW COMMENTS

Below I have listed a number of issues which should be included in the Secretary of State Election Division monitoring policies covering Electronic Voting machines.

1. Incident Report Forms and RoV Record Keeping:

- A. Forms to be filled out by every voter who has experienced a problem (re.: incident) while voting
- B. Forms to be made available at every polling (voting) site in California
- C. 20 to 50 forms at each site
- D. Forms to be sequentially numbered and accounted for by each county RoV
- E. One copy goes to the voter, one copy to the RoV, and one copy to the SoS
- F. A detailed posting of every incident report must be posted on the Internet 36 hours after the close of the election
- G. Each county RoV office must maintain and report a detailed record of all incidents and reports filled out and submit their records to the SoS after each election.

2. Election Day "Tech Inspections" of all Electronic Voting Equipment

- A. Tech Inspection based on the NASCAR Race Day tech inspection model
- B. Prior to opening of the polling sites, on election day, copies must be made ("burnt") of all harddrives, memories, and any and all CD's, and other removeable storage devices(memory cards, flash cards, memory sticks, etc) inserted into any electronic voting equipment, prior to, during and after the election. This includes a copy of the election ballot software used to prepare all the equipment for the election, This includes, but is not limited to all equipment used at county central tabulating headquarters and each and every polling site, in each county. This also includes, and is not limited to all DRE's, PBR (polling place ballot recorders) and any and all electronic equipment used to read, store, and record ballots and votes, used at every polling site and includes all software, codes, and programs used to conduct, run, and carry out all election functions electronically.
- C. The same procedure must be repeated after the close of the voting, and at the close of the tabulating done at the central tabulating location.
- D. All digital copies are to be reviewed, inspected, and analyzed by certified and SoS approved software experts, and compared to all software copies held in escrow.
- E. All the inspections and digital/electronic copying is to be conducted by SoS approved and certified Computer Sciences technology specialists
- F. All personnel costs of the specialists are to be born by each county
- G. Certified specialists must be on location at all times prior to the start of voting all through the completion of the Central Tabulation process

3. Polling Site Electronic Voting Equipment

- A. If it is financially and logistically impossible to comply with a NASCAR Race Day Tech Inspection model on polling site electronic voting equipment, then no such types of equipment can be used at the polling sites.
- B. All voting must be done by hand marked paper ballots.

- C. All ballots must be hand counted
 - D. At each polling site, upon completion of vote tabulation, the totals for that particular polling site are to be posted outside the polling site, visible to the public. All the individual polling site totals are to be posted on the Internet within 24 hours after the close of voting.
 - E. HAVA exempts a jurisdiction from using an electronic overvote and under-vote notification device if that jurisdiction uses a paper ballot voting system. See HAVA Title III, Subtitle A, Section 301, 42 USC 15481, (a) , (1), (B)
- 4. Disqualification Standards and Conditions**
Based on the NASCAR Race Day Tech Inspection Model
- A. If the State certified and appointed tech inspectors are prevented in any way from inspecting, analyzing, and reviewing any part of the software, firmware, and hardware covered in Section 2.
 - B. If there is any difference from the software held in escrow and the software in use.
 - C. Any violations of State Election Codes
 - D. Other
- 5. Seizure of Malfunctioning Touchscreen DRE's**
- A. SoS mandates that any Touchscreen DRE be immediately removed from use/service during the election when that specific touchscreen has been reported to polling site workers as having changed the voter's vote selection
 - B. A full and detailed statement and incident form is to be completed by the voter and the polling site captain, including the serial number of the touchscreen.
 - C. The polling site captain is to personally contact the SoS, and report the touchscreen incident immediately upon notification by the voter.
 - D. The voter is to be instructed by the polling site captain to call the SoS touchscreen problem specific hotline and report the incident as well
 - E. SoS is to set up a special, dedicated phone line for this specific problem only
 - F. The problem touchscreen is to be shipped within 24 hours directly to the SoS in Sacramento.
 - G. The problem touchscreen cannot be touched by county IT personnel at any time.
 - H. The problem touchscreen is to be treated as evidence in a felony vote tampering investigation.
 - I. SOS is to launch a felony vote tampering investigation of each and every instance of touchscreen vote switching
 - J. The same standards and conditions apply when a DRE switches (changes) a voter's vote selection

Sincerely
MARC KEENBERG

DEBUNKING the RoVs' IT SECURITY CLAIMS:

At the Monday, July 30 Secretary of State hearing on the SoS E-Voting Top to Bottom Review, there was much testimony and claims made by various IT "chiefs" from numerous Registrar of Voters departments from throughout California. These IT "experts" made repeated and strenuous statements that their electronic voting equipment could not possibly be hacked and altered due to the fact that they employed and utilized anti virus and anti spyware programs. Furthering support of their security procedures, they stated that they frequently updated their Microsoft, and anti-virus and anti-spyware programs, which, in their minds guaranteed that they have made it impossible to hack into their equipment and cause potential damage to the integrity of the elections. Assured of their own impregnable security measures, these IT gurus were convinced of their ingenious defense tools. And they tried to convince the SoS and the public that they actually knew what they are doing.

However, there are major flaws, inaccuracies, and deceptions inherent in their claims of security knowledge and measures. To begin with, these IT "chiefs" all stated that their Electronic Voting Equipment is **NOT** connected to the internet, so it cannot be hacked into. If this is true, how do they receive and install their Microsoft, anti-virus, and anti spyware updates? It is impossible to update these programs without being connected to the internet. In order to receive the correct updates, the program's home site must first read your computer to find out what you need to receive. Second, the updates are sent into your computer through the internet. If what they say is true, that they do update these programs, then their e-voting equipment is at times connected to the internet. Do they have firewalls on their equipment? When their equipment is connected to the internet, does the e-voting software "call" home? One would merely look at the firewall's logs to see that, if they use a firewall. And do these IT "experts", so obsessed as they are with security, even bother to find out who their e-voting equipment is contacting when connected to the internet while updating their security programs? And, how do they update their software on the DRE's and PBR and other polling site equipment? Do they connect these to the internet as well?

Further demonstrating their complete and total lack of knowledge of how anti-virus and anti-spyware programs work, these IT "experts" proudly proclaimed that these programs would prevent any intrusions and virus and malware insertions into their equipment. Well, these security programs use a data base of known and identified malware programs for the detection and prevention applications. If a program is not in their known data base, these programs will not detect it. As any program which would be used to alter and/or manipulate the vote tabulation and count records of an e-voting machine would be very precisely use specific, it would be a program not ever used on any other computer other than an e-voting computer. Consequently, any vote altering program would not be exposed into the electronic environment from which the anti-virus and antispyware programs use as a data bank. Therefore, the anti-spyware and anti-virus programs are next to useless in preventing a use specific vote altering program. As further evidence of their complete and total lack of understanding the security involved in e-voting equipment, these IT "experts" never once mentioned any security procedures insuring that each and every removeable memory data storage device

(CD's, flash cards, smart cards, flash drives, etc) are clean of any possible malicious vote altering programs. This is the way that this malware is introduced into the system. They perform no "due diligence" analysis of the data on these memory devices and they have no interest or concern about inherent built in vote altering programs imbedded within the program's software.

All the RoV personnel who spoke never once acknowledged or gave any indication of awareness of the voluminous incidents of e-voting problems which have happened in America since 2000. They are either oblivious of this or they are incredibly ignorant. Either way, this is an intolerable position to take on their part.

After listening to the various IT "experts" pontificate on their extraordinary security measures, and realizing how glaringly wrong, misleading and deceptive their claims were, one comes to only one conclusion. That is, these RoV IT "experts" knew what they were saying was incorrect, or they are completely and totally ignorant of what real security is involving e-voting equipment. Their pompous, arrogant, elitist attitudes cannot and will not compensate for their utter and complete ignorance of implementing truly effective security and defense measures necessary to protect the sanctity of the vote in America.

MARC KEENBERG

From: Rick Crawford
Sent: Wednesday, August 01, 2007 5:06 AM
To: Voting Systems
Subject: Comments on Top-to-Bottom Review of Voting Systems

FROM: Rick Crawford

Dear Secretary Bowen,

BRIEF BIO:

My background includes over 18 years as a Computer Security researcher. My research has been funded primarily by federal agencies, including the Air Force Information Warfare Center, DARPA, Dept. of Energy, NIST, NSF, and the National Security Agency. Although some of my research (on malicious code detection) was classified by the NSA, I have 11 peer-reviewed publications in the open literature.

My work encompasses the broader social context in which Information Technologies are used: I co-developed and taught what seems to have been the first class on Computer Ethics in the UC system.

SITUATION ASSESSMENT:

In the 2000 and 2004 presidential elections, this nation's voting systems performed so poorly, that many Americans questioned the legitimacy of the elections' outcomes. In an attempt to bind the nation's wounds, the Commission on Federal Election Reform, co-chaired by former President Jimmy Carter and former Secretary of State James Baker, issued a final report, "Building Confidence in U.S. Elections". In it (http://www.american.edu/ia/cfer/report/CFER_section3.pdf), section 3.3 on "Security for Voting Systems" states,

"The greater threat to most systems comes ... from insiders who have direct access to the machines. ... There is no reason to trust insiders in the election industry any more than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it."

I would add that computerized insider attacks at America's major financial institutions involving hundreds of millions of dollars are not unusual, despite extensive security precautions. As another example,

08/01/2007

insider attacks by Aldrich Ames (CIA) and Robert Hanssen (FBI) caused considerable damage, but that harm was limited by those organizations' underlying secure design principles (e.g., separation of privilege).

This is why security must be designed into a system, not tacked on as an afterthought. And it demonstrates why we need reliable methods to *detect* manipulations after the fact, even if we are unable to prevent them. Your Red Team leader's overview correctly emphasizes these points (http://www.sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf). These points -- insider threats, and multi-layered security-in-depth design -- are among *THE* most elementary aspects of computer security.

That is why I am absolutely appalled to read quotes from the 3 voting machine vendors disputing the conditions of the Red Team testing. It is far worse to read similar quotes from the President of the Calif. Association of Clerks and Elections Officials.

As though reading from the same playbook, these parties claim that Red Team testing was "unrealistic" because (1) the team had too much access and knowledge, and (2) the Red Team did not face a Blue Team (i.e., operational security procedures).

But their claim #1 denies the threat of insider attacks, and their claim #2 denies the need for a multi-layered security-in-depth design!

It simply is not credible that voting machine vendors are so ignorant of basic security. And since the President of the Calif. Assoc. of Clerks and Elections Officials was quoted in the San Francisco Chronicle (7/3/07) as saying he personally administers the voting system in his county, I would like to assume he knows a little about computer security.

Yet either these parties are woefully ignorant about the most elementary aspects of computer security, or they intentionally are denying that any "realistic" security threats or flaws could exist. Such a denial of reality would be so blatant, as to bring to mind Saddam Hussein's Minister of Information, who insisted to reporters that, "We have them on the run," even though American tanks already were roaming the streets of Baghdad.

(Diebold certainly was aware of some of their security flaws: David Wagner's 3/15/07 Congressional testimony described how Diebold had been informed privately about a flaw in 1997, yet despite recurring public reports of this flaw, still had not fixed it 10 years later.)

Unfortunately, by denying the problem, these vendors (and apparently also the Calif. Assoc. of Clerks and Elections Officials) have chosen to become part of the problem, rather than part of the solution.

SHORT-TERM RECOMMENDATIONS:

Democracy requires that the casting of ballots be secret,

but that the counting of votes be accurate and transparent to the public. All 3 tested systems revealed security flaws so egregious, that they should be decertified. The InkaVote system (whose manufacturer was unwilling or unable to comply with the testing protocol) likewise should be decertified. These decertifications should be unconditional, i.e., the Secretary should *not* allow County election officials to attempt to "patch" fundamental design flaws by operational procedures.

In light of the serious design and configuration flaws found in all systems tested so far, the Secretary should provisionally (de-)certify any other DRE systems in use within the state, subject to the condition that each can be used (in the near term) only if similar design flaws are not found by similar TTBR testing. Such short-term testing should *not* consider any alleged protective effects of County operational procedures. This is because, in the short-term, it is impractical to assess the composite of an insecure design coupled with assorted County procedures that are either secret or only documented informally. Moreover, the adequacy of implementation of those security procedures cannot be verified until the election is already underway.

Regarding the Calif. primary election scheduled for Feb. 2008, one option is to mandate absentee ballots. In the Nov. 2006 election, nearly 42 percent of voters chose absentee ballots. A second option is to reschedule the Feb. 2008 election. California should lead the nation in demonstrating, by example, that we will not tolerate a sham election that violates the trust voters have placed in the process. Better to have an election that is late, but reliable. Any other state using similar machines should be shamed into following the Calif. example. Presidential primary candidates should demonstrate their commitment to accurate and transparent elections by pledging to remove their name from the ballot of any state that fails to follow California's standard.

LONGER-TERM RECOMMENDATIONS:

Every technology is situated in a context comprised of social, institutional, political, and economic factors. Unfortunately, in the case of voting machines, none of these contextual factors currently is favorable for election accuracy and transparency. Clearly the security of voting machine technology must be improved. But that cannot occur in isolation.

Therefore, the Secretary should use (provisional) certification *strategically* to transition the marketplace, so that voting machine vendors compete to achieve open standards of security and usability. In conjunction with those changes in technology, the Secretary, working with the Legislature and the Attorney General, should alter the institutional context of use, so that Counties employ a certain minimal level of uniform security procedures, so that election workers are adequately trained in those procedures, so that election-day *implementation* of security is inspected and verified, and so that

appropriate legal liability serves as an incentive for compliance.

Finally, to achieve a fair and level playing field, it is imperative that the state also transition to a mandate of *interoperability*,
SO THAT NEVER AGAIN CAN VOTING MACHINE VENDORS DICTATE THE TERMS OF SECURITY TO OVERLY-COMPLIANT ELECTION OFFICIALS.

From: Hebard &/or Peggy Olsen
Sent: Wednesday, August 01, 2007 7:17 AM
To: Voting Systems
Subject: rebuttle to registrars etc.request for field testing. can't make safe elections

My background is programing since 80's wrote entire database for my classroom as well as assembling terminal from ICs and multiuser computers from boards.

- 1 Their field testing argument sounds good; but it is irrelevant in this case.
- 2 The objective is to convince voters their vote was really counted while all uncertain action occurs unwatchable inside of a metal box.
- 3 They are saying they will prevent all hacking! Not convincing!
- 4 Most people who most of the time watch the DRE machines are not PhD in Computer programer / hardware and hardware experts! Will not make voters trust!
- 5 They cannot see the defects discovered by Debra Bowen's teams being used to hack the election. Will not make voters trust!
- 6 Most of the time DRE are watched by people who do not understand unmaskable resets, subroutines, infinite loops , conditional statements, strings, numbers nor boot strap loaders or how viruses work etc.
We are to believe morrons could help make elections accurate!
- 7 If the security needed were applied the vote would no longer be secret because a guard would be needed to watch for bogus cards to be inserted in machines. as well as other tampering and could see who the voter voted for. This violates voter laws!
We need to retrain dope sniffing dogs to sniff cards with bogus code on them to alter the election. Good Luck!
- 8 Invisable ballots should be forbidden. Don't know where stored if even counted, If paper same as screen with using untrusted looking device. (computer program) Does not increase confidence.
- 9 Security must be considered in designing each part. Will increase confidence!
- 10 Security must be considered in assembling parts together.
Will increase confidence more than Registrar's hot air!
- 11 Accomidating handicapped and different languages must be separated from the counting prosscoss so voters can understand the counting prosscoss in Optical scanner. Will increase voter confidence.
- 12 The microprocessor in counting machine must be incapable of executing code not stored in read only memory to avoid viruses and specious code. Will increase confidence!
- 13 There is no believable set of field rules which will make the make it possible for registrars or assistants to be able to monitor any fraud which is occurring least prevent it.
Registrars hot air to convince us does not inspire confidence!
- 14 It will difficult to rework the current machines to prevent fraud.
- 15 I believe it is possible to design groups of machines with security as the first priority, transparency as the second priority, and accuracy as the third priority to be used to vote with and make the prosscoss visable to every one in the county via the internet as a publishing device not a voting device.
- 16 A secure machine could be designed starting with redesign of the microprocessor to be incapable of executing any code not stored in read only memory--viruses could not be added. Would increase voter confidence.

17 Have the counting done by a optical scanner which does nothing else and understands a specially constructed voting language readable by all voters using words like ADD Sum etc. and posted on the machine. Would increase voter confidence.

18 All the handicapped facilities and different languages should be done by a non counting machine which prints a paper ballot which the voter must sign that he/she checked. Would increase voter confidence.

19 All precinct counts would be posted on the internet in real time.
Would increase voter confidence!

20 All summations of those counts would also be posted in real time.
Would increase voter confidence!

21 Any adjustments made by the registrar would also be posted in real time with rationale for doing so. Making this public would increase voter confidence.

22 each voter would get acknowledgement that his ballot was counted or a reason why not or any problems with it. Would increase voter confidence.

23 Eliminate excluding voters for any reason because more damage than by allowing all felons to vote.

Hebard Olsen Teacher of computer programming in High School
Created database of assignments, Seating, Grades , and actual learning packages in Science and math.

From: Donna & Mitch Pomerantz
Sent: Wednesday, August 01, 2007 5:01 PM
To: Voting Systems
Subject: Comments on Voting Systems Report August 1

Importance: High

August 1, 2007

The Honorable Debra Bowen
Secretary of State
1500 11th Street, 6th Floor
Sacramento, CA 95814

Re: Comments for the California Top-to-Bottom Voting Systems Review
"Final Accessibility Review Report"

Dear Secretary Bowen:

My name is Donna Pomerantz and I am very active in local, state and national organizations/community. So that you may have some background and know my credentials I will name some of the following bodies of which I am an active participant.

- Pasadena Accessibility & Disability Commission, Chairperson
- Los Angeles County Commission on Disabilities, Commissioner
- California Council of the Blind, Vice President, San Gabriel Valley Chapter
- Los Angeles County Registrar Recorder's Accessibility Advisory Committee, Member
- American Council of the Blind, Member
- Community Rehabilitation Services Independent Living Center, Member, Board of Directors

There are more, but I wish to limit this to those bodies that have a relevance to this subject. As you can see there is a cross disability perspective in these positions, but in my letter I will focus on Blindness and Issues of Language and Traumatic Brain Injury.

I have reviewed the July 26, 2007 Accessibility Review Report for California that concludes the Hart, Sequoia, and Diebold electronic voting systems to be non-compliant with the accessibility requirements of HAVA and the 2005 Voluntary Voting System Guidelines.

I am genuinely troubled that the findings of this report may lead to decertification of voting systems that are already in place to allow for a private, independent, accessible voting experience for people with disabilities.

I concur that there are valid flaws in the current systems, not one system is full proof or fully accessible for every person who has a disability, all systems have their strengths and weaknesses. But in the "red team testing" these systems were tested in a lab setting and not in the "real world environment" therefore the comparison is flawed as well.

However, the solution is not to completely decertify the equipment that is currently in use. This would completely disenfranchise voters with disabilities and of those with and without disabilities there is a diverse representation of those who speak a language other than English. These systems have made it possible for those who have disabilities and those for whom English is a second language to vote independently,

privately and using systems that are accessible to them.

Now on a personal note, I decided in this last election to be a pollworker and was also very excited that for the first time in my life I would be able to vote privately and independently at my home precinct just like everyone else. If I could only find the words that could express how liberating it was before, during and after I voted privately and independently just a block or two from my residence. In this voting experience for the first time in my life I had choices. I was not segregated. I did not "have" to vote early at another location that was a bit further than my residence. I was not forced to "hire" a reader to fill out the ballot "for" me. I really was "set free" to make choices just like everyone else. I was no longer being treated like a "second class citizen" just because I have a disability. How truly liberating. This is an experience that I will never forget.

Please don't take this away from me. I have tasted freedom and it is good. Yes, there is work to do but while that valuable work is being done, please allow me to keep those rights and don't take them away because there is still more work to be done. I want to keep on voting independently and be allowed to make choices. I want to encourage more of my community to do as I did. Once they too are able to taste freedom, they will never forget.

I can say now that I do know what a privilege it is to be able to vote privately and independently, please don't take that away from me.

Respectfully,

Donna Pomerantz

From: Phil Johnston
Sent: Wednesday, August 01, 2007 5:01 PM
To: Voting Systems
Subject: Red Team Review of Diebold, Sequoia, Hart, and ES&S Machines

Secretary Bowen,

As an IT Professional and advocate for free, fair and TRANSPARENT elections who is gravely concerned about the use of Electronic Voting Machines, THANK YOU for performing the Red Team Review of Diebold, Sequoia, Hart, and ES&S Machines. As suspected and predicted, the machines demonstrated massive security flaws.

As you must also be aware, the lack of secure and consistent policies and procedures involving the administration and use of these machines is also a source of massive security flaws. Either one of these flaws is cause enough for great concern. Taken together, it is frankly quite chilling in its implications for potential corruption.

In light of these concerns, I sincerely hope you will decertify these machines and not allow their use under any circumstances, conditionally or otherwise. As an interim solution to make up the deficit created by this decertification, I suggest using Optical Scan Ballots in their place. Optical Scan Ballots can be scanned quickly, are highly accurate, and provide a paper trail in the event that a recount is needed.

Just the same, as a necessary procedure to test and maintain accuracy, mandatory recounts of some statistically significant percentage of the total for each precinct should be implemented.

Finally, in an effort to bolster your confidence in standing up to the vendors of these Electronic Voting Machines, please know that I voted for you in hopes that you would do just that. So far, you have demonstrated courage in standing up to these people whose only real interest is in their bottom line, NOT the integrity of our democracy. I applaud your efforts and encourage you to do what is best for our democratic process, not the special interests of the voting machine manufacturers.

Thank you,

Philip Johnston

Computer Resource Specialist
Media Services Kerr Hall

64
868
12
edu

From: Paul Lehtc
Sent: Wednesday, August 01, 2007 4:34 PM
To: Voting Systems;
Subject: Top to Bottom Review: Decertify all Systems

Dear Secretary of State Bowen:

As you know, you are statutorily authorized to conduct this top to bottom review for the purposes of assessing the suitability of voting systems for use in California. As an election lawyer with some litigation experience in California elections, I wish to offer the following comments supporting complete decertification of all electronic voting systems in use in California for the reasons stated below, particularly emphasizing your own inability, on account of vendor resistance and delay, to even complete and accomplish your own duties of inspection and review on account of vendor opposition to producing any and all information.

1. It is clear that the Secretary has authority under Elections Code section 19203 to "make all arrangements for the time and place to examine voting equipment proposed to be sold in this state." You made those arrangements, you know the manner in which they were not complied with was numerous and egregious. This alone prevents you from forming a belief that you have properly inspected those voting systems such that you can approve them. You would be speculating as to software not provided or reviewed, and information withheld. Thus, the information required to be provided by vendors is insufficient to form a finding that the systems comply with California. Accordingly, this alone requires decertification.

2. Under elections code section 19205, the software is required to be suitable for the purpose intended. However, all vendor contracts of which I am aware routinely disclaim the implied warranties of merchantability and fitness for a particular purpose. This constitutes a signed statement for each vendor DENYING that their voting systems will work for their usual purpose (the general legal definition of merchantability) and it constitutes DENYING that the systems will work for the particular purpose intended, namely elections in California Counties (the general definition of fitness for a particular purpose). These denials are, standing alone, sufficient evidence not only to decertify, but to conclude beyond any doubt that the manufacturers themselves do not believe in and do not stand behind their products, and do not in fact think they are suitable for the purpose of California elections in a way that is meaningfully relevant to the public's goals of transparent and accurate elections. See [my legal white paper on this at http://www.wheresthepaper.org/ZeroGuarantee0707.pdf](http://www.wheresthepaper.org/ZeroGuarantee0707.pdf)

3. The security papers adopted by the Secretary as contractually or legally demanded by vendors constitute significant if not total (in some instances) restrictions on the discretion of the Secretary to inspect and evaluate voting systems. These requirements, be they from trade secrecy or contract, constitute additional conditions blinding the eyes and limiting the ability of the Secretary to do her job and support the public interest.

4. False Statements and Fraud by Vendors. <http://www.sequoiavote.com/bAVCEdge.php> states as follows, and has so stated since at least August 2004, and constitutes a warranty and representation that inheres in the contacts Sequoia signed, since it is an express warranty it is

not waivable:

Unmatched Security

The AVC Edge® provides nothing less than 100 percent accuracy, privacy and security.

- The Audit Trail provides an **unalterable electronic record of all votes cast** during an election

For reasons clearly established in the Top to Bottom and red team reviews, this statement is false and fraudulent. This constitutes an independent basis for rescission of contract under the law of fraud and false pretenses because the records ARE alterable, and the systems are NOT 100% accurate, private, and secure.

5. History of Inaction. I personally sued Sequoia in April 2005, on issues including the "yellow button" that, pressed twice, allows unlimited manual voting. Sequoia has proven an intense pattern of recklessness by taking no action on this, despite all the notice one could possibly have of this problem See www.votersunite.org/info/lehtolawsuit.asp (choose "complaint" near bottom)
6. Diebold represented to the NH Ballot Commission on videotape that they would do whatever the California SOS required. They did this to obtain a NH approval. Obviously this was a false statement. Diebold, and all other vendors, are NOT LISTENING nor do they sincerely wish to have their code vulnerabilities corrected. This is an additional reason, in the nature of "other good cause" sufficient for decertification.
7. Decertification can and should be sought also under Election Code section 19214.5.
 - (a) [...] for an unauthorized change in hardware, software, or firmware to any voting system certified or conditionally certified in California." This should include a prohibition on doing business in California for 3 or more years, and refund of money under subsection (4).
8. Local elections officials are also prevented by vendors from doing a proper inspection every two years, and this is supporting cause for decertification under Elections Code section 19220. The elections official of any county or city using voting or vote tabulating equipment shall inspect the machines or devices at least once every two years to determine their accuracy. IT IS IMPOSSIBLE To determine accuracy under conditions of secret vote counting or trade secret software. Most certainly any TIMELY determination of this accuracy, prior to certification of the election result is not possible, especially when local elections officials claim to be too busy to provide whatever very limited information they do have access to. Here again, it is impossible for the Secretary of State, or any rational human being, to form a rational belief that a complete top to bottom review has been had. Secret vote counting defeats this entirely.

Please decertify the non-transparent, secret vote counting software from all vendors, as it completely prevents and defeats the democratic accountability of elections. Whenever the private power exceeds the government power, as FDR specifically noted, we have met the definition of fascism. To approve any of these systems is to accept that private power of corporations is greater than the public interest in transparency, since they insist on

secrecy in vote counting. I do not believe that you could, consistent with your oath of office, allow any vendors to continue to do business, since you would be violating your duty to uphold the Constitution and laws of the state of California and its people, in favor of corporate power, and implicitly finding that power superior to the sovereignty of California. This is impossible, if we remain a democracy.

Very truly yours

Paul R Lehto
Attorney at Law

--

Paul R Lehto, Juris Doctor

From: Nancy Tob
Sent: Wednesday, August 01, 2007 4:08 PM
To: Jenny Clark
Cc: Voting Systems
Subject: Re: Recommendations for the General Election of 2008

Secretary Bowen,

I will add my congratulations and thanks to you and your staff, for initiating and following through with the red team testing.

The office of the New Hampshire Secretary of State has graciously provided the following presentations on hand counting methods and management, as well as disability accessibility in NH voting systems.

http://www.democracyfornewhampshire.com/files/Dem4NH_DisabilityVoting.pdf

http://www.democracyfornewhampshire.com/files/democracyfest_reconciliation_handcounting.pdf

Our Deputy Attorney General, Bud Fitch, has also provided an invaluable presentation on election night reconciliation, here:

http://www.democracyfornewhampshire.com/files/democracyfest_reconciliation_handcounting.pdf

Additionally, I am attaching a draft version of a Hand Counting Primer, for your review. This includes information from the presentations cited above.

As the nation looks to California, I pray you and your state have the courage and strength to do what must be done, what we all must do, and get rid of these secret vote counting technologies that are plaguing our country and undermining our democracy.

Best,

Nancy

--

Nancy Tobi
Chair, Fair Elections Committee
Legislative Coordinator, Election Defense Alliance

On 8/1/07, **Jenny Clark** > wrote:

Thank you! Secretary of State Debra Bowen for the review of electronic voting machines!

I understand you are soliciting public comments on the issue, through today.

Yes, all e-voting systems must be decertified at once! Good luck!

08/02/2007

I have been aware of the fraudulent voting machines for many years and have been appalled at the lack of serious review and public awareness (thanks to the media blackout on the subject). So I am especially grateful for your "Red Team" review.

With the Emmy nominated "Hacking Democracy" in documentaries this year, maybe that will help shed some light on this serious problem. You may recall that even optical scan voting systems are hacked in this film. Any marking or counting device that relies on computer technology can be hacked.

There was a time we all believed a "paper trail" attached to e-voting machines would be a good answer. However, since new information and evidence of fraudulent counts, conflicting exit polls and a host of other evidence, I now believe that the best solution is to simply scrap all computerized technology in our voting systems.

What voters need and want and deserve is a "paper ballot". We do not need a receipt to take home nor do we need a small percent of our votes audited as the paper "trail" proponents argue.

The best solution for accurate vote counts is to return to the simple hand counted paper ballot, hand counted in full public view at the precinct level. The totals at the precinct will match the number of voters who signed in to vote. The paper should be of a durable stock to allow many hand counts of multiple-candidate/issues on the ballot. Even if you paid the counters \$20 an hour, you still would save many millions by avoiding complex computer upgrades year to year, and other expenses.

I am not an expert on computers or hand counting, but I highly suggest that you seek advise from many experts who are knowledgeable on how to do hand counts.

Posted below is a link and an article about how to conduct a hand counted paper ballot election. Do not be swayed by nay-sayers who think this solution is a return to the dark ages. Indeed, many countries around the world use this system just fine and are perplexed with the US fixation on voting machines. It is totally doable, even in a large state like California. It keeps all elections as local as possible at the precinct level.

I hope that California will once again be a leader for the nation on this issue of e-voting. Every technological fix suggested by computer experts is another doorway for hacking. The accountability and prosecution of the fraud that has already occurred should be firm and swift.

Good luck!
Thank you,
Jenny Clark

See this link for information on "An Election Preparedness Kit", written by hand counted paper ballot expert Nancy Tobi from New Hampshire, who is another good source for you, on the training required to perform hand counted ballots. It should not take too long to do the training. I have copied Nancy on this e-mail to make it easy for you to contact her.

<http://www.democracyfornewhampshire.com/node/view/2606>

This article explains in simple terms how easy and inexpensive it is to use the hand counted paper

ballot voting system.

<http://www.smirkingchimp.com/node/8842>

On-Site Observations of the Hand-Counting of Paper Ballots and Recommendations for the General Election of 2008

by **Sheila Parks** | Jul 20 2007 - 9:44am |

Between May 2, 2006 and November 7, 2006, I observed the hand-counting of paper ballots in three elections in two New England states. The purpose of these observations was to gather first-hand data concerning the feasibility, effectiveness and accuracy of the use of HCPB. These elections were as follows:

- (1) Rockport, Massachusetts (MA), on May 2, 2006, Town Election
- (2) Hudson, MA, on May 8, 2006, Town Election
- (3) Acton, Maine (ME), on November 7, 2006, General Election

All three hand-countings of paper ballots were conducted smoothly and were finished in a timely manner. This paper describes the various protocols used and presents recommendations for the use of hand-counted paper ballots (HCPB) in the upcoming elections of 2008. Absentee ballots, provisional ballots and chain of custody of the ballots are not dealt with in this paper, although they are also crucial elements of an HCPB system.[1] Much has been written about the fraud and error associated with the use of electronic voting machines - both Direct Recording Electronic (DRE'S/touchscreens) and Optical Scan (op scans/opti scans).[2] Because of this fraud and error, HCPB have been put forth as an alternative to electronic voting machines.[3] The use of an HCPB system will ensure that each vote is counted as intended and as cast by the voter. Although HCPB do not address the egregious suppression of the vote (mostly of people of color, elders and low income people), partnering a solution to the elimination of this suppression with the use of HCPB is the only way to have honest and transparent elections.

The jurisdictions that I observed were not selected randomly. They were places that I could drive to comfortably from my home in Boston, MA. Moreover, I was interested in observing an election in Acton, ME because the Town Clerk had told me that after the first hand-counting, the ballots would be hand-counted a second time.[4] I received permission to observe the elections from each Secretary of State, or their assistants, and from each Town Clerk. For full transparency, I introduced myself as an advocate of HCPB, who wanted to observe an HCPB election. I was very well received and felt comfortable in all places. All three Town Clerks were very generous with their time and expertise.

In each of the three elections observed, number two pencils were used by the voters to hand mark their paper ballots. In each of the elections, the counters worked in teams of two. In addition, the counters were told that it was the intent of the voter that was to be counted, and when in doubt, the counters called over the Town Clerk or Warden[5] to ask questions about specific ballots and how to count them. Finally, in each of the elections, the counters were able to hand-count the paper ballots in a short time (see specifics below).

ACTON, ME, NOVEMBER 7, 2006, GENERAL ELECTION

I will first describe the HCPB election in Acton, ME on November 7, 2006 because this protocol used a procedure that would produce the most accurate count of the votes - namely, a second hand-count was done immediately after the first hand-count.

The ballot box was a plain, wooden box with a slot into which voters put their ballots. There

were six teams, of two counters each, doing the hand-counting. The counters came in specifically to count; they had not worked at the polls earlier in the day. Each team consisted of a Republican and a Democrat. The teams first counted the ballots into batches of 50, and then these batches of 50 were counted again.

The teams then hand-counted the votes cast in each contest for each batch of 50 ballots in the following manner: One member of the team would read out loud the name marked off for each contest; the other member of the team marked the vote on a tally sheet that corresponded to the ballot. A voter's entire ballot was tallied for all of the contests before the counters went on to tally the next voter's ballot. The talliers counted each vote by making a hash mark (small, straight vertical line). [6] After four vertical lines were made, a fifth line was made diagonally through the first four marks. For each person running for office (and for each initiative), the tally sheet was marked off into five columns vertically and two rows horizontally, providing 10 rectangular spaces in each of which five hash marks could be written - a total of 50 hash marks - i.e., votes - per contest or initiative. A dark horizontal line separated the names in each contest. At the end of the counting of all of the races in a batch of 50 ballots, the counters totaled the hash marks for each race on the tally sheet and entered that number on the tally sheet in the "TOTAL VOTE" column. There was a special sheet for write-ins.

Immediately after the first hand-count of a batch of 50 ballots, a second hand-count, on a new tally sheet, was done of this same batch of 50 ballots by these same counters. Again, the entire ballot of each voter was tallied before the counters proceeded to the next voter's ballot. This time, the person who had read the names out loud marked each vote on the tally sheet, and the person who had tallied read out loud the ballot choices. After the votes on all 50 ballots in a batch were marked on the tally sheet, the totals for each contest were obtained and written on the tally sheet. If the totals for the candidates in any contest or for any initiative were not exactly the same on the first and second tally sheets (i.e. on the first and second countings), these contests or initiatives were counted a third time. I observed such a situation two times.

The HCPB election in Acton, ME demonstrates that paper ballots can be hand-counted immediately a second time, at the precinct on election night, before the results are posted at the precinct, in order to ensure an honest and transparent count in a timely manner. The election in Acton, ME also indicates that paper ballots can be hand-counted in a very short time. With seven races and two initiatives, the six teams of two people each were able to hand-count twice 944 ballots in four hours.

ROCKPORT, MA, MAY 2, 2006, TOWN ELECTION HUDSON, MA , May 8, 2006, TOWN ELECTION

The elections in Rockport and Hudson will be discussed together because they were similar in various respects. Both counted the votes cast only once, [7] and both used the same kind of tally sheets provided by the MA Secretary of State. In both jurisdictions the ballots were counted into batches of 50. The tally sheet was a large piece of paper that was marked off into a grid with horizontal and vertical lines forming small rectangular boxes (similar to the squares of graph paper). The vertical columns were marked with a heavy line at each multiple of five columns. There were 50 rectangular boxes across each horizontal line. At the top of the tally sheet, each vertical column was numbered from 1-50. On both the left hand and right hand sides of the tally sheet were the names of the people running in that particular race. One tally, as a hash mark, was put into one box, beside the name of the person voted for. A voter's entire ballot was tallied for all of the contests before the counters went on to tally the next voter's ballot. After the 50 ballots were tallied, the totals for each contest were entered into the "Totals" column at the end of the 50th box. Blanks and write-ins were also

marked on this sheet. Four or five teams of two poll workers did the hand-count. One read from the ballot, and the other person placed the hash mark in the appropriate box on the tally sheet.

Rockport, MA used an old wooden ballot box.[8] A poll worker turned the brass handle on the box as each voter put her/his ballot into the box. Numbers on the front of the box automatically changed as ballots were placed in it, counting the cumulative number of ballots placed in the box. The machine marked each ballot with the precinct number down the center of the ballot as it went through the machine. The preceding characteristics of the ballot box provided a measure of security for the ballots, minimizing the danger of stuffing the ballot box, a criticism often leveled at the HCPB process. As noted earlier, this paper does not examine in detail issues of security such as chain of custody, but rather deals with protocols for HCPB.

There were two crews of poll workers, morning and afternoon. One crew came in at 6:30AM and worked until 12:30PM. The second crew came in at 12:30PM and worked until 6:30PM. At 6:30PM, the second crew went home for dinner until 8PM, when they came back to hand-count the paper ballots. The morning shift came back at 6:30PM to work at the polls and then to hand-count the paper ballots. The polls closed at 8PM. The paper ballots were hand-counted by five teams of two workers each.

In Hudson, the ballot box was an old box made of gray wood. The ballot box rang when the voter put in her/his ballot, and the poll worker turned the crank of the box, moving the ballot from the slot of the box into the box. When the poll worker cranked the ballot into the ballot box, each ballot was inked with "Town of Hudson, precinct 6." [9] This ballot box also provided a degree of security for the ballots.

The Clerk could hire eight people per precinct, not including the Warden and Clerk, who were also present for the hand-counting. There were two shifts of poll workers, 7AM-5PM and 5PM-8PM, which was when the polls closed. The second shift did the counting. Poll workers had to be registered voters in the town of Hudson. Although it was preferred that the counters lived in the precinct where they worked, it was not necessary.

The elections in Rockport and Hudson again demonstrate that paper ballots can be hand-counted in a reasonable time. In Rockport, it took about one hour to hand-count 522 ballots; there were six races and no initiatives. In Hudson it took about one hour to hand-count 59 ballots; there were 14 races and no initiatives. As noted, both communities used ballot boxes that provided a degree of security for the ballots.

RECOMMENDATIONS TO BEGIN WITH THE 2008 GENERAL ELECTION (WHICH INCLUDES THE PRESIDENTIAL ELECTION)

Recommendations Based on My Observations

(1) Based on my observations in Acton, ME, this paper recommends the hand-counting of paper ballots followed immediately by a complete second hand-counting and a reconciliation of the two counts, if necessary, by additional counting. [10] A second hand-counting is crucial to check the accuracy of the first hand-count. If a discrepancy is found between the two countings, counting should continue until the counts are reconciled. This paper also recommends the procedure used in Acton of counting the ballots into batches of 50, counting a batch of 50 and then immediately counting that batch of 50 again. Some critics of electronic voting machines have pointed out the need to obtain a second count, called an audit, after the first original tabulation of votes; however, there is no consensus as to how such an audit should or could be done. The second counting of ballots recommended in this paper goes beyond the concept of an audit to a comprehensive process encompassing a second counting of every vote and a reconciliation of the two counts.

(2) From my observations of these three hand countings, I prefer the tally sheets used in Acton, ME over the graph-like grid used in both Rockport, MA and Hudson, MA. During my observations, it appeared that the Acton tally sheet was easier for the counters to use. With the grid-like tally sheets, care had to be taken by the counters not to lose their place.

(3) Because HCPB require careful attention to and scrutiny of the ballots, it is recommended that people who have not worked at the polls all day come in to do the counting, as in Acton, ME.

(4) As noted, this paper does not deal in detail with the issue of security of the ballots. However, it is recommended that research be done concerning the cost of manufacturing ballot boxes with the characteristics described for Hudson, MA and Rockport, MA.

Additional Recommendations

The present author has been involved with voting rights for the last five years. Based on her previous work, [11] she also further expands the use of HCPB to include the following recommendations:

(1) In addition to the four recommendations presented above, it is recommended that an HCPB protocol also have the following characteristics: (a) Ballots would be counted at the precinct by registered voters in that precinct. (b) The counting would be done in full view of the public. (c) The counting would be videotaped. (d) The results would be posted at the precinct immediately after the count. (e) To be manageable, precincts would be no larger than 1000 registered voters. (Because the concept of HCPB operates at the precinct level, even large communities can adopt such a system.) (f) In each precinct there would be at least 10 teams of two counters each (a Democrat and a Republican). [12] These teams would count the ballots, one counter reading the name and the other counter making the mark on the tally sheet. For the second counting, the counters on each team would switch roles. (g) Whether or not there would be observers as part of the team of counters, and if so, how many, needs more research and is beyond the scope of this paper.

(2) This paper recommends that poll workers who participate in the process of HCPB be paid at a rate that will be respected by the community. This will be possible because a large amount of money will be saved with the elimination of electronic voting machines. The Help America Vote Act (HAVA) paid states hundreds of millions of dollars to buy electronic voting machines, both DRE'S and/or op scans. [13] One machine can cost anywhere from \$3,000 - \$5,000 [14] and that amount does not include storing, maintenance, and upgrade. In contrast, for an HCPB election, the cost for the counting could be \$2400.00 per precinct for each election, with ten teams of two workers each, as described above, and paying each worker \$20/hour for six hours (\$120). HCPB by registered voters from the precinct would also keep the money in the community. As is true for op scan electronic voting machines, money would also have to be spent for the cost of printing the ballots. [15] If hundreds of millions of dollars had not been spent for the purchase, storage and upgrade of electronic voting machines, imagine the money our communities could have used for health care and education.

EPILOGUE

On January 4, 2006, I had the good fortune to watch on TV the voting in Congress for Speaker of the House. One at a time, each representative called out orally her/his choice for Speaker, and that vote was tallied by hand. This hand counting of oral votes was done by two Republicans and two Democrats, all of whom had been appointed by the Clerk of the House. The Electronic Board that usually counts the votes of the Representatives was not used for this count; the official vote was tallied by hand. I could not help but wonder how the Representatives would have felt had their votes not been recorded accurately, or not at all, as

voters throughout the USA experienced in recent elections. For voters in each precinct in the USA, hand-counting of paper ballots would assure that each of our votes is counted as intended and as cast, as the oral votes of our Representatives, were hand-counted, as intended and as cast, in the House of Representatives.

ENDNOTES

[1] For a beginning discussion of chain of custody, see the present author's paper *Hand-Counted Paper Ballots Now*. A version of this article first appeared in the April 2006 issue of *Tikkun*, <http://www.tikkun.org/magazine/specials/article.2006-04-10.1693298872>, retrieved from the Web February 28, 2007. An updated version can be found at <http://electionfraudnews.com/News/HCPBNow.htm>, retrieved from the Web February 28, 2007. "Ballot boxes must be clearly marked and visible in plain view. Ballot boxes will be sealed and locked whenever they contain ballots and are not being actively used. Ballot boxes are secured from the beginning of voting until the end of counting by a chain of custody procedure. Ballot boxes never leave the polling place until after the vote is counted, audited and certified. Each time ballot boxes move from the physical control of or visual contact from one person to another, a duplicate record signed by all counters and observers must be made relinquishing and gaining control. There will be a documentation process wherein each ballot box will have a record of its handling from the beginning of the day to the end of counting. On the web site of computer science expert Professor Douglas W. Jones, there is a very clear and detailed protocol for "Ballot and Ballot Box Transportation" and "Ballot Storage." The reader is referred specifically to these two sections (the last two on this link): <http://www.cs.uiowa.edu/~jones/voting/paper.html>

[2] Listed here are some of the outstanding articles about the fraud and error resulting from electronic voting machines; some are from the mainstream media, others from scholarly sources, and yet others from technical groups: (1) The public hacking of electronic voting machines by Harri Hursti, working with Black Box Voting, <http://www.bbvforums.org/forums/messages/2197/6847.html>, retrieved from the Web February 21, 2007. (2) The U.S. Government Accountability Office (GAO) in its nonpartisan September 2005 report on elections states in its conclusions: "Numerous recent studies and reports have highlighted problems with the security and reliability of electronic voting systems § the concerns they raise have the potential to affect election outcomes § Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, But Key Activities Need to be Completed.", <http://www.gao.gov/new.items/d05956.pdf>, retrieved from the Web March 7, 2007. (3) Article by Robert F. Kennedy, Jr. in *Rolling Stone* (Issue 1002, June 15, 2006), http://www.rollingstone.com/politics/story/11717105/robert_f_kennedy_jr_will_the_next_election_be_hacked/print, retrieved from the Web February 21, 2007. (4) Report of the Brennan Center Task Force of NYU, on June 27, 2006, http://www.brennancenter.org/press_detail.asp?key=100&subkey=36345, retrieved from the Web February 21, 2007 and http://brennancenter.org/dynamic/subpages/download_file_38150.pdf, retrieved from the Web February 22, 2007. (5) Papers by Ed Felton et al. from Princeton University in Sept. 2006, <http://dubiousprofundity.com/hackthevote.pdf>, retrieved from the Web February 21, 2007. (6) Problems that occurred with electronic voting machines in many states in the General Election on November 7, 2006, especially the 18,000 undervotes in Sarasota County, FL, http://www.nytimes.com/cq/2006/12/20/cq_2056.html, retrieved from the Web February 20, 2007. (7) NIST discussion draft, December 1, 2006, <http://vote.nist.gov/DraftWhitePaperOnSlinVMSG2007-20061120.pdf>, retrieved

from the Web February 22, 2007. (8) The annotated bibliography by Rady Ananda, <http://tinyurl.com/2gwlve>, retrieved from the Web May 11, 2007.

[3] On August 4, 2006, Nancy Tobi posted this article about HCPB in NH, http://www.opednews.com/articles/genera_nancy_to_060804_the_granite_state_de.htm, retrieved from the Web March 12, 2007. An editorial first carried in the Ketchikan Daily News, December 1, 2006, written by Editor Terry Miller, called for HCPB for the president and vice president, <http://www.ketchikandailynews.com/>, retrieved from the Web January 12, 2007. (Thanks to John Gideon of Daily Voting News for pointing out the Ketchikan editorial.) On December 7, 2006, the editorial was then picked up by the Juneau Empire, http://juneauempire.com/smart_search/, retrieved from the Web January 12, 2007. Rady Ananda wrote an HCPB Implementation Strategy for 2007 on January 3, 2007, http://www.opednews.com/articles/opedne_rady_ana_070102_evoting_exit_strateg.htm, retrieved from the Web March 13, 2005. In February 2007, in Missouri (MO), Show Me The Vote, led by Phil Lindsey, introduced an initiative to go on the ballot that, if passed, would mean that MO would not use electronic voting machines in their elections, but would use HCPB. This initiative must first get enough votes from the public to appear on the ballot, <http://www.scoop.co.nz/stories/HL0702/S00271.htm>, by Michael Collins, retrieved from the Web March 12, 2007. (To contact Show Me The Vote, email Phil at galloglas@sbcglobal.net.) Another HCPB initiative, led by Kathleen Wynne, is in the form of a petition from the American People to Congress, urging Congress to reintroduce the Paper Ballot Bill of 2006, <http://hcpbnow.org/petition.html>, retrieved from the Web July 13, 2007. In June 2007, at The DFA (Democracy for America) Democracy Fest in New Hampshire, in a telephone call to the attendees, Representative Dennis Kucinich stated that he will introduce The Paper Ballot Bill of 2007, mandating HCPB for all federal offices. Kucinich has changed the bill from his 2006 version, H.R. 6200, which had mandated HCPB for the offices of president and vice-president only, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6200ih.txt.pdf, retrieved from the Web, March 30, 2007.

[4] I observed one of the three HCPB methods authorized by the Maine Secretary of State, called "The Reading Method": "The team counts each lot together; 1 member reads and the other member tallies. The team members then switch roles, so that the tally is done a second time. If they agree, that count is completed. If there is a discrepancy, the team must recount the race or races where the count was off. Š." From Maine Revised Statutes Annotated (MRSA), CONDUCT OF ELECTIONS, Chapter 9, page 3, (Title 21-A §695).

[5] "Warden" is the name used in Massachusetts for the poll worker in charge of the election in that precinct. Different names are used in different states. The person is not an elected official

[6] In April 2004, Teresa Hommel described some hand-counting methods used in Canada and New York City, <http://wheresthepaper.org/CountPaperBallots.htm>, retrieved from the Web January 13, 2007.

[7] Another method of hand-counting paper ballots is the sort and stack protocol, <http://www.sos.nh.gov/FINAL%20EPM%208-30-2006.pdf> (pp 144-146), retrieved from the Web May 11, 2007. In this method, used by the state of New Hampshire, the ballots are first sorted into stacks for each candidate, and then the stacks are counted. In email correspondence, December 2, 2006 and December 4, 2006, with Nancy Tobi from Democracy for New Hampshire, Tobi states that NH uses the sort and stack method for both election night counts and for recounts. She says that it is used primarily for "Š single member

racers - where there is a yes/no choice." and for straight ticket votes. Sort and stack is not usable in all situations. With this protocol, as with those used in Rockport and Hudson, votes are counted only once; the manual recommends a second count if there is a "close race." A "close race" is not defined. A mandatory second count for all ballots could be added to this protocol.

[8] The ballot box said "Town of Rockport, Precinct 2" and was dated 1922.

[9] The ballot box was made by S. Ralph Cross and Sons, Inc., 120 Mayfield Street, Worcester 2, MA, now out of business. The box was dated 1971.

[10] Joanne Karasak has recommended a first count followed by "an immediate second 'blind' count (blind count meaning that the second team of counters do not know the total on the first count)." Email posted June 26, 2007. Based on my observations in Maine, I think it would be too confusing to change counters.

[11] See Sheila Parks, *What Went Wrong in Ohio & Black Box Voting*,

<http://www.tikkun.org/magazine/reviews/article.2006-01-06.7975946864> , retrieved from the Web March 18, 2007; Sheila Parks, *Hand-Counted Paper Ballots Now* (see endnote 1); Roy Lipscomb and Sheila Parks, *Hand-Counted Paper Ballots: Frequently Asked Questions*, <http://www.scoop.co.nz/stories/HL0705/S00261.htm> , retrieved from the Web May 20, 2007.

[12] If there additional parties on the ballot, representatives from these parties should also participate in the counting.

[13] Thanks to my good friend Lucius Chiaraviglio, HCPB activist, for his help with this endnote, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ252.107,

retrieved from the Web March 13, 2007.

[14] Thanks to Paul Letho for sending me this information. See Appendix A,

<http://www.votersunite.org/info/SequoiaContract.pdf> , retrieved from the Web March 18, 2007, for the contract between Snohomish County, Washington and Sequoia Voting Systems, Inc. for a detailed example of what electronic voting machines cost. This contract was for more than \$5 million dollars. Appendix A is contained in his lawsuit against Sequoia Voting Systems, Inc., www.votersunite.org/info/lehtolawsuit.asp , retrieved from the Web March 18, 2007.

[15] Email correspondence, March 6, 2007, with Chief Legal Counsel, Election Division, Office of the Secretary of State, MA. In MA in 2006 there were 71 precincts using HCPB. For the MA State Primary election in 2006, the cost was \$444 per precinct (which included two parties) for ballot printing, which included absentee ballots, specimen ballots and instruction cards. For the General Election in 2006, the cost was \$391 per precinct.

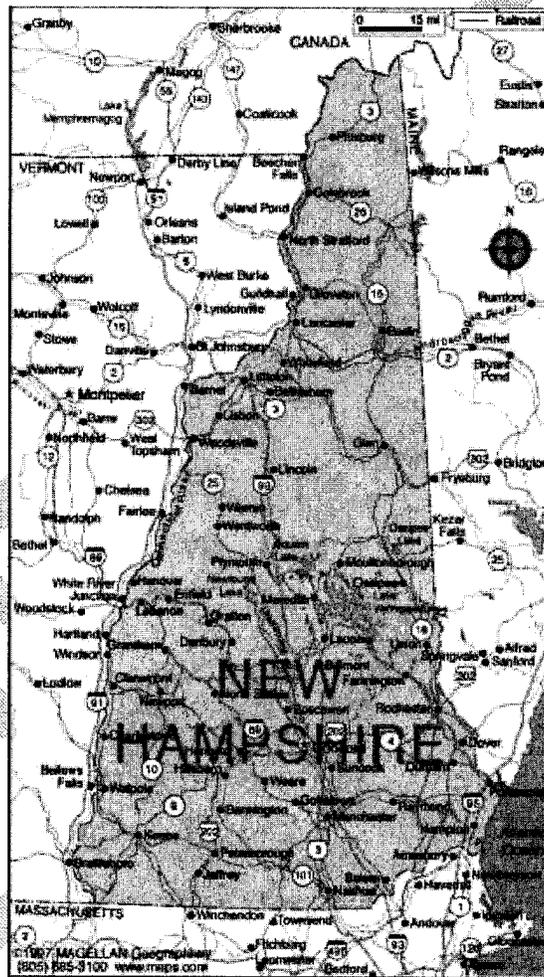
Copyright © 2007 by Sheila Parks, Ed.D.

ABOUT AUTHOR

Sheila Parks, Ed.D., is an Organizing Consultant who lives in Boston, MA. She is a long time feminist and peace & justice activist/organizer on many issues and has been involved in the current wave of voting rights for five years.

Sheila Parks's blog |

Hand Counting Paper Ballot Elections: A Primer



Lessons from New Hampshire

CONTENTS

The New Hampshire Tradition of Democratic Elections	4
National Political Geography Supports Hand Counting	4
California study reinforces need in the Granite State to rid ourselves of secret vote counting technology	5
Hand Count Basics.....	6
Management Considerations	6
Methods for Hand Counting Paper Ballots	6
Why Hand Counting on Election Night is Better than Post Election Audits	7
Foundations for Hand Counted Paper Ballot Elections	7
Legal Infrastructure: Elected (not appointed) Election Officials	7
Legal Infrastructure: Voter Intent.....	8
Legal Infrastructure: Paper Ballot is Vote of Record.....	8
Challenges to Running Hand Count Elections.....	8
Support for Hand Counted Paper Ballot Elections.....	9
Community	9
Training.....	9
Hand Counting Large Numbers of Paper Ballots, even Complex Ballots.....	9
Hand Count Systems as Self-authenticating Systems for Election Integrity.....	10
Feasibility of Hand Count Elections	10
Manual Central Tabulation.....	10
Lessons Learned from New Hampshire*	10
Counting in New Hampshire	11
A wide range of situations calls for different solutions	11
The New Hampshire Secretary of State's position	11
Hand Count and Reconciliation Methodology*	11
elements in Hand Count Elections.....	12
Recruiting counters & observers.....	12
Management Primer for Hand Count Elections*	12
Calculating Contests per Ballot.....	12
Team Availability on Election Night	13
Estimating Hand Counting Staff.....	13
Calculating Staff.....	13
The Sort and Stack Method for Hand Counting*	13
Overview of Sort and Stack Method	14
Advantage of sort and stack method	14
Rule of Thumb for Sort and Stack.....	14
Choosing Number of Sort and Stack Observers.....	14
Organizing For the count	15
Oath of Office	15
Training	15
Steps to Implement Sort and Stack Method	15
Election Night Reconciliation*	17
Ballot Inventory	18
Ballots Used	18
Counting Number of Voters Voting	19
Total Votes Counted	19
Votes Cast For An Office	19
Expected Undervote	20
Analysis And Figures For Nationwide Costs of Replacing DREs With Paper Ballot Voting Systems	21
Replacing the Nation's DREs with Optical Scanners.....	21
Replacing the Nation's DREs with HCPB Elections	21
Supporting Information for the Elimination of DREs	22

National Institute of Standards and Technology (NIST) Study 2006..... 22
Election Science Institute Study 2006 23
RESOURCES..... 24

DRAFT

The New Hampshire Tradition of Democratic Elections

New Hampshire has many years' experience with hand counted paper ballot election administration and management. This document shares some information from the New Hampshire experience. Even with our robust tradition of hand counted elections, New Hampshire, like most, if not all, other states, nonetheless allows the use of computerized vote counting machines, and some 55% of our polling places have chosen that method to tabulate their votes.

New Hampshire citizens, election officials, and elected officials, are in a continuing process of evaluating these different methods and their place in our elections. We, like the rest of the nation, have a lot of work ahead of us to improve and sustain our democratic elections.

But New Hampshire has a long standing tradition of grassroots democracy, and it holds us in good stead as we work on these issues. Our proud and honored traditions of hand counted elections have been enriched through the years by a cadre of patriots, from our local election officials on up to our legendary Secretary of State, the Honorable William Gardner.

These traditions deserve to be shared. This is what this document is intended to do.

Although some of the qualities of our traditions and culture described herein may seem provincial and regionally wedded, these are simply the manifestations of universal concepts and principles relating to American ideals of democracy and civic responsibility to uphold the Constitution and defend the American Republic through a rigorous application of free, fair, open, and honest elections.

These principles, and the manner in which we apply them to our New Hampshire system of elections, can be easily translated to any other state in the nation. New Hampshire state officials from the Departments of State and Justice have been generous in providing straightforward training materials that describe the logistical management details necessary for conducting successful hand count elections. Some of this information is included in this document, and additional resources from these public servants are listed here as well.

National Political Geography Supports Hand Counting

In fact, much of the nation still enjoys hand counted paper ballot elections. The Election Assistance Commission's 2004 Election Day Survey reports the following data regarding national use of hand counting on election night.

- 1,734 hand count jurisdictions among 6,568 jurisdictions nationwide (26.4%)
- Hand counting used for about 1% of ballots in nation

Significant hand count states include the following:

- Wisconsin
- Maine
- Vermont
- New Hampshire
- Texas
- Massachusetts
- Nebraska
- Montana
- Kansas.

California study reinforces need in the Granite State to rid ourselves of secret vote counting technology

In July 2007 California's Secretary of State released a report on testing that she had ordered for computerized voting machines used in California elections. The testing included Diebold optical scanners like those used in 55% of our New Hampshire polling places.

California ran "red team" tests, meant to expose vulnerabilities in the face of intended tampering and fraud. From the report:

Each "red team" was to try to compromise the accuracy, security, and integrity of the voting systems without making assumptions about compensating controls or procedural mitigation measures that vendors, the Secretary of State, or individual counties may have adopted. The red teams demonstrated that, under these conditions, the technology and security of all three systems could be compromised.

California's tests proved the computerized voting equipment used in our elections have no place in a democratic society. They are, in fact, designed with back doors to facilitate election tampering.

Where there are elections, there is intent to commit fraud. The difference between hand count and computerized elections is the scale and opportunity to commit fraud. The old saw about the ballot boxes that end up in the harbor doesn't acknowledge that where hand count elections provide opportunities for retail fraud, computerized elections offer one stop shopping for wholesale fraud.

In New Hampshire we learned the hard way from the 2002 phone jamming scandal, that fraud is typically executed by insiders, often at a high level with access to money and control. California's tests prove the ease in which this can occur with computerized technology:

Consider an attack that replaces the firmware of a voting system with firmware that is malicious. Developing the malicious firmware, and building the software mechanism to install it, requires an expert or team of experts. But carrying out the attack requires only access to a voting system (i.e., someone voting) and not technical expertise.

The computerized voting industry claims that keeping secret the technology counting our votes "protects" the vote count. California's report puts this myth soundly to rest:

[T]he red teams wish again to emphasize the inadequacy of "security through obscurity" as a key defensive mechanism. No security mechanism should ever depend on secrecy. At best, secrecy should be a single security mechanism in a layer of defensive security mechanisms.

Why are New Hampshire citizens allowing the continued use of these machines in our elections?

We pride ourselves on being first in the nation, yet 55% of our polling places continue to use secret vote counting technology!

Every city and town in New Hampshire has the legal right and responsibility to choose its method of state-approved vote counting. In New Hampshire, we have only two approved methods: hand count or Diebold-count.

We can, and should, all say no to Diebold's trade secret vote counting technology.

In March, 2006, the New Hampshire Ballot Law Commission disregarded more than four hours of public testimony and re-approved Diebold optical scanning machines for use in the Granite State.

The Commission applied no standard for approval other than their stated fear that we could not run our elections without them. Only two city clerks testified in favor of approving the machines, giving the same reason: fear of running elections without them.

The Commission approved vote counting technology "protected" by trade secrecy laws; even election officials are not allowed to see how our votes are being counted. They approved secret vote counting (a hallmark of kleptocracy, not democracy), even after they were presented with countless reports and the vendor's own admission of known defects and risks in the equipment.

They displayed an unhealthy addiction to vote counting technology that is decidedly anti-democratic, but which apparently provides some ease in running elections.

The standard for democratic elections is not ease of use.

Diebold optical scanners have fraud-by-design technology, so any insider can flip an election faster than you can say "I want my democracy back".

45% of our New Hampshire polling places hand count our votes. They have developed effective and efficient hand count methodologies. They find community volunteers who are honored to be ballot counters.

In stark contrast to Diebold-sponsored secret vote counting elections, our hand count elections comply with the New Hampshire Constitutional requirement to "sort and count" our votes in "open meeting."

New Hampshire's hand count towns successfully apply a time honored, fully observable, method of ballot counting, yet the New Hampshire Ballot Law Commission approved vote counting machines because they feared we can't hand count our elections.

Our legislature can provide better guidance to the Ballot Law Commission for approving vote counting methods, and can legislate against secret vote counting technologies. Let's hope we see some real movement in this direction in the coming legislative session.

As we continue to defend our first in the nation primary, let's move forward in New Hampshire to be first in the nation in election integrity.

Let's rid the state of secret vote counting. If we can't do it in New Hampshire, what hope is there for the rest of the nation?

Hand Count Basics

MANAGEMENT CONSIDERATIONS

Running a hand count paper ballot (HCPB) election involves good management:

- YOU MANAGE **PROCESS**
- YOU MANAGE **PEOPLE**
- YOU MANAGE **PAPER**
- YOU MANAGE **NUMBERS**

With the right methodology and management in place, the costs come down; the integrity of the election goes up.

METHODS FOR HAND COUNTING PAPER BALLOTS

New Hampshire has identified two accepted and widely used methods for hand counting paper ballots. The sort and stack method is considered more effective and efficient than the read and mark method. This document describes the sort and stack method.

When you have 3-4 people on a team you have built in double checks. You don't necessarily need to rely on post count audits because you are doing simultaneous verification.

In New Hampshire, we have very liberal recount laws, and our manual recounts are integrated into the election system as a natural check and balance on the first counts. The recounts effectively serve as random audits, in this way. But rather than following a statistical formula, the recounts operate under intelligent selection. If a candidate feels something should be double checked, then it is.

WHY HAND COUNTING ON ELECTION NIGHT IS BETTER THEN POST ELECTION AUDITS

There are legitimate concerns about chain of custody if you allow the counting to go past election night, and if you rely on post election "audits" rather than election night first count verification to ensure the integrity of election results.

In New Hampshire, our laws require all counting to be concluded on election night and local election officials may not leave the polls until this is done. Ballot boxes are then sealed and signed by election officials and stored locally unless collected for a recount.

Checks and balances are facilitated by the candidate-requested recounts, which begin the Wednesday of the week following Election Day, and are conducted centrally by the Secretary of State's office; these are manual counts in full public observance.

You can see a state recount online at the Democracy for New Hampshire website:
See our "**We're Counting the Votes and You Can Too**" videos:
<http://www.democracyfornewhampshire.com/node/view/2648>

New Hampshire has some of the most liberal recount laws in the country, and conducts 10-30 recounts every election cycle. Typically at least one outcome is changed in the recount because we tend to have close races – mostly due to the structure of our government, which includes a very large 400+-person citizen legislature (1 rep for every 3089 voters). This is the largest state legislative body in the nation, and provides a fertile ground for our grassroots, participatory culture of democracy.

FOUNDATIONS FOR HAND COUNTED PAPER BALLOT ELECTIONS

Legal Infrastructure: Elected (not appointed) Election Officials

In the Granite State all counting is done at the city ward or town polling places. It is all local. By law, local election officials and jurisdictions make decisions about which State-approved method of counting they will employ.

Each jurisdiction has 8 constitutionally elected election officials. The election (rather than appointment) of community election officials responsible for managing elections results in a fairly intimate grassroots democratic election administration. In this environment neighbors are beholden to each other in the conduct of their elections.

Our elected election officials include the Moderator, Clerk and Selectmen. Additionally, there are a number of appointed election officials as well including, but not limited to, assistant moderator, moderator-clerk-or selectmen pro tem, deputy voter registrars, and ballot clerks (ballot inspectors). The introduction of additional counters to assist at the end of the night would bring more appointed election workers into the polling place and would likely cause the appointed election officials to significantly outnumber the elected election officials.

For this reason, it is important that hand count teams are representative, including members from both of the major political parties as well as independents and other parties that may be represented on the ballot.

Nonetheless, the management of elections by community members elected by their neighbors has a distinct leavening effect on the integrity of our elections.

This is quite different from some of the bureaucratic management of elections seen outside of New England. This community-based election system is very supportive of grassroots democracy, and is one of the reasons visitors to the Granite State often remark that "democracy works" here.

Legal Infrastructure: Voter Intent

New Hampshire has more than 200 years of case law relating to **voter intent**. With solid legal protection of voter intent, New Hampshire's election system comfortably lends itself to hand counting. Voters expressing their political intent with their hand marked ballots, can rest assured that each voter has equal protection under our laws to ensure that their intent is listened to.

The State Election Procedure Manual (<http://www.sos.nh.gov/HAVA/Procedure%20Manual-90403.pdf>) prescribes legally accepted protocols for determining voter intent in disputed cases.

Legal Infrastructure: Paper Ballot is Vote of Record

New Hampshire state law recognizes the paper ballot as the vote of record, and mandates all recounts to be manually counted.

The NH Constitution requires that our votes be "sorted and counted" in "open meeting."

55% of our polling places use Diebold optical scanners and 45% hand count. The New Hampshire legislature, citizen advocacy groups, and the New Hampshire HAVA State Plan Committee, are currently researching questions around the constitutionality of using different vote counting technologies.

In 1994 New Hampshire passed the first paper ballot law in the nation, which states that "no voting machine or device shall be used in any election in this state unless it reads the voter's choice on a paper ballot" (RSA 656.41).

Challenges to Running Hand Count Elections

Staffing is a significant challenge for election officials wanting to run hand count elections. The following observation is offered by an election official in a large New Hampshire city:

"The reality is that we have trouble staffing our polling areas with 9 election officials (moderator, clerk, 3 selectmen, 4 ballot inspectors). Because these officials are all elected or appointed by the parties, there is little accountability if someone chooses to no-show or call in that they will be absent at the last minute. Implying that it would be "easy" to line up 24 people to work each polling area is simply unrealistic. (That would require that [our city] find an additional 135 people to assist at our nine polling places.) It would take the 9 election officials in one of our city wards, where 5,000 ballots may be cast, about 3 hours to hand count their ballots. Add another hour for paperwork, packing, locking up the polls, and returning everything to City Hall, and these folks will be making their returns around midnight. (Our polls are open 6 a.m. - 8 p.m.) I might suggest, however, that there would be value in building a list of the names and telephone numbers of individuals who are willing to volunteer at the polls and to make that list available to the community's chief election official. It would take a lot of non-partisan, discreet manpower, and money, to implement these ideas."

SUPPORT FOR HAND COUNTED PAPER BALLOT ELECTIONS

Community

The Online Etymology Dictionary tells us that the word "vote" is derived from the Latin "votum" meaning "a vow, wish, promise, dedication." This is not surprising. When we vote, we are expressing our commitment to our community. When our community reads our voter intent on our hand marked ballot, it is expressing its commitment back to us. This is the heart and soul of a healthy democracy.

Just as we would not use computers to sign a marriage contract, our hand marked, hand counted paper ballot voting system is as close as we can get to sign and seal our commitment to each other in our communities.

This is why the introduction of cold, computerized, machines into this arrangement is so intuitively unsettling. We have no relationship with these things. They take no oaths of allegiance to us. And they can't sit in a jail cell if they defraud us. These computers, with their complexities, their secret vote counts, their private allegiance to their programmers, their potential for insidious tricks, come between us and our community.

When you remove community from the act of voting, something ineffable is lost. People sense this, and their civic participation in voting declines.

New England in general has long standing traditions of grassroots democracy, from the traditional Town Hall Meeting, to the New England states' original Constitutions, such as in New Hampshire and in Massachusetts, which prescribe the sorting and counting of our votes in open meeting. We New Englanders are used to coming together to slug it out in public, open meeting. We are used to looking our neighbour in the eye while we debate the purchase of a new police cruiser, the opening of a new school, the hiring of a road agent, all these important decisions that we must make together for the collective good of our community.

Communities in New Hampshire often make a celebration out of Election Day. They hold quilt raffles, bake sales, and other sundry events. Adults and children alike invariably find something of interest at the local polls on Election Day, irrespective of their feelings for the candidates and their campaigns in the electioneering zones outside the polling place.

In New Hampshire, being a vote counter is considered a great community honor in the hand count election towns. Volunteers are sworn in on Election Day, and they take their oath of office seriously.

Lyndeborough election official Walter Holland, when training his volunteer hand counters, reminds them to "handle their neighbors' votes with care."

Training

The State invests heavily into poll worker and election official training, and the State also holds forums for our election officials to facilitate information sharing and transmission of local traditions, lessons learned, and what not. The ongoing training and information sharing allows local election officials to learn from the state and from each other, and to continuously improve their skills in election administration. This is critical because of the nature of local elections, which involves citizen officials, all of whom have other jobs, and for whom the election work is primarily a labor of love and virtual volunteerism, undertaken in the election cycle timeframe.

Hand Counting Large Numbers of Paper Ballots, even Complex Ballots

One of our hand count towns counts up to 3600+ ballots on election night. This is an important data point because the national average number of ballots in any precinct is less than 1000. In other words, New Hampshire hand count towns can manage up to 3 or 4 times the

national average of ballots processed in any given precinct. Because of our large legislature, we also have some of the more complex ballots in the nation (many multi-member districts).

At close of the count and reconciliation, local jurisdictions communicate their numbers to the Secretary of State's office for centralized tallying, where the reported results from each city and town are manually entered into a spreadsheet.

Hand Count Systems as Self-authenticating Systems for Election Integrity

With proper management, you can hand count your ballots using teams of 3-4 people, meaning **3-4 sets of eyes on every count, every tally mark, every contest, every ballot**. This is a self-authenticating system. Complex audit protocols, as defined in proposed federal legislation and in some state laws, are moot in this type of system. Because we have identified methodologies that integrate reconciliation into the process of counting, the self-auditing mechanisms are quite advanced and ensure a high level of integrity for the system overall.

In this way, the "auditing" occurs during the first count itself, when it matters, because this, after all, is the count that declares the winner (as opposed to machine "audits" promoted in some national legislative proposals, and in various state laws, which are intended, albeit weakly, to identify problems with the system but not intended to affect outcomes).

Feasibility of Hand Count Elections

Five or so well managed self-auditing teams of 2-4 people can count roughly 1000 ballots in less than 2 hours.

All told, with final reconciliation of registration checklists, number of ballots in and out, etc. the whole process is complete in less than 3 hours on election night. Many New Hampshire counters are community volunteers (all sworn in to office on election night).

New Hampshire has found the local hand count method - using teams of three - costs 7 cents per contest on a ballot, meaning \$1.05/ballot for a typical 15 contest general election ballot.

The State of NH, which conducts 10-30 manual recounts every election cycle, estimates cost for hand counting at around 7 cents per race on the ballot. This is for a 3-person team, each getting paid \$10/hr.

What this means is that it doesn't matter how large is the population of a state or county, it matters how many ballots are processed in any given polling place, and whether or not there is the political and community will and the infrastructural integrity to conduct hand count, observable, self-authenticating, elections.

MANUAL CENTRAL TABULATION

On the day after Election Day in New Hampshire, results are tabulated manually by the Secretary of State's office. The State Police pick up the signed Return of Votes from each town and carry them in manually to the Secretary of State's office by around 8 AM in the morning after the election. The results are then entered manually to a spreadsheet program, and aggregated.

In the case of city wards, the signed Return of Votes from the Wards are manually carried to City Hall and the city results are then aggregated there. The city results are manually carried to the Secretary of State's office.

Lessons Learned from New Hampshire*

**From the NH Department of State: Hand Count Methods and Costs
Address to Democracy Fest Annual National Convention, June 10, 2007
Sheraton Wayfarer, Bedford, NH, By Anthony Stevens, Assistant Secretary of State,*

In New Hampshire, decisions regarding vote counting methods are locally-based, often as included in a town meeting warrant article.

The decision to use a vote counting machine is subject to NH Ballot Law Commission approval. Following are some facts about New Hampshire elections, and why the state provides fertile ground for hand counted election administration.

COUNTING IN NEW HAMPSHIRE

In New Hampshire, approximately 80% of our ballots are counted using optical scan machines, and 20% are hand counted.

- 139 polling places (45%) in NH rely on hand counting
- 170 polling places (55%) in NH rely on optical scanning machines
- 138 jurisdictions (58%) in NH rely on hand counting
- 98 jurisdictions (42%) in NH rely on optical scanning machines

NH has perhaps the highest volume of hand recounts conducted at state level in the nation.

- 10-32 recounts per election cycle
- 50-136 candidates involved per cycle
- Current Secretary of State has been involved in over 300 hand-counted recounts.
- In the 2004 general election, there were 7 hand counting polling places with over 2,500 persons registered to vote.
- Each counted over 2,000 ballots, or over 3 X the ballots cast in an average-sized US precinct.

A WIDE RANGE OF SITUATIONS CALLS FOR DIFFERENT SOLUTIONS

New Hampshire jurisdictions vary widely in their needs.

- Individual New Hampshire polling places served as few as 18 registered voters and as many as 18,974 registered voters in 2006.
- New Hampshire has 7 polling places with over 10,000 registered voters, which is over 6 times the national average polling place size.
- The size of the polling place affects decisions regarding counting methods.
- One size does not fit all.

THE NEW HAMPSHIRE SECRETARY OF STATE'S POSITION

- Supports hand counting and optical scanning counting methods.
- Seeks to identify best practices, recognizing that all ballot counting methods are under scrutiny and will need improvement over time.
- Continues to learn from local officials and promote best practices in counting using hand counting and optical scanning methods.
- Recognizes that there is probably more than one way to count ballots correctly.

Hand Count and Reconciliation Methodology*

**From the NH Department of State: Hand Count Methods and Costs*

Address to Democracy Fest Annual National Convention, June 10, 2007

Sheraton Wayfarer, Bedford, NH, By Anthony Stevens, Assistant Secretary of State, New Hampshire

http://www.democracyfornewhampshire.com/files/Hand_count_training_D-fest_July_5_2007.pdf

The Secretary of State indicates a preferred method in the *New Hampshire Election Procedure Manual*, which is the sort-and-stack method based on observation in recounts.

In this method, many of the steps are similar to the read-and-mark method, also used heavily in the Granite State. Generally, the sort-and-stack method is not used by the Secretary of State in recounts for multi-seat races, although the method can be used by treating every candidate as a separate contest. Local traditions reveal that the sort-and-stack method may not yet be used as widely as the read and mark method in New Hampshire polling places on election night.

ELEMENTS IN HAND COUNT ELECTIONS

Following are the foundational elements that come into play in hand counted elections. These are all described more fully below.

- Planning
- Recruiting
- Knowing your method & how to present it
- Preliminary organizational work
- Training
- Oath of office
- Opening ballot box, counting and distributing ballots
- Tallying votes in contests
- Entering on tally sheet
- Moderator (local election manager) review
- Dealing with discrepancies

RECRUITING COUNTERS & OBSERVERS

Consider the following to help recruit poll workers for hand counted elections.

- Cost estimates of \$10 per hour here are on the high side. Many counters in New Hampshire work for between \$0 and \$5 per hour and are justly proud of their contribution.
- Locations paying \$0-\$5 per hour are some of the most effective at inspiring and recruiting good election night counters of all ages.
- Plan on using a second shift for counting. This makes it easier to recruit people with day jobs
- High school students are now required to contribute community service hours and log them. They are a good target group for recruiting as poll workers.
- 17-year olds qualify as vote counters in New Hampshire & other states.
- Seek a balanced mix.
 - Numbers person
 - Young people
 - Middle aged
 - Older people
 - Managers
- Count your contest equivalents on the ballot, to get a sense of the work needs.
- Know your method.
- Estimate your target number of counters & observers at each table.
- Estimate the number of sets of eyes per ballot.
- Consider using people who have worked all day as observers rather than counters.

Management Primer for Hand Count Elections*

**From the NH Department of State: Hand Count Methods and Costs*

Address to Democracy Fest Annual National Convention, June 10, 2007

Sheraton Wayfarer, Bedford, NH, By Anthony Stevens, Assistant Secretary of State,

New Hampshire

http://www.democracyfornewhampshire.com/files/Hand_count_training_D-fest_July_5_2007.pdf

CALCULATING CONTESTS PER BALLOT

- The number of contests per ballot varies widely.
- In NH, the typical range on a primary or general election ballot is 12 contests, plus questions.

- The NH state representative contest normally is a multiple-seat race, with as many as 26 candidates running for 13 seats in the same district.
 - We would count this example as 13 contest equivalents. When added to 11 other contests on the ballot, the contest equivalents on this ballot should be estimated as $13 + 11 = 24$ contests.

TEAM AVAILABILITY ON ELECTION NIGHT

The following estimates should be adjusted according to how many contests or contest equivalents appear on the ballot.

- 3 hours available (8 PM to 11 PM) X 60 minutes X 60 seconds = 10,800 seconds per team available in one night.

Assumptions:

- Second shift (8-11 PM) brings in fresh counters.
- 20 minutes of training is included in 3 hours

ESTIMATING HAND COUNTING STAFF

Average U.S. precinct in 2006 = 936 registered voters X 67% turnout in general election = 627 ballots X 20 contests/ballot = 12,540 contests to count.

Assumption:

It takes approximately **6 seconds** to hand count a contest on a ballot.

This is based on:

- Videos and interviews with towns that conduct hand counts efficiently
- Secretary of State experience with hand counting
- Experienced towns average 4 - 5 seconds to count each contest on a ballot, including training time, sorting, stacking and counting

Assumptions:

- In NH, general election ballots may contain contests for as few as 12 positions per ballot and contests for as many as 25 position equivalents.
- Multi-seat races are harder to count than races with single outcomes.

CALCULATING STAFF

- 12,540 contests to count X 6 seconds for a team to count a contest in NH experience = 75,240 seconds required on election night, divided by 10,800 (3-member) team seconds available per night = 7 teams needed.
- **7 teams X (2 counters + 1 observer = 3 persons per team) = 21 counters/observers + 3 managers = 24 total staff**

Estimated Staff Costs

21 counters/observers X 3 hours @ \$10/hr = \$630

3 managers X 4 hours @ \$20/hr = \$240

Total: \$870

Using 3 person counting teams:

\$870 per polling place/627 ballots counted @ 20 contests/ballot = \$1.39/ballot, or **\$0.07/contest on a ballot**

The Sort and Stack Method for Hand Counting*

**From the NH Department of State: Hand Count Methods and Costs
Address to Democracy Fest Annual National Convention, June 10, 2007
Sheraton Wayfarer, Bedford, NH, By Anthony Stevens, Assistant Secretary of State,
New Hampshire*

Following are detailed instructions for hand counting using the sort and stack method.

OVERVIEW OF SORT AND STACK METHOD

I. Ballots are sorted into piles:

- One pile for different categories
- Each candidate or alternative on a question
- Overvotes (defective in that contest)
- Undervotes (skipped races)
- Write-ins
- Ballots requiring voter intent judgment calls for the moderator (local election manager)

ADVANTAGE OF SORT AND STACK METHOD

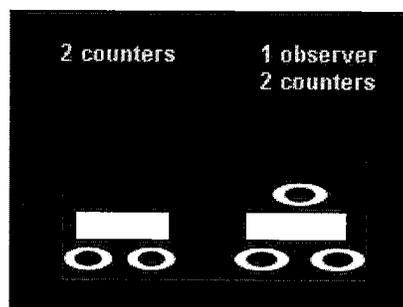
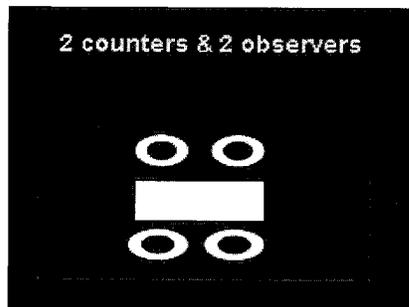
- Counters and observers are looking at only one candidate or question on the ballot.
- Counters' and observers' eyes do not have to move to different locations on the ballot and on the tally sheet.
- Counters and observers have to focus on getting only one thing right. When looking for evidence of only one mark on one precise location on the ballot, it is harder to make mistakes.
- Recording the number of votes for a candidate or question is done when the stack is counted.
- Other methods rely on a separate mark on a tally sheet being made with each ballot. This requires more sets of eyes to track accurately.

RULE OF THUMB FOR SORT AND STACK

- Aim for at least 3 sets of eyes on each ballot, and each vote recording.
- Using a 2-person team, that might mean that both members watch as one member sorts the ballots.
- At least one member checks the marks again when counting the number of ballots in the stack.
- Both members count each pile and record and check the sum on the tally sheet.

CHOOSING NUMBER OF SORT AND STACK OBSERVERS

- The more sets of eyes on a single ballot, the greater certainty in the results.
- Generally, this means the more observers, the greater degree of certainty in the results.
- (Still, using the sort and stack method, 2 counters (no observers) can apply 3-4 sets of eyes to each ballot, and still achieve accuracy.)
- An extra set of observers for 7 teams would cost \$210 (7 observers X 3 hours X \$10/hour) in an average US polling place counting a 20-contest ballot without volunteer help.
- New Hampshire recounts rely on observers selected by the candidates, often resulting in tables with 4 or 5 persons – 2 counters and 2-3 observers.



ORGANIZING FOR THE COUNT

- Close the polls
- Verify all absentee ballots processed
- Rearrange the polling place for counting
- Have the checklist (pollbook) supervisors count the number of voters who are checked off as having voted.
- Identify those who will be counting.
- Identify those counters who have not yet taken the oath of office.

OATH OF OFFICE

Swear in non-election officials as election officials

"I, (state your complete name), do solemnly swear (affirm), that I will bear faith and true allegiance to the United States of America and the State of New Hampshire, and will support the constitution thereof. So help me God. This I do under the pains and penalties of perjury.

Alternate language for those scrupulous of swearing, or mentioning God in this matter, is set forth in italics.

TRAINING

- Read the instructions for counting to all the election officials who will be counting.
- Provide clear directions regarding method to achieve consistency.
- The moderator (senior local election official) has control and should exercise it.
- If people insist on using another counting method, consider asking them to act as an observer.
 - *Observing the counters count is a key role and helps achieve accuracy.*
- Oath of office and training take 20 minutes.

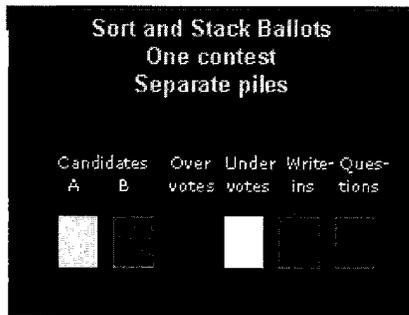
STEPS TO IMPLEMENT SORT AND STACK METHOD

Distributing ballots to teams

1. Open the ballot box in view of the public.
2. Place an established quantity of ballots on the table to be used by each counting team.
3. Both members count the ballots in groups of 50.
4. If it becomes necessary to redo a particular part of the process because the results do not equal the number of ballots, counters can afford to recount 50.
5. Counting by stack facilitates continuous self-auditing and ongoing reconciliation of the count.

Start counting ballots

6. Team members should look at each ballot to ensure it is sorted into the correct pile.
7. Once each table has the ballots assigned to it sorted into the six piles, start the counting process with the pile of ballots for the first candidate on the ballot.
8. All other ballots should be set aside, but remain in public view on that table.



Counting ballots

9. The team should count the ballots in the first candidate's pile into groups of ten.
10. Stack each group of ten ballots and the remainder at right angles to each other on the same pile.
11. Both counters count the piles of ten, plus remainders, agree on the number and enter it in the tally sheet.
12. Counting in stacks of ten facilitates ongoing reconciliation of votes and ballots counted during the count.

Tally Sheet – single contest

	Candidate A	Candidate B	Candidate C	Under vote	Over vote	Write ins	TOTAL
1st group of 50 ballots	19	17	9	4	1	0	50
2nd group of 50 ballots	17	22	8	3	0	0	50
3rd group of 50 ballots	16	18	11	3	1	1	50
4th group of 50 ballots	18	20	9	2	0	1	50
TOTALS	70	77	37	12	2	2	200

Next candidate, same contest

13. Then begin counting the next candidate in the same contest.
14. When all the piles have been counted and checked, that counting team is done with that set of ballots for that candidate in that contest.
15. Counters agree on the number to enter on the tally sheet.
16. If there is another candidate in that contest, counters count the pile for that candidate and agree on the number to enter on the tally sheet.

Same contest, counting the piles of undervotes and overvotes

17. Counters count separately the piles for undervotes and overvotes and agree on the numbers to enter on the tally sheet.
18. The team should add the votes for each candidate (including write-ins) and the number of undervotes (skipped/abstentions) and overvotes (defective) in that contest.
19. Enter the total in the far right column of each row. It should equal 50.

Next contest

20. Begin the sorting and counting process for the first candidate in the next contest.

21. When all piles for that contest have been counted, checked and entered on the tally sheet, that counting team is done with that set of ballots for that contest.
22. The team should add the votes for each candidate (including write-ins) and the number of undervotes (skipped/abstentions), and overvotes (defective) in that contest. That number should equal 50.

Tallying

23. Tally sheets should be turned in - after the numbers equal 50 on the far right, and the aggregate of votes = 200 on the bottom right.
24. Tally sheets should be signed by the counters before being turned in.
25. Moderator should designate someone who routinely works with numbers to tally and check the team tally sheets.

Moderator (local election manager) Review

26. The moderator (manager) should stop before announcing the results and check the final tallies.
27. If a count was done of the total number of persons checked off as having voted on the checklist, the aggregate tallies for each contest (office or question) should be verified against that count.
28. The total votes for all candidates (including write-ins) in a single contest, plus the undervotes (skipped/abstentions) in that contest, plus the overvotes (defective) in that contest, should equal the total number of ballots used.

Dealing with Discrepancies

29. The moderator should be looking for any significant discrepancies between the totals. It may be difficult to get a perfect count from the checklist (pollbook).
30. It is not essential that the total count for each office or question exactly match the total of those checked off on the checklist (pollbook).
31. Provided the write-in, undervotes (skipped/abstentions) and overvotes (defective) were tallied, the totals from one contest to the next for the same set of ballots should be the same (50 per batch).
32. Tally sheets from each team should be carefully checked as each contest is counted. Reconciliation should be kept current during the night.
33. Any mismatch of votes per contest with number of ballots per batch should be addressed immediately.
34. When the last tally sheet is handed in for the last race, reconciliation should be largely complete. Little tally work remains.
35. If any discrepancies are found, the moderator should investigate and attempt to resolve the discrepancy before declaring the results.

Advantages of using tally sheets to track undervotes and overvotes

- Tally sheets permit ongoing reconciliation (number checking) as the count progresses.
- Surprises at the end are less likely.

Election Night Reconciliation*

** From the NH Department of State: Election Procedure Manual
<http://www.sos.nh.gov/FINAL%20EPM%208-30-2006.pdf>*

Moderators are obligated to ensure that votes are counted accurately. (RSA 659:60.)

Moderators are strongly encouraged to adopt an election night reconciliation procedure that checks the apparent results of the ballot counting against other known election statistics to ensure that the results are accurate.

It is inherent in the nature of an election night count, particularly at polling places that hand count ballots, that even the most careful election officials can make mistakes. Most of the officials conducting the counting will have been working for 12 or more hours before the counting process starts. Often the counting is done under the pressure of the candidates, the public and the press watching and anxiously waiting for the results. Therefore, taking the steps described below to ensure that the count is accurate is necessary.

Each election, a small number of polling places report results which are conspicuously inaccurate. The results report votes for the candidates in a given race that when added together total more than the reported number of ballots used, or more than the total number of voters reported as voting. In most cases, an inquiry by the Secretary of State or a recount disclose a counting or tabulation error. Either mistakes are made when tallying up the counts done by individual teams doing hand counts or errors are made in the manner in which ballots which were machine counted but contain write-in votes are counted.

When election night results are invalid on their face, this diminishes the public's trust in our election system. It often results in a call for a recount. Finding and correcting easily identifiable errors on election night is less work and less expensive than a recount.

A great deal of effort is taken to afford every qualified voter the opportunity to vote quickly and easily. That effort is ineffective unless every vote is accurately counted. Voters deserve the extra effort that is required to conduct a reconciliation of election night results with other election statistics.

BALLOT INVENTORY

The inventory of ballots is the starting point for the election night reconciliation of ballot counts. The ballot inventory establishes a baseline of how many ballots were used at the election. The moderator and clerk are required to keep track of the ballots made available for use at the election and those actually used. The Return of Votes that must be filed with the Secretary of State requires a report of the number of ballots used.

The Ballot inventory should start with determining the number of ballots received from the Secretary of State ("SOS"). During the counting process, determine the number of ballots produced by the Accessible Voting System ("AVS") the telephone – fax voting system that must be available for use by voters with disabilities.

The number of absentee ballots must be determined. This can be done during the hand count by segregating the ballots or this can be kept track of during the processing of absentee ballots. At elections where federal office only ballots are used, these will always be absentee ballots, the number of these ballots should be kept track of separately. When reconciling the votes cast for federal offices, these federal office only ballots should be included in the calculation of the total number of ballots used at the election. When reconciling the votes cast for state and county offices the number of federal office only absentee ballots must be subtracted from the total number of ballots used.

BALLOTS USED

Determine the total number of ballots used at an election as follows:

Election Day Ballots received from SOS =	_____
+ Ballots from IVS	_____
+ State Absentee Ballots Cast	_____
+ Federal Office only Absentee Ballots Cast	_____
+ Absentee Ballots/Photocopy ballots used for election day ballots	_____

- Spoiled Ballots _____
- Election Day Ballots not used _____
- = **Total Ballots Cast at the Election** _____

COUNTING NUMBER OF VOTERS VOTING

The Return of Votes form requires that the number of voters checked off on the checklist as having voted must be counted and reported.

HAND COUNT POLLING PLACES. In a hand count town the check-in checklist should be counted and compared to the check-out checklist to establish the number of voters who voted.

MACHINE COUNT POLLING PLACES. In a machine count town the number of voters checked off on the check-in checklist should be compared to the results tape from the ballot counting machine. The total ballots counted reported on the end of the election results tape must be added to the number of ballots that had to be hand counted. Typically a small number of ballots are rejected as not readable by the Accuvote optical scanning machine. These should be put in the side pocket during polling hours and hand counted after the polls closed. These ballots, which are entirely hand counted, are not included by the machine in its report stating the total number of ballots counted. Other ballots which contain write-in votes or which were read by the Accuvote machine as entirely blank will be found in the write-in bin beneath the machine. These ballots are included in the total ballots counted reported by the machine. Do not add them in twice.

The total from the tape plus the number of completely hand counted ballots is a statistic that serves the same function in a machine count town that the check-out checklist serves in a hand count town. This total of ballots should be compared to the number of voters checked off as having voted on the check-in list to determine the total number of voters who voted.

TOTAL VOTES COUNTED

The next step in reconciliation is to determine the total votes counted for each contested office or question. To effectively reconcile the election night results it is necessary to count not only votes for candidates in a race but also the number of voters who skip the race, that is abstain (submit a ballot with no candidate marked for that race). A ballot in which the voter overvoted, that is marked two or more candidates for a race where the instruction is to vote for no more than one, should for this purpose be treated as a skipped or abstention. The same applies in a multi-seat office where the voter votes for more than the permissible number of candidates. Because the voter may only vote for the permitted number and it is impossible to determine which candidates the voter preferred most, the ballot is treated as if the voter did not vote for anyone for that office.

RACES BLANK, SKIPPED, OVERVOTED AND ABSTENTIONS. In a hand count polling place the counting teams should be instructed to record the number of ballots where the voter skipped or abstained from voting in the race and the number where the voter overvoted. These numbers must be reported along with the total number of votes for each candidate and write-in.

The ballot counting machine automatically records as a "blank" each ballot where the voter skipped the race or abstained or where the voter overvoted. It is necessary to count the abstentions and overvotes only on the ballots that are entirely hand counted. If entirely blank ballots are found in the write-in bin which were improperly marked and can be hand counted, it will be necessary to subtract that ballot from the total blanks reported on the machine tape for every race where a vote is counted for a candidate.

VOTES CAST FOR AN OFFICE

To determine the total votes cast for an office:

- For each office (vote for no more than one):
- All votes for first candidate _____

+ All votes for second candidate _____
 + All voters for each additional candidate _____
 + All write in votes _____
 + All blank/skipped/abstention/
 overvote ballots _____
 = **Total votes counted for the office** _____

Reconciliation. The election night results are reconciled if each of these statistics are equal for each contested race or question.

Ballots used = _____
Voters Voting = _____
**Total Votes Counted for the
 Office/Question** _____

Small differences in the number of ballots used, number of voters voting and the total number of votes counted for an office or question sometimes occur even when counts are accurate due to human error in marking the checklist. Under no circumstances should the total votes counted for an office or question exceed the total number of ballots used or the total number of voters voting. Every effort should be made to resolve any discrepancies of this character. Errors in the other direction, where there are fewer total votes counted than ballots used or voters voting are problematic, but do not create conspicuously invalid results.

If you are certain there is no counting error, declare the final results even if a small difference exists. Occasional human error in checking the checklist as voters check in or in counting large numbers of blank ballots when determining the number of ballots used are unavoidable. Make the existence of that difference part of the record of the results. The difference usually will not be an issue, unless the margin of victory is less than the difference. In that case, a candidate will often request a recount.

EXPECTED UNDERVOTE

A second approach to reconciling election night results is to compare the total votes counted for each candidate and write in the total number of voters voting/total number of ballots used and assess whether the undervote makes sense. At every election a certain number of voters will abstain in certain races, i.e. they will not vote for any candidate. Alternately, they will purposefully or by error vote for too many candidates, an overvote, thereby casting a ballot with the same effect as an abstention.

The rate of such undervoting is reasonably stable for the races at the top of the ballot. At elections where voters are voting for President of the United States, an undervote of 1/2 of one percent (.005) is common. Therefore, when reconciling the apparent results at an election where President is being voted for, if your results suggest that more than 3% (.03) of the voters did not vote for President, this is a warning sign. This result is possible, but should prompt the moderator to recheck the results before announcing them.

At an election where the Governor is the top candidate on the ballot, the undervoting rate is less constant, but generally should be less than 5% (.05). The same is true for candidates for United States Senate. If the apparent election night results indicate that more than 5% of the voters did not vote for Governor or United States Senator, the moderator should re-check the numbers before announcing the results.

The undervote rate for Representative to Congress can average around 4 – 5%. Therefore, results indicating that more than 7% of the voters did not vote in that race should prompt a review of the numbers. The undervote rate for offices below these on the ballot is too unpredictable to be helpful in reconciliation. However, it is sometimes the case that if an error is found regarding a top-of-the-ballot race, for example that the results from a hand count team were omitted from the tally, that error will have affected all the races and questions on the ballot. Checking the

undervote for the top of the ballot races is another effective way to identify problems with the tallying.

Analysis And Figures For Nationwide Costs of Replacing DREs With Paper Ballot Voting Systems

Following are realistic numbers for replacing Direct Electronic Recording (DRE) systems with paper ballot systems – optical scanner and hand count, including transitional costs such as training, configuration and integration.

REPLACING THE NATION'S DRES WITH OPTICAL SCANNERS

According to Election Data Services in 2006 there were 69,382 precincts (1,142 counties) using DRE voting systems.

Optical scan device \$5,000/ea
Programming \$500/election

Assuming 100% replacement for one device per precinct:

69,382 precincts X \$5,500 = **\$381,601,000.**

To allow for back up devices, add an additional device for every 4 precincts (shared backup):

$\$381,601,000 \times 1.25 =$ **\$477,001,250**

Adding Replacement of DREs for Disability Compliance

Ballot Marking Device \$6,000/ each

69,382 precincts X \$6,000 = **\$416,292,000.**

Integration, training and recruitment rough estimate is \$4,000 per precinct:

69,382 X \$4,000 = **\$277,528,000**

TOTAL COST FOR DRE REPLACEMENT WITH PAPER BALLOT OPTICAL SCAN EQUIPMENT: \$477,001,250 + \$416,292,000. + \$277,528,000 = \$1,170,821,250

REPLACING THE NATION'S DRES WITH HCPB ELECTIONS

In New Hampshire, we have collected information on hand count costs through many years' experience of manual state wide recounts, and through limited surveys of NH hand count towns. Generally, hand count towns estimate their election costs at around \$700 / election, with some of our NH hand count towns counting up to 3,600 ballots per polling place.

New Hampshire hand count towns count up to 3-4 times the national average of ballots processed in any given polling place (the national average is 1000 ballot / polling place) - but we have not found the cost to vary much. This is largely due to the level of volunteerism among hand counters, who come to count because it is considered an honor within their community, rather than to get paid.

Using proper management and efficient processes, hand counting requires 5 teams of 4 people (2 counter/tallyers and 2 observers) to count 1000 ballots in about 2-3 hours. This is accounting for a typical general election ballot, consisting of 12-15 races.

The State of New Hampshire, which conducts 20-30 manual recounts every election, estimates costs for hand counting at around 7 cents per race on the ballot. This is for a 4-person team, each getting paid \$10/hr.

For a general election ballot of 15 races; this comes to \$1.05 / ballot.

NOTE: New Hampshire ballots are among the most complex in the nation, because of our large legislature, consisting of 400 state reps. This means New Hampshire has many multi-member districts. These races are more complex and time consuming to count than a typical one seat/district race with only a handful of candidates running for that single seat. For instance, a single district in New Hampshire might have as many as 26 candidates running for 13 seats. This means that hand counters are counting the votes for each of those 26 names. Obviously, this takes more time than counting a 2-3 person race running for one seat.

For a typical average precinct by national standards (1000 ballots per precinct), a hand count election would cost 1,000 ballot X \$1.05cents = \$1050.

For our **69,382 DRE** precincts, Election Data Services gives us the number of **65,959,464 registered voters**. If every registered voter cast a ballot:
 $65,959,464 / 1000 = 65,959 \times \$1050 = \mathbf{\$69,256,950}$

For hand counting voting systems to replace DREs, you would need to incorporate sufficient management staffing, training and recruitment funds.

Management, training and recruitment rough estimate is \$2,000 per precinct:

$69,382 \times \$2,000 = \mathbf{\$138,764,000}$

TOTAL COST FOR DRE REPLACEMENT WITH PAPER BALLOT HAND COUNT SYSTEM PLUS REPLACEMENT DISABILITY UNITS: \$69,256,950 + \$138,764,000 = \$208,020,950

Supporting Information for the Elimination of DREs

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) STUDY 2006

I. Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC

2.1 DRE Systems and Security

DRE machines are essentially notebook computers programmed to display ballot images, record voter choices, and store the electronic CVRs on removable memory cards. They are comparatively easy to use, particularly by those with impaired vision; they can also produce an audio ballot for blind voters. They typically produce a start-of-day zero report and an end-of-day summary printout of the ballots cast on the machine, but they do not require or produce paper ballots, and it is this aspect that has helped to make them popular with election officials who have had to deal with logistical and accuracy problems and historical fraud in handling and counting paper ballots.

But many people, especially in the computer engineering and security community, assert that DREs are vulnerable to undetectable errors as well as malicious software attacks because there is no audit mechanism other than what the DRE can report on: how many records it has stored, ballot styles, etc. Potentially, a single programmer could "rig" a major election. ***The computer security community rejects the notion that DREs can be made secure, arguing that their design is inadequate to meet the requirements of voting and that they are vulnerable to large-scale errors and election fraud.***

One conclusion drawn by NIST is that the lack of an independent audit capability in DRE voting systems is one of the main reasons behind continued questions about voting system security and diminished public confidence in elections. NIST does not know how to write testable requirements to make DREs secure, and NIST's recommendation to the STS is that the DRE in practical terms cannot be made secure. Consequently, NIST and the STS recommend that VVSG 2007 should require voting systems to be of the SI [software independent] "class," whose

readily available (albeit not always optimal) examples include op scan and DRE-VVPAT.

The widespread adoption of voting systems incorporating paper did not seem to cause any widespread problems in the November 2006 elections. But, the use of paper in elections places more stress on (1) the capabilities of voting system technology, (2) of voters to verify their accuracy, and (3) of election workers to securely handle the ballots and accurately count them. Clearly, the needs of voters and election officials need to be addressed with improved and new technology. The STS believes that current paper-based approaches can be improved to be significantly more usable to voters and election officials, and that other kinds of all electronic IV (software IV) and E2E cryptographic systems may possibly achieve the goal of secure paperless elections. **However, for VVSG 2007, the STS judges that designs for these new systems are still immature and that developing testable requirements for these approaches is not yet feasible. Industry has not yet responded in a significant way with new designs, and some method for jumpstarting industry to design and market these approaches may be beneficial.**

These systems may be dependent on software to an extent, however not nearly to the extent that today's DREs rely on software correctness. How this software would be specified and tested remains a matter of debate. **Currently, the STS is divided on whether software IV [independent verification] systems are possible to secure at this point without further research.**

ELECTION SCIENCE INSTITUTE STUDY 2006

II. The Election Science Institute Study of DRE VVPAT for Cuyahoga County showed a ten percent error rate for VVPAT printouts, rendering these votes unreadable and unusable for hand counts in an audit or recount situation.

Following the 2004 General Election in Ohio, Cuyahoga County adopted a new voting system using the Diebold touch-screen voting system. The new system complies with both the new federal election technology standards established under the Help America Vote Act of 2002 (HAVA) and with recently enacted Ohio legislation that requires voting systems to produce a paper ballot that can be verified by the voter. Under Ohio law, this paper ballot (Voter Verified Paper Audit Trail (VVPAT) serves as the official ballot in the event of recount or contested election. The May 2006 Primary, the first major election using the new system, presented an opportunity to assess the new system's benefits and weaknesses. The Cuyahoga County Board of Commissioners decided that an independent scientific analysis of the Primary election would give elections officials objective feedback on the accuracy, reliability and usability of the new voting system.

In April 2006, the Cuyahoga County Commissioners engaged Election Science Institute (ESI) to study all aspects of the new system during the Primary Election. Voting devices are only a small part of an election system: any thorough assessment of a voting system must include an evaluation of the administrative procedures, pre-election programming and testing of the machines, voter and booth worker interaction, and counting and auditing procedures. Although the touch screen systems are vastly different from optical scan and punch card, it still holds true that an election will be only as successful and reliable as the human administration of all system components.

Summary of Key Findings

Key Finding: After three months of exhaustive research, empirical evidence supports the key definitive finding: ***The machines' four sources of vote totals – VVPAT individual ballots, VVPAT summary, election archive, and memory cards – did not agree with one another.*** The current election system appears to provide some of its promised benefits at potentially great cost; namely, that the election system, in its entirety, exhibits shortcomings with extremely serious consequences, especially in the event of a close

election. These shortcomings merit urgent attention. ***Relying on this system in its present state should be viewed as a calculated risk in which the outcome may be an acceptable election, but there is a heightened risk of unacceptable cost.***

Manual Count of Paper Ballots

Key Finding: VVPAT's were missing, missing information and the tally of the individual ballots did not always match the VVPAT summary printed at the end of Election Day. In order to validate the accuracy of Election Day vote tabulations by the Cuyahoga County BOE Diebold voting system, ESI conducted a manual count of the VVPAT paper ballots. Using a recount fixture that allowed for viewing the tapes without handling them, a team of election officials, booth workers and students tallied the votes for governor on each tape. The paper ballot tallies were initially compared to the results report printed on the VVPAT tapes. When the count did not match the count provided by the results report, the paper ballots were recounted.

- ***85% of the VVPAT Ballots and VVPAT Summaries reconciled after the primary manual count, where approximately 15% required a secondary count***
- ***1.4% of the VVPAT cartridges exhibited missing ballots.***
- ***16.9 % of VVPAT tapes showed a discrepancy of 1 - 5 votes between the tally of ballots and the results report; 2.1 % showed a discrepancy of over 25 votes.***
- ***During the manual recount, team members discovered 40 VVPAT tapes (9.66%) that were either destroyed, blank, illegible, missing, taped together or otherwise compromised.***
- Identifying information on the VVPAT tape such as precinct information and machine identification was inconsistent, as were the summary reports printed at the end of the day. 2.8% of the VVPATs were missing machine ID numbers; 5.4% did not identify the precinct, increasing the difficulty of a meaningful audit and raising questions about the integrity of the vote count.
- VVPATs showed evidence of booth workers using trial and error to print reports and start up or close down the machines; workers apparently attempted to overcome printer problems by shutting down machines, removing and replacing cards, and restarting machines.
- 72% of the labels identifying canisters containing the VVPAT tapes were missing information. 46% of the canister labels were blank.
- Booth workers frequently failed to sign the tapes. Such failures in chain of custody also increase the risk of a legal challenge.

RESOURCES

Election Data Services 2006 Voting Equipment Report

http://www.edssurvey.com/images/File/ve2006_nrpt.pdf

NH Department of State: Improving Disability Access for Voters

http://www.democracyfornewhampshire.com/files/Dem4NH_DisabilityVoting.pdf

NH Department of Justice: Counting and Reconciliation on Election Night

http://www.democracyfornewhampshire.com/files/democracyfest_reconciliation_handcounting.pdf

NH Department of State: Hand Count Methods and Costs

http://www.democracyfornewhampshire.com/files/Hand_count_training_D-fest_July_5_2007.pdf

Democracy for New Hampshire: "We're Counting the Votes" videos

<http://www.democracyfornewhampshire.com/node/view/2648>

Democracy for New Hampshire: "We're Counting the Votes" booklet

<http://www.democracyfornewhampshire.com/node/view/2606>

Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC,
William Burr, John Kelsey, Rene Peralta, John Wack, National Institute of Standards and
Technology, November 2006

ESI Study of DRE VVPAT for Cuyahoga County

http://www.votingindustry.com/TabulationVendors/1stTier/Diebold/esi_cuyahoga_final.pdf

NH Department of State: Election Procedure Manual

<http://www.sos.nh.gov/FINAL%20EPM%208-30-2006.pdf>

NH Department of State: Election Laws

<http://www.sos.nh.gov/statutes.htm>

DRAFT

From: Michelle Gabriel
Sent: Wednesday, August 01, 2007 3:19 PM
To: Voting Systems
Cc: Voting Rights; CEPN
Subject: Comments for Top to Bottom Review

Dear Top to Bottom Review Committee:

Thank you for your work. I attended the hearing and I have some comments and suggestions.

1. The deadline for decertifying is this Friday, but that only effects the primary. There are other deadlines for the June 2008 and November 2008 elections. I think that given there was not enough time to do a full review, that some changes should be made for Friday but that further work and changes can be made for the other elections.

a) One suggestion for this Friday's decision is to :

1. Decertify any equipment that was NOT submitted for the review. These suppliers have shown that they do not want to do business with this state by disregarding the request.

2. Decertify any equipment that shows the possibility of viral or wholesale fraud. There were questions asked and answered at the hearings that point to this information being available in the private reports.

3. With the remaining equipment - require for the February primary that all counties use hand marked optical scan, with or without precinct based optical scan machines, and one DRE, Automark or other accessible device either per county or per precinct for disabled access. In this way, given that all counties have central optical scan for counting absentee ballots, they would have to buy a minimum amount of equipment.

4. Implement a risk based audit that will be worked out in detail prior to the February primary. Work with County Elections officials on best practice policies and procedures for carrying out the audit, and help with all operational details that these officials may face. Such audits will be necessary no matter what kind of system, including hand counts, is put into place.

b) Please work with the Attorney General to sue the voting system vendors for providing equipment that does not meet contractual agreements, etc etc. Try to get the money back!!!

2. The further work that should be done is exactly what the County Elections Officials asked for - testing in a real world environment, not a laboratory. No more sitting in a room and thinking good (or bad) thoughts, no more mitigations that are never tested, results that can't be checked, etc. By actually showing a smoking gun or not, we should be able to see if the security mitigations are as good as we are told.

A) Mock election - perform a mock election for a county that has real equipment, real polling sites, real poll workers recruited, real hours, real chain of custody, real mitigations, etc etc. Have a red team attack based on all PUBLIC information and also given certain levels of INSIDER information. Let's see if the election can be hacked. Have the voting be on a typical long ballot but for fun things that the common citizen will vote on. (I think that American Idol gets more votes than a real life election.)

B) Another option would be have a real election but add a bogus item to vote on as the goal for the hackers. This would be very difficult to

do since it is a felony to fix an election in anyway but I'm sure the legal teams of the state could figure out how to deal with that.

Sequoia agrees with me. Here is what the Sequoia representative says: In summary, a more effective test would have been for the Red Team to have attacked a simulated target jurisdiction. Said jurisdiction would have prepared the equipment in keeping with traditional, current, and legally mandated equipment and procedural safeguards. The results of this test would have pointed out true weaknesses in election process security and provided real data from which governments could have improved their security profile.

Obviously, the SoS should set up the limits of the mock election, not the vendors.

3 If you are thinking of any new mitigations, ...

a) please look at the complete system implications. The VVPAT was supposed to be a mitigation - instead it is a multi-million dollar fiasco. Many activists tried to stop these from being certified for all the reasons that elections officials now complain about them - unreliable, hard to handle, more pollworker training, denial of service attack - but to no avail. Please don't put in a new mitigation that will cause unintended consequences. At the hearing I spoke on the tamperproof tape. What if it is tampered with? Is there a policy of what to do with those votes on those machines? Can such a policy be used in a "vote annihilation" attack if the votes from those machines are not counted?

b) The elephant in the living room for elections officials is what to do if the mitigations are penetrated. This has to be made clear before any mitigation is considered "acceptable" A mitigation only works if when it is penetrated there is a way to tell it has been breached and way to deal with the breach. If not, what is the point of having the mitigation?

4. If there are no mitigations that can work, please state that clearly and why. There may be some security flaws so grievous that nothing is good enough to stop it.

5. If you are going to allow systems to be used with mitigations, please examine the mitigations currently in use and evaluate them as to not just how easily they could be penetrated but also how many times in a real election they are not fully implemented. At the hearing I stated a few of them. There are many many more. Please read all postings of incidents to judge whether these security measures are really a viable layer of security and the consequences of their not working. I have much information on this and would be available to share it with you if needed.

Thank you for reading my comments.

Michelle Gabriel

From: Ardis Bazyn [
Sent: Wednesday, August 01, 2007 3:53 PM
To: Voting Systems
Subject: Comments on Top to Bottom Review

BAZYN COMMUNICATIONS

“True Vision With Insight”

August 1, 2007

The Honorable Debra Bowen
Secretary of State
1500 11th Street, 6th Floor
Sacramento, CA 95814

Re: Comments for the California Top-to-Bottom Voting Systems Review “Final Accessibility Review Report”

Dear Secretary Bowen:

As one of the original Advisory Committee members to assist in writing the state plan for the Help America Vote Act of 2002 (HAVA), I have participated in many ad hoc and ongoing committees in California on voting issues. I have represented the California Council of the Blind in many hearings, accessibility committees, and also volunteer on the Los Angeles County Specific Needs Committee. CCB has often partnered with other groups of people with disabilities in order to support their rights to equal access, independence, and privacy.

I have reviewed the July 26, 2007 Accessibility Review Report for California that concludes the Hart, Sequoia, and Diebold electronic voting systems to be non-compliant with the accessibility requirements of HAVA and the 2005 Voluntary Voting System Guidelines. I want to express concern that the report’s findings may lead to a decision to decertify all or some of these voting systems disenfranchising countless Californians with disabilities from exercising their right to an accessible, private, and independent vote. Our CCB membership has long advocated for accessible voting machines. The Accessibility Report identifies deficiencies with the reviewed systems and also recommends short term solutions for elections and long term mitigation strategies to address the deficiencies. We agree that a short term strategy can mitigate a number of the identified problems.

08/02/2007

The report does not recommend decertification of any or all of the systems as either a short or long term strategy. We agree with this finding as well. Decertification, without an identified and readily accessible replacement system, would result in the inability of our members to vote with independence and privacy. This would be in violation of federal and state law. We support you in adopting short term remedial mitigation measures for the 2008 elections as an alternative to decertification. We urge you to advise County election officials as well as the Hart, Sequoia, and Diebold vendors to implement the measures identified in the report.

For the long term, we urge you to actively seek out, review, and certify new technologies and voting systems that refine and enhance the promise of an accessible, private, and independent vote for Californian's with disabilities. We would urge you to give an adequate time frame for advocates to participate from around the state. In this particular process of the review and certification hearings, the time-line was very short. We look forward to working in collaboration with you and disability rights advocates to ensure that the voting needs of people with disabilities, particularly the visually impaired, are fully understood and addressed.

Sincerely,
Ardis Bazyn
California Council of the Blind, Voting Rights Representative

From: Steven Rosenfeld
Sent: Wednesday, August 01, 2007 4:20 PM
To: Voting Systems
Subject: Ohio suit shows faulty audit logs

Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, CA 95814

Dear Secretary Bowen,

I'm writing because ongoing litigation challenging the results of a 2006 judicial election in Columbus Ohio has highlighted serious problems with vote count accuracy and audit logs in ES&S's iVotronic voting systems.

Unfortunately, many people who testified on Monday in opposition to DREs did not cite specifics. However, the record in *Squire vs. Geer* (Franklin County Court of Appeals, Case No. 06-APD-12-1285) could provide a basis for decertifying certain DREs.

Magistrate Joel Sacco found, "For the November 7, 2006 general election, in 721 out of 835 Franklin County precincts, the public count on DREs did not equal the number of signatures in the poll books plus provisional votes cast minus the number of cancelled votes." This means 86.3% of the precincts had vote totals that failed to match signatures in the poll books. The BOE "reported 2,824 more votes cast than signatures scanned," the court found.

Equally important, however, was the breakdown of the machine's audit systems, specifically the real time audit log paper rolls, which prevented a fair and accurate recount.

Apart from administrative breaches of protocol, such as opening sealed audit logs without observers present, there was expert testimony that many of the actual paper rolls were incomplete. At the end of rolls where the vote tally is printed, figures either were missing, incomplete or only zeros appeared. In some cases, the printers ran out of paper before all votes were totalled. In court, Rebecca Mercuri, Ph.D. estimated 5% to 10% of the audit logs malfunctioned.

This is a summary of testimony given under oath and an Ohio magistrate's findings. Below are links to two articles, while partisan in tone, nonetheless elaborate on these points.

Sincerely,

Steven Rosenfeld

Co-author of "What Happened in Ohio: A Documentary Record of Theft and Fraud in the 2004 Election" (The New Press, 2006)

<http://www.freepress.org/departments/display/19/2007/2712>
<http://www.freepress.org/departments/display/19/2007/2719>

08/02/2007

From: Brina-Rae Schuchman
Sent: Wednesday, August 01, 2007 2:11 PM
To: Voting Systems
Subject: Please Make Voting True Again

To: CA Secretary of State Debra Bowen and staff and testing people.

Dear Secretary Bowen,

Thank you for working so hard and caring so much about election integrity and democracy in America to do the top to bottom review of computerized election machines, to the extent you have had time for it.

You are spending a lot of time and money to see if there is any way that the vendors computers might be ok for voting.

It is necessary because the fault-filled computers have been sold and distributed everywhere. It is unfortunate, because

they can not be ok for voting. It is like expecting a real horse to act like a painted horse on a carousel.

Vendors can call a computer a "voting machine" but that doesn't make it one.

The vendors complain about the testing because they don't want to be found out. They did not create the machines to do elections right. In all honesty, they created the machines to win elections for Bush and Republicans. Period. Some admitted that publicly. Since they were not created with the right intention, they will never be right for honest elections.

Their computers could be made of gold. They could shine and enchant people with their shine. But since they count votes in secret **they can NEVER be ok for sustaining democracy.**

They could be tested in a Lab, they could be tested on a slab,
They could be tested at a Poll, they could be tested in a bowl.
They could be tested by a Prof, they could be tested for a poof,
They could be tested in a house, they could be tested with a Mouse.

It doesn't matter where they are tested; who tests them; how they test them; how many times they test them!

They are computers. **Computers** are susceptible to any number of kinds of invasion, by their nature. Therefore, **Computers are dangerous anywhere around elections.**

Elections are as sacred as the flag. They are a time for honoring our country.

They must be "above suspicion", "beyond a shadow of a doubt."

Computers are never beyond a shadow of a doubt.

08/02/2007

Computers are to elections as cheating is to honor.

Computers may NEVER be right for voting, even with open source code; there will ALWAYS be reason to DOUBT any computers and their output, BECAUSE Human Beings are involved. Some will want to mess things up; some will want to win; democracy and country be damned.

A substantial amount of expensive hand-auditing may help catch some computer fraud, but some could still be there, and **we will never never know for sure**. That is simply unacceptable.

The time and expense of doing extra audits added to the high initial costs of these computer machines, plus annual maintenance, storage, distribution, and training costs makes them an **in-valid substitute** for Paper Ballots, Hand Counted with some amount of verifying Recounting; that is cheaper, fast enough and more believable.

Common Sense tells us to demand an end to vendors' and election officials' deception, lies, intimidation, threats, fear-mongering and self-serving that are poisoning the Secretary of States' office Review climate .

The Diebold, Sequoia, ES&S and CivicHart **computers were never good for elections**. They should be taken back by the companies and the money returned to the US Treasury and or the sellers should go to jail for the massive consumer fraud they have perpetrated upon America as they have undermined democracy. Crimes have been committed.

As a nation we can not tolerate this sabotage of our elections that is weakening our country. **Elections are a Public Interest**, not for anyone's private gain.

Elections are simple. They only require honest people, attention, work, time, patience, education, **paper and pens**.

Mark the paper. Protect the paper. Count the marks. Verify the counts. Total the marks.

Report the totals when the counting is done.

Let that be as honest and true as is humanly possible.

That's all there is to it.

We are beholden to Secretary of State Bowen for doing the job we hired her to do. We applaud her and encourage her to do all in her power to set California's elections right. That will help every citizen; what's good for the country is good for even reluctant vendors and election officials.

Brina-Rae Schuchman

From: Kathay Feng
Sent: Wednesday, August 01, 2007 2:09 PM
To: Voting Systems
Subject: 8-1-07 TTBR Red Team Comment Letter Final

August 1, 2007

The Honorable Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, CA 95814
Sent via email to votingsystems@sos.ca.gov

RE: Top-To-Bottom Review of Voting Machines

Dear Secretary Bowen:

On behalf of California Common Cause, I am writing with regard to your office's "red team" reports reviewing the security and accessibility of several voting systems currently in use released on July 27, 2007.

California Common Cause is a non-profit, non-partisan citizens' lobby that works to strengthen governmental accountability and public civic participation. In 2002, we were the lead plaintiffs in litigation that forced California to switch off of punch card voting machines because of high voter error rates, particularly amongst minority voters. The settlement led the way to California's leadership in transitioning to new, more accessible, and more accurate voting machines. Our California members are committed to supporting voting technology that ensures voter accessibility as well as vote security.

The reports contained findings that question the security and accessibility of these voting systems. The red team testers stated that they focused their testing on the technology of the voting systems rather than on the policies, procedures, and laws of the Secretary of State or local election officials intended to compensate for any technological shortcomings. To the extent that vulnerabilities were found, we support the recommendations calling for compensating controls, including the development of security plans that address physical security, security training of staff, and contingency planning.

We oppose any action that would remove these machines from use in the near term elections. Our recommendation is based on the following reasons:

1. In Section 6.0 (Results and Interpretations) of the Overview of Red Team Reports, the University of California technology experts stated that they believe the information in the reports would allow the voting system vendors to take corrective action to mitigate or eliminate the security vulnerabilities that the technology team reported: "We request that the Secretary of State provide the public and confidential reports to the respective vendors... With their intimate knowledge of their systems, this should be enough to enable them to determine, and take, appropriate corrective action." Additionally, the red team testing was conducted under laboratory conditions without simulating the actual pre-election day and election day security procedures that normally occur during elections. Because of this, we believe that the red team testing results do not compel removal from use. We also

08/02/2007

strongly disfavor any removal of these machines from use in the near term based on accessibility non-compliance.

2. Removing these machines from use in the near term would result in decreased access for voters with limited English proficiency and voters with disabilities in the counties currently using such voting systems. Voting machines with an electronic interface offer increased access to the polls for such voters compared with purely paper-based voting systems. For example, ballots in multiple languages can be displayed much more easily on an electronic display screen than on a purely paper ballot, benefiting voters whose first language is not English.

3. Removing these machines from use in the near term could force counties to retrain poll workers on how to set up new voting systems, which takes away from the time that counties could spend to train poll workers to offer better customer service. We believe that this is likely to have a negative impact particularly on the ability of poll workers to serve language minority voters and voters with disabilities.

4. We believe the potential for confusion is particularly significant given the lack of time for counties to conduct voter education before the early February 2008 election.

Sincerely,

Kathay Feng
Executive Director
California Common Cause

From: Grace Cooper
Sent: Wednesday, August 01, 2007 11:49 AM
To: Voting Systems
Subject: electronic voting...yes or no...and whatever else..response for Debra Bowen, Secretary of State

It may be late for input, but I was returning from Mexico and could not attend the hearing on Monday. I have worked 7-8 elections in Sacramento County, and do not believe that anyone is playing games with the equipment of trying to fix the elections, BUT, I DO have major concerns about using ANY electronic voting equipment, and I DO believe that it is possible that there are interests out there who would happily "fix" an election if they could figure out how to do it. I believe that they did work on that in Florida, for instance, in 2000, and also in Ohio in 2004. Just those two places alone should make us wary of electronic voting equipment. In the final analysis, I believe, it was the Supreme Court in 2000 that disenfranchised the voters by stopping the counting and declaring that Bush had won ...and it would be just awfully unfair to go ahead and re-count those ballots; let's just say Bush won and be done with it. In Ohio, somewhat different; there was fiddling around with the equipment during the recounts, and there was plenty of disenfranchisement work that was done ahead of time and during the election itself.

I TRULY BELIEVE THAT THE ONLY WAY WE CAN FEEL SURE THAT WE HAVE OPEN AND HONEST ELECTIONS IS TO RETURN TO PAPER BALLOTS THAT ARE COUNTED, FIRST, AT THE PRECINCT LEVEL, AND THEN TURNED IN TO THE CENTRAL TABULATING FACILITIES.

I ALSO BELIEVE THAT WE SHOULD DO A COST COMPARISON....THE COST OF ALL MAIL-IN BALLOTING (AS IN OREGON) AS OPPOSED TO THE COST OF PRECINCT OPERATIONS, VOTING AT THE POLLING PLACE. I ALSO DO NOT CONSIDER THAT YOUR RECENT STUDY/TEST SHOULD HAVE INCLUDED INPUT FROM THE VARIOUS AND SUNDRY ROVs THROUGHOUT THE STATE. (I am concerned that some of them may have "conflicts of interest").

I will be happy to volunteer, barring family emergency, to assist with counting at precincts, if that is necessary....or to work with our local office of the Registrar of Voters on election night so that we will have a public and open counting of all ballots, including Absentee and Provisional– after signatures have been verified by the ROV staff. The staffs at the various ROV offices may be resistant to change, for whatever reason – a stubborn desire to stick with what they consider to be reliable procedures, or resistance to having to figure out split shifts so that old ladies like me don't have to work a 14 or 16-hour shift !! (A strong recommendation I would make.)

In the final analysis, I do not believe we can or should EVER trust the election results when elections are conducted on machines we KNOW are vulnerable to hacking – whether direct or remote.

Sincerely, Grace Cooper

From: Dylan Boot
Sent: Wednesday, August 01, 2007 11:56 AM
To: Voting Systems
Subject: Voting Access for People with Disabilities

Debra Bowen
CA Secretary of State

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,

Dylan Boot. MS

Peer Support Specialist
Access to Independence (a2i)
(Formerly The Access Center of San Diego, Inc.)
New Web Address: www.a2isd.org

NAME CHANGE:

Please note: Beginning 1-1-07, the Access Center will become: Access to Independence and our web address will be a2isd.org. Our individual e-mail addresses have also changed, but the transition is transparent. When you receive this e-mail, please note my new e-mail address and make the necessary changes to your records. Access to Independence thanks you!

08/02/2007

From: Carol Bronder
Sent: Wednesday, August 01, 2007 12:15 PM
To: Voting Systems
Subject: Red Team Review

Dear SOS Bowen,

I received an e-mail from Velvet Revolution asking me to thank you for the independent review of voting systems in CA. Obviously the results are incriminating and the security flaws present in these systems uncovered by your review as well as other independent tests must not be tolerated. Please follow-through in decertifying these machines in California. There is no room in a democracy for an election system that is based on technology that cannot be trusted to count every vote, accurately. I have been in constant contact with Minnesota's SOS Mark Ritchie on voting security issues in our state. SOS Ritchie believes that the auditing and security procedures put into place in the 2006 elections (in which he won) are adequate. I personally disagree with him, based on studies and opinions such as those advanced by fellow Minnesotan Bruce O'Dell--an experienced IT security expert and election reform activist. Please read Bruce's piece in Scoop from October 6, 2006.

<http://www.scoop.co.nz/stories/HL0610/S00419.htm>

His closing paragraph is particularly germane:

"There was a remarkable article published by the Computer Professionals for Social Responsibility in 2001, citing work by the Caltech-MIT Voting Project:

... our best efforts applying computer technology have decreased the accuracy of elections, to the point where the true outcomes of many races are unknowable. Many technologists and technology enthusiasts will read the above words and refuse to believe them. 'There must be some other explanation,' they will say. 'Nothing has been proven,' they will say. 'Future technology will be better,' they will say. But there is no other plausible explanation: new technology may have reduced the cost of elections, and certainly has increased counting speed, but the above results show no statistically significant progress in elections accuracy over people counting paper ballots, one at a time, by hand.

Let me recap: voting by computer may be inherently untrustworthy and in practice poorly crafted, overpriced, prone to breakdowns and wide open to subversion - but at least it's less accurate than counting by hand.

Here's an indictment of the IT profession, and a fine irony: **the degree of independent hand-auditing of paper ballot records sufficient to verify the corresponding computerized vote tallies is comparable to the effort required to more accurately count all the ballots by hand in the first place, dispensing with the machines.** But until that day arrives, the programs that the voting vendors actually distribute - as opposed to the software they may say they distribute - will continue to determine who takes power after the votes are tallied."

Thank you,

Carol Bronder

08/02/2007

From: Jenny Clark
Sent: Wednesday, August 01, 2007 3:31 PM
To: Voting Systems
Cc: Nancy Tobi
Subject: Recommendations for the General Election of 2008

Thank you! Secretary of State Debra Bowen for the review of electronic voting machines!

I understand you are soliciting public comments on the issue, through today.

Yes, all e-voting systems must be decertified at once! Good luck!

I have been aware of the fraudulent voting machines for many years and have been appalled at the lack of serious review and public awareness (thanks to the media blackout on the subject). So I am especially grateful for your "Red Team" review.

With the Emmy nominated "Hacking Democracy" in documentaries this year, maybe that will help shed some light on this serious problem. You may recall that even optical scan voting systems are hacked in this film. Any marking or counting device that relies on computer technology can be hacked.

There was a time we all believed a "paper trail" attached to e-voting machines would be a good answer. However, since new information and evidence of fraudulent counts, conflicting exit polls and a host of other evidence, I now believe that the best solution is to simply scrap all computerized technology in our voting systems.

What voters need and want and deserve is a "paper ballot". We do not need a receipt to take home nor do we need a small percent of our votes audited as the paper "trail" proponents argue.

The best solution for accurate vote counts is to return to the simple hand counted paper ballot, hand counted in full public view at the precinct level. The totals at the precinct will match the number of voters who signed in to vote. The paper should be of a durable stock to allow many hand counts of multiple-candidate/issues on the ballot. Even if you paid the counters \$20 an hour, you still would save many millions by avoiding complex computer upgrades year to year, and other expenses.

I am not an expert on computers or hand counting, but I highly suggest that you seek advise from many experts who are knowledgeable on how to do hand counts.

Posted below is a link and an article about how to conduct a hand counted paper ballot election. Do not be swayed by nay-sayers who think this solution is a return to the dark ages. Indeed, many countries around the world use this system just fine and are perplexed with the US fixation on voting machines. It is totally doable, even in a large state like California. It keeps all elections as local as possible at the precinct level.

I hope that California will once again be a leader for the nation on this issue of e-voting. Every technological fix suggested by computer experts is another doorway for hacking. The accountability and prosecution of the fraud that has already occurred should be firm and swift.

Good luck!
Thank you,
Jenny Clark

See this link for information on "An Election Preparedness Kit", written by hand counted paper ballot expert Nancy Tobi from New Hampshire, who is another good source for you, on the training required to perform hand counted ballots. It should not take too long to do the training. I have copied Nancy on this e-mail to make it easy for you to contact her.

<http://www.democracyfornewhampshire.com/node/view/2606>

This article explains in simple terms how easy and inexpensive it is to use the hand counted paper ballot voting system.

<http://www.smirkingchimp.com/node/8842>

On-Site Observations of the Hand-Counting of Paper Ballots and Recommendations for the General Election of 2008

by **Sheila Parks** | Jul 20 2007 - 9:44am |

Between May 2, 2006 and November 7, 2006, I observed the hand-counting of paper ballots in three elections in two New England states. The purpose of these observations was to gather first-hand data concerning the feasibility, effectiveness and accuracy of the use of HCPB. These elections were as follows:

- (1) Rockport, Massachusetts (MA), on May 2, 2006, Town Election
- (2) Hudson, MA, on May 8, 2006, Town Election
- (3) Acton, Maine (ME), on November 7, 2006, General Election

All three hand-countings of paper ballots were conducted smoothly and were finished in a timely manner. This paper describes the various protocols used and presents recommendations for the use of hand-counted paper ballots (HCPB) in the upcoming elections of 2008. Absentee ballots, provisional ballots and chain of custody of the ballots are not dealt with in this paper, although they are also crucial elements of an HCPB system.[1]

Much has been written about the fraud and error associated with the use of electronic voting machines - both Direct Recording Electronic (DRE'S/touchscreens) and Optical Scan (op scans/opti scans).[2] Because of this fraud and error, HCPB have been put forth as an alternative to electronic voting machines.[3] The use of an HCPB system will ensure that each vote is counted as intended and as cast by the voter. Although HCPB do not address the egregious suppression of the vote (mostly of people of color, elders and low income people), partnering a solution to the elimination of this suppression with the use of HCPB is the only way to have honest and transparent elections.

The jurisdictions that I observed were not selected randomly. They were places that I could drive to comfortably from my home in Boston, MA. Moreover, I was interested in observing an election in Acton, ME because the Town Clerk had told me that after the first hand-counting, the ballots would be hand-counted a second time.[4] I received permission to observe the elections from each Secretary of State, or their assistants, and from each Town Clerk. For full transparency, I introduced myself as an advocate of HCPB, who wanted to observe an HCPB election. I was very well received and felt comfortable in all places. All three Town Clerks were

very generous with their time and expertise.

In each of the three elections observed, number two pencils were used by the voters to hand mark their paper ballots. In each of the elections, the counters worked in teams of two. In addition, the counters were told that it was the intent of the voter that was to be counted, and when in doubt, the counters called over the Town Clerk or Warden[5] to ask questions about specific ballots and how to count them. Finally, in each of the elections, the counters were able to hand-count the paper ballots in a short time (see specifics below).

ACTON, ME, NOVEMBER 7, 2006, GENERAL ELECTION

I will first describe the HCPB election in Acton, ME on November 7, 2006 because this protocol used a procedure that would produce the most accurate count of the votes - namely, a second hand-count was done immediately after the first hand-count.

The ballot box was a plain, wooden box with a slot into which voters put their ballots. There were six teams, of two counters each, doing the hand-counting. The counters came in specifically to count; they had not worked at the polls earlier in the day. Each team consisted of a Republican and a Democrat. The teams first counted the ballots into batches of 50, and then these batches of 50 were counted again.

The teams then hand-counted the votes cast in each contest for each batch of 50 ballots in the following manner: One member of the team would read out loud the name marked off for each contest; the other member of the team marked the vote on a tally sheet that corresponded to the ballot. A voter's entire ballot was tallied for all of the contests before the counters went on to tally the next voter's ballot. The talliers counted each vote by making a hash mark (small, straight vertical line).[6] After four vertical lines were made, a fifth line was made diagonally through the first four marks. For each person running for office (and for each initiative), the tally sheet was marked off into five columns vertically and two rows horizontally, providing 10 rectangular spaces in each of which five hash marks could be written - a total of 50 hash marks - i.e., votes - per contest or initiative. A dark horizontal line separated the names in each contest. At the end of the counting of all of the races in a batch of 50 ballots, the counters totaled the hash marks for each race on the tally sheet and entered that number on the tally sheet in the "TOTAL VOTE" column. There was a special sheet for write-ins.

Immediately after the first hand-count of a batch of 50 ballots, a second hand-count, on a new tally sheet, was done of this same batch of 50 ballots by these same counters. Again, the entire ballot of each voter was tallied before the counters proceeded to the next voter's ballot. This time, the person who had read the names out loud marked each vote on the tally sheet, and the person who had tallied read out loud the ballot choices. After the votes on all 50 ballots in a batch were marked on the tally sheet, the totals for each contest were obtained and written on the tally sheet. If the totals for the candidates in any contest or for any initiative were not exactly the same on the first and second tally sheets (i.e. on the first and second countings), these contests or initiatives were counted a third time. I observed such a situation two times. The HCPB election in Acton, ME demonstrates that paper ballots can be hand-counted immediately a second time, at the precinct on election night, before the results are posted at the precinct, in order to ensure an honest and transparent count in a timely manner. The election in Acton, ME also indicates that paper ballots can be hand-counted in a very short time. With seven races and two initiatives, the six teams of two people each were able to hand-count twice 944 ballots in four hours.

ROCKPORT, MA, MAY 2, 2006, TOWN ELECTION HUDSON, MA , May 8, 2006, TOWN ELECTION

The elections in Rockport and Hudson will be discussed together because they were similar in various respects. Both counted the votes cast only once,[7] and both used the same kind of

tally sheets provided by the MA Secretary of State. In both jurisdictions the ballots were counted into batches of 50. The tally sheet was a large piece of paper that was marked off into a grid with horizontal and vertical lines forming small rectangular boxes (similar to the squares of graph paper). The vertical columns were marked with a heavy line at each multiple of five columns. There were 50 rectangular boxes across each horizontal line. At the top of the tally sheet, each vertical column was numbered from 1-50. On both the left hand and right hand sides of the tally sheet were the names of the people running in that particular race. One tally, as a hash mark, was put into one box, beside the name of the person voted for. A voter's entire ballot was tallied for all of the contests before the counters went on to tally the next voter's ballot. After the 50 ballots were tallied, the totals for each contest were entered into the "Totals" column at the end of the 50th box. Blanks and write-ins were also marked on this sheet. Four or five teams of two poll workers did the hand-count. One read from the ballot, and the other person placed the hash mark in the appropriate box on the tally sheet.

Rockport, MA used an old wooden ballot box.[8] A poll worker turned the brass handle on the box as each voter put her/his ballot into the box. Numbers on the front of the box automatically changed as ballots were placed in it, counting the cumulative number of ballots placed in the box. The machine marked each ballot with the precinct number down the center of the ballot as it went through the machine. The preceding characteristics of the ballot box provided a measure of security for the ballots, minimizing the danger of stuffing the ballot box, a criticism often leveled at the HCPB process. As noted earlier, this paper does not examine in detail issues of security such as chain of custody, but rather deals with protocols for HCPB. There were two crews of poll workers, morning and afternoon. One crew came in at 6:30AM and worked until 12:30PM. The second crew came in at 12:30PM and worked until 6:30PM. At 6:30PM, the second crew went home for dinner until 8PM, when they came back to hand-count the paper ballots. The morning shift came back at 6:30PM to work at the polls and then to hand-count the paper ballots. The polls closed at 8PM. The paper ballots were hand-counted by five teams of two workers each.

In Hudson, the ballot box was an old box made of gray wood. The ballot box rang when the voter put in her/his ballot, and the poll worker turned the crank of the box, moving the ballot from the slot of the box into the box. When the poll worker cranked the ballot into the ballot box, each ballot was inked with "Town of Hudson, precinct 6." [9] This ballot box also provided a degree of security for the ballots.

The Clerk could hire eight people per precinct, not including the Warden and Clerk, who were also present for the hand-counting. There were two shifts of poll workers, 7AM-5PM and 5PM-8PM, which was when the polls closed. The second shift did the counting. Poll workers had to be registered voters in the town of Hudson. Although it was preferred that the counters lived in the precinct where they worked, it was not necessary.

The elections in Rockport and Hudson again demonstrate that paper ballots can be hand-counted in a reasonable time. In Rockport, it took about one hour to hand-count 522 ballots; there were six races and no initiatives. In Hudson it took about one hour to hand-count 59 ballots; there were 14 races and no initiatives. As noted, both communities used ballot boxes that provided a degree of security for the ballots.

RECOMMENDATIONS TO BEGIN WITH THE 2008 GENERAL ELECTION (WHICH INCLUDES THE PRESIDENTIAL ELECTION)

Recommendations Based on My Observations

(1) Based on my observations in Acton, ME, this paper recommends the hand-counting of paper ballots followed immediately by a complete second hand-counting and a reconciliation of the two counts, if necessary, by additional counting.[10] A second hand-counting is crucial to

check the accuracy of the first hand-count. If a discrepancy is found between the two countings, counting should continue until the counts are reconciled. This paper also recommends the procedure used in Acton of counting the ballots into batches of 50, counting a batch of 50 and then immediately counting that batch of 50 again. Some critics of electronic voting machines have pointed out the need to obtain a second count, called an audit, after the first original tabulation of votes; however, there is no consensus as to how such an audit should or could be done. The second counting of ballots recommended in this paper goes beyond the concept of an audit to a comprehensive process encompassing a second counting of every vote and a reconciliation of the two counts.

(2) From my observations of these three hand countings, I prefer the tally sheets used in Acton, ME over the graph-like grid used in both Rockport, MA and Hudson, MA. During my observations, it appeared that the Acton tally sheet was easier for the counters to use. With the grid-like tally sheets, care had to be taken by the counters not to lose their place.

(3) Because HCPB require careful attention to and scrutiny of the ballots, it is recommended that people who have not worked at the polls all day come in to do the counting, as in Acton, ME.

(4) As noted, this paper does not deal in detail with the issue of security of the ballots. However, it is recommended that research be done concerning the cost of manufacturing ballot boxes with the characteristics described for Hudson, MA and Rockport, MA.

Additional Recommendations

The present author has been involved with voting rights for the last five years. Based on her previous work,[11] she also further expands the use of HCPB to include the following recommendations:

(1) In addition to the four recommendations presented above, it is recommended that an HCPB protocol also have the following characteristics: (a) Ballots would be counted at the precinct by registered voters in that precinct. (b) The counting would be done in full view of the public. (c) The counting would be videotaped. (d) The results would be posted at the precinct immediately after the count. (e) To be manageable, precincts would be no larger than 1000 registered voters. (Because the concept of HCPB operates at the precinct level, even large communities can adopt such a system.) (f) In each precinct there would be at least 10 teams of two counters each (a Democrat and a Republican).[12] These teams would count the ballots, one counter reading the name and the other counter making the mark on the tally sheet. For the second counting, the counters on each team would switch roles. (g) Whether or not there would be observers as part of the team of counters, and if so, how many, needs more research and is beyond the scope of this paper.

(2) This paper recommends that poll workers who participate in the process of HCPB be paid at a rate that will be respected by the community. This will be possible because a large amount of money will be saved with the elimination of electronic voting machines. The Help America Vote Act (HAVA) paid states hundreds of millions of dollars to buy electronic voting machines, both DRE'S and/or op scans.[13] One machine can cost anywhere from \$3,000 - \$5,000[14] and that amount does not include storing, maintenance, and upgrade. In contrast, for an HCPB election, the cost for the counting could be \$2400.00 per precinct for each election, with ten teams of two workers each, as described above, and paying each worker \$20/hour for six hours (\$120). HCPB by registered voters from the precinct would also keep the money in the community. As is true for op scan electronic voting machines, money would also have to be spent for the cost of printing the ballots.[15] If hundreds of millions of dollars had not been spent for the purchase, storage and upgrade of electronic voting machines, imagine the money our communities could have used for health care and education.

EPILOGUE

On January 4, 2006, I had the good fortune to watch on TV the voting in Congress for Speaker of the House. One at a time, each representative called out orally her/his choice for Speaker, and that vote was tallied by hand. This hand counting of oral votes was done by two Republicans and two Democrats, all of whom had been appointed by the Clerk of the House. The Electronic Board that usually counts the votes of the Representatives was not used for this count; the official vote was tallied by hand. I could not help but wonder how the Representatives would have felt had their votes not been recorded accurately, or not at all, as voters throughout the USA experienced in recent elections. For voters in each precinct in the USA, hand-counting of paper ballots would assure that each of our votes is counted as intended and as cast, as the oral votes of our Representatives, were hand-counted, as intended and as cast, in the House of Representatives.

ENDNOTES

[1] For a beginning discussion of chain of custody, see the present author's paper *Hand-Counted Paper Ballots Now*. A version of this article first appeared in the April 2006 issue of *Tikkun*, <http://www.tikkun.org/magazine/specials/article.2006-04-10.1693298872>, retrieved from the Web February 28, 2007. An updated version can be found at <http://electionfraudnews.com/News/HCPBNow.htm>, retrieved from the Web February 28, 2007. "Ballot boxes must be clearly marked and visible in plain view. Ballot boxes will be sealed and locked whenever they contain ballots and are not being actively used. Ballot boxes are secured from the beginning of voting until the end of counting by a chain of custody procedure. Ballot boxes never leave the polling place until after the vote is counted, audited and certified. Each time ballot boxes move from the physical control of or visual contact from one person to another, a duplicate record signed by all counters and observers must be made relinquishing and gaining control. There will be a documentation process wherein each ballot box will have a record of its handling from the beginning of the day to the end of counting. On the web site of computer science expert Professor Douglas W. Jones, there is a very clear and detailed protocol for "Ballot and Ballot Box Transportation" and "Ballot Storage." The reader is referred specifically to these two sections (the last two on this link): <http://www.cs.uiowa.edu/~jones/voting/paper.html>

[2] Listed here are some of the outstanding articles about the fraud and error resulting from electronic voting machines; some are from the mainstream media, others from scholarly sources, and yet others from technical groups: (1) The public hacking of electronic voting machines by Harri Hursti, working with Black Box Voting, <http://www.bbvforums.org/forums/messages/2197/6847.html>, retrieved from the Web February 21, 2007. (2) The U.S. Government Accountability Office (GAO) in its nonpartisan September 2005 report on elections states in its conclusions: "Numerous recent studies and reports have highlighted problems with the security and reliability of electronic voting systems § the concerns they raise have the potential to affect election outcomes § Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, But Key Activities Need to be Completed.", <http://www.gao.gov/new.items/d05956.pdf>, retrieved from the Web March 7, 2007. (3) Article by Robert F. Kennedy, Jr. in *Rolling Stone* (Issue 1002, June 15, 2006), http://www.rollingstone.com/politics/story/11717105/robert_f_kennedy_jr__will retrieved from the Web February 21, 2007. (4) Report of the Brennan Center Task Force of NYU, on June 27, 2006, http://www.brennancenter.org/press_detail.asp?key=100&subkey=36345, retrieved from the Web February 21, 2007 and http://brennancenter.org/dynamic/subpages/download_file_38150.pdf, retrieved from the Web February 22, 2007. (5) Papers by Ed Felton et al. from Princeton University in

Sept. 2006, <http://dubiousprofundity.com/hackthevote.pdf>, retrieved from the Web February 21, 2007. (6) Problems that occurred with electronic voting machines in many states in the General Election on November 7, 2006, especially the 18,000 undervotes in Sarasota County, FL, http://www.nytimes.com/cq/2006/12/20/cq_2056.html, retrieved from the Web February 20, 2007. (7) NIST discussion draft, December 1, 2006, <http://vote.nist.gov/DraftWhitePaperOnSIIinVVS2007-20061120.pdf>, retrieved from the Web February 22, 2007. (8) The annotated bibliography by Rady Ananda, <http://tinyurl.com/2gw1ve>, retrieved from the Web May 11, 2007.

[3] On August 4, 2006, Nancy Tobi posted this article about HCPB in NH, http://www.opednews.com/articles/genera_nancy_to_060804_the_granite_stat retrieved from the Web March 12, 2007. An editorial first carried in the Ketchikan Daily News, December 1, 2006, written by Editor Terry Miller, called for HCPB for the president and vice president, <http://www.ketchikandailynews.com/>, retrieved from the Web January 12, 2007. (Thanks to John Gideon of Daily Voting News for pointing out the Ketchikan editorial.) On December 7, 2006, the editorial was then picked up by the Juneau Empire, http://juneauempire.com/smart_search/, retrieved from the Web January 12, 2007. Rady Ananda wrote an HCPB Implementation Strategy for 2007 on January 3, 2007, http://www.opednews.com/articles/opedne_rady_ana_070102_evoting_exit_str retrieved from the Web March 13, 2005. In February 2007, in Missouri (MO), Show Me The Vote, led by Phil Lindsey, introduced an initiative to go on the ballot that, if passed, would mean that MO would not use electronic voting machines in their elections, but would use HCPB. This initiative must first get enough votes from the public to appear on the ballot, <http://www.scoop.co.nz/stories/HLO702/S00271.htm>, by Michael Collins, retrieved from the Web March 12, 2007. (To contact Show Me The Vote, email Phil at galloglas@sbcglobal.net.) Another HCPB initiative, led by Kathleen Wynne, is in the form of a petition from the American People to Congress, urging Congress to reintroduce the Paper Ballot Bill of 2006, <http://hcpbnow.org/petition.html>, retrieved from the Web July 13, 2007. In June 2007, at The DFA (Democracy for America) Democracy Fest in New Hampshire, in a telephone call to the attendees, Representative Dennis Kucinich stated that he will introduce The Paper Ballot Bill of 2007, mandating HCPB for all federal offices. Kucinich has changed the bill from his 2006 version, H.R. 6200, which had mandated HCPB for the offices of president and vice-president only, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6200ih.txt.pdf, retrieved from the Web, March 30, 2007.

[4] I observed one of the three HCPB methods authorized by the Maine Secretary of State, called "The Reading Method": "The team counts each lot together; 1 member reads and the other member tallies. The team members then switch roles, so that the tally is done a second time. If they agree, that count is completed. If there is a discrepancy, the team must recount the race or races where the count was off. Š." From Maine Revised Statutes Annotated (M RSA), CONDUCT OF ELECTIONS, Chapter 9, page 3, (Title 21-A §695).

[5] "Warden" is the name used in Massachusetts for the poll worker in charge of the election in that precinct. Different names are used in different states. The person is not an elected official

[6] In April 2004, Teresa Hommel described some hand-counting methods used in Canada and New York City, <http://wheresthepaper.org/CountPaperBallots.htm>, retrieved from the Web January 13, 2007.

[7] Another method of hand-counting paper ballots is the sort and stack protocol, <http://www.sos.nh.gov/FINAL%20EPM%208-30-2006.pdf> (pp 144-146), retrieved from the Web May 11, 2007. In this method, used by the state of New Hampshire, the ballots

are first sorted into stacks for each candidate, and then the stacks are counted. In email correspondence, December 2, 2006 and December 4, 2006, with Nancy Tobi from Democracy for New Hampshire, Tobi states that NH uses the sort and stack method for both election night counts and for recounts. She says that it is used primarily for "Š single member races - where there is a yes/no choiceŠ." and for straight ticket votes. Sort and stack is not usable in all situations. With this protocol, as with those used in Rockport and Hudson, votes are counted only once; the manual recommends a second count if there is a "close race." A "close race" is not defined. A mandatory second count for all ballots could be added to this protocol.

[8] The ballot box said "Town of Rockport, Precinct 2" and was dated 1922.

[9] The ballot box was made by S. Ralph Cross and Sons, Inc., 120 Mayfield Street, Worcester 2, MA, now out of business. The box was dated 1971.

[10] Joanne Karasak has recommended a first count followed by "an immediate second 'blind' count (blind count meaning that the second team of counters do not know the total on the first count)." Email posted June 26, 2007. Based on my observations in Maine, I think it would be too confusing to change counters.

[11] See Sheila Parks, *What Went Wrong in Ohio & Black Box Voting*, <http://www.tikkun.org/magazine/reviews/article.2006-01-06.7975946864>, retrieved from the Web March 18, 2007; Sheila Parks, *Hand-Counted Paper Ballots Now* (see endnote 1); Roy Lipscomb and Sheila Parks, *Hand-Counted Paper Ballots: Frequently Asked Questions*, <http://www.scoop.co.nz/stories/HLO705/S00261.htm>, retrieved from the Web May 20, 2007.

[12] If there additional parties on the ballot, representatives from these parties should also participate in the counting.

[13] Thanks to my good friend Lucius Chiaraviglio, HCPB activist, for his help with this endnote, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ252.107, retrieved from the Web March 13, 2007.

[14] Thanks to Paul Letho for sending me this information. See Appendix A, <http://www.votersunite.org/info/SequoiaContract.pdf>, retrieved from the Web March 18, 2007, for the contract between Snohomish County, Washington and Sequoia Voting Systems, Inc. for a detailed example of what electronic voting machines cost. This contract was for more than \$5 million dollars. Appendix A is contained in his lawsuit against Sequoia Voting Systems, Inc., www.votersunite.org/info/lehtolawsuit.asp, retrieved from the Web March 18, 2007.

[15] Email correspondence, March 6, 2007, with Chief Legal Counsel, Election Division, Office of the Secretary of State, MA. In MA in 2006 there were 71 precincts using HCPB. For the MA State Primary election in 2006, the cost was \$444 per precinct (which included two parties) for ballot printing, which included absentee ballots, specimen ballots and instruction cards. For the General Election in 2006, the cost was \$391 per precinct.

Copyright © 2007 by Sheila Parks, Ed.D.

ABOUT AUTHOR

Sheila Parks, Ed.D., is an Organizing Consultant who lives in Boston, MA. She is a long time feminist and peace & justice activist/organizer on many issues and has been involved in the current wave of voting rights for five years.

Sheila Parks's blog |

From: Valerie Arita
Sent: Wednesday, August 01, 2007 9:16 AM
To: Voting Systems
Cc: Connie Soucy
Subject: Re: Voting System

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 30, 2007

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,
Valerie Arita

Program Manager
Access to Independence (a2i)
(Formerly The Access Center of San Diego)

From: Parcels, Barbara
Sent: Wednesday, August 01, 2007 9:46 AM
To: Voting Systems
Subject: Comment on Voting Machines

Dear Secretary of State Bowen:

Thank you for reviewing the voting machines used in the State of California. I have worked as a poll worker with both types of Diebold voting machines used in San Diego County, both the touch-screen models, and the "optiscan" system. (I summarize them below the line). When I am not working as a poll worker, I am a programmer for a Fortune 50 corporation.

It is my opinion that the best, easiest, most reliable, and most affordable voting system for all parties concerned would be a version of the Diebold optical-scanning system which has been used in San Diego, which uses paper/cardboard ballots, incorporating instead of Diebold's software, open-source software running both the scanner and the central tabulator.

It seems to me that the greatest weakness of the new voting systems is the lack of transparency in the vote-tallying methods. Vote-tallying has been remanded to electronic code which the vendors state is "covered by trade secrets" and thus they prohibit it from being examined in detail for flaws in accuracy, honesty, reliability etc.

"Open-source" software, on the other hand, has all its inner workings fully open to public scrutiny. As such, governmental agencies, university researchers, security experts, and interested citizen activists can all examine the code, and an open and clear discussion of its strengths and weaknesses can be held. Many more "eyes" are examining it, increasing the odds of discovering defects so that they can be fixed. Such open-source code could be compiled into "certified" versions by the government for each election, and any machine found running an other-than-certified version for that election would be out of compliance. The source code for each "certified version" would be published publicly, such as on the SOS website, for full and open examination.

Several organizations are working on open-source code for American voting machines. Australia already has a working open-source software that they have used in several elections. See <http://www.openvotingconsortium.org/>; Australia's open-source code-- <http://www.wired.com/techbiz/media/news/2003/11/61045>; Open Vote Foundation (providing a version of Australia's code to California)-- <http://www.worldchanging.com/archives/000330.html> and <http://www.wired.com/politics/security/news/2004/01/61968>.

My experiences with the voting machines as a poll worker: In the 2004 primary we used the touchscreen Diebold voting machines. At that time they did not have the "receipt printer" (voter-verified printout) mounted. This system consisted of several touchscreen devices that the voters voted on, and one small module that sat on our table, which we used to program the voting cards for the voters. The voting cards were programmed according to the voter's party registration, the voter inserted them into the touchscreen machine, and the machine then presented them with the appropriate ballot according to their party. The famous problems with the San Diego primary, in my polling place at least, were due to junior-high-school-level mistakes by whoever set up the tabletop card-writing module. It failed to bring up its card-writing software upon power-up,

08/02/2007

presenting us instead with a blank Windows desktop. Whoever set it up failed to even put a shortcut to the software on its (Windows CE) desktop, nor did they put a shortcut to it in the 'Startup' folder. See my full description of this incident at http://www.crocuta.net/Dean/San_Diego_Voting_Machines_Foulup.htm.

In the 2005 special election (the next time I worked as a poll worker), we used the Diebold "opti-scan" system. In this system all voting was done on paper ballots (the same as used by vote-by-mail voters), which were scanned through a single optical scanner which then dropped them into the ballot box. The scanner was the only piece of electronic equipment in the polling place in this election, and worked fine for us. Even if it hadn't, we would still have been able to let people vote; they would have put their completed paper ballots in another sealed ballot box, to be counted later, instead of through the scanner.

In the 2006 primary we used the Diebold "opti-scan" system again, and also had one Diebold touch-screen system, with "receipt printer" this time, for use by handicapped people if desired.

It is my understanding that in both these systems, the "opti-scan" and the touchscreen, there is another unit down at the Registrar of Voters, which is used to gather the voting tallies from the electronic memory modules of the optical scanner or the touchscreen. This is the "Central Tabulator".

Sincerely Yours,

Barbara Parcels

From: Claire Stratton
Sent: Wednesday, August 01, 2007 9:16 AM
To: Voting Systems
Cc: Connie Soucy; Mark Carlson; Valerie Arita
Subject: Voting Machines
Importance: High

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 30, 2007

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,

Claire Stratton

Claire Stratton

08/02/2007

From: Elizabeth Turner
Sent: Wednesday, August 01, 2007 9:03 AM
To: Voting Systems
Subject: Opinion on voting machines

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 30, 2007

Dear Ms. Bowen:

I am asking you to ensure that the **Disabled Community in California has the opportunity to vote independently and privately**. People with disabilities want & need an accessible and secure voting system. Because of recent studies suggesting that these voting machines are not secure, it is being suggested that they be removed before the next election. Unfortunately, Federal legislators realized last week that there was insufficient time to decertify and develop an entirely new automated voting system in time for the 2008 elections.

Currently, certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

I support the State in including accessibility testing as part of the State certification process. My hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. I also recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities, and security.

Concerned citizen & advocate for people with disabilities,

Elizabeth Turner
Grant/Executive Assistant
Access to Independence (a2i)
(formerly The Access Center of San Diego)

NAME CHANGE: Please note: Beginning 1-1-07, the Access Center will become: Access to Independence and our web address will be a2isd.org. Our individual e-

08/02/2007

mail addresses have also changed, but the transition is transparent. When you receive this e-mail, please note my new e-mail address and make the necessary changes to your records. Access to Independence thanks you!

PRIVACY NOTICE - This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain information protected by confidentiality laws and regulations. If you are not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you may not review, use, copy, disclose or distribute this message, attachments, or any of the information contained in this message to anyone. If you have received this e-mail in error, do NOT read the content transmitted, please notify us immediately by e-mail and delete this e-mail message, attachments, and all copies.

From: Ann West
Sent: Wednesday, August 01, 2007 7:34 AM
To: Voting Systems
Subject: 7/30 hearing

Dear Secretary of State Bowen,

I attended the July 30 hearing in Sacramento, and I am writing now to call your attention to two things.

1. At the hearing the final speaker stated that only 20% of the eligible disabled voters were voting. What this suggests, I believe, is that the dre's (which the disabled voters know are now being used in the counties) may not be perceived as the solution to their problem.
2. After the 7/30 hearing, I watched a 5 o'clock News report on Sacramento KCRA Channel 3 during which Kim Alexander was being interviewed about the hearing. The audience of viewers was then asked to contact the station to say whether or not they thought that electronic voting machines should be used in elections. At the conclusion of the show the results of the survey were announced: **A TOTAL OF 79% OF THE VIEWERS WHO HAD CONTACTED THE STATION THOUGHT THAT THE ELECTRONIC VOTING MACHINES SHOULD NOT BE USED IN ELECTIONS, AND ONLY 21% FELT THAT THEY SHOULD CONTINUE TO BE USED.**

If one were to extrapolate from such findings, the conclusion would be that hearings such as the one in Sacramento on 7/30 can only serve to create a more aware public that is able to draw its own conclusions about the value of the expensive and risky electronic voting systems being adopted in the counties.

Thank you for your efforts on behalf of our democracy.

Sincerely,
Ann West

From: Pat Leahan
Sent: Wednesday, August 01, 2007 8:08 AM
To: Voting Systems
Subject: Please hold the voting machine vendors accountable!

Dear Secretary of State Bowen,

Thank you so very much for conducting the voting machine review. What an important action you took for the voting public. We are deeply grateful.

I first became aware of some voting machine problems when I began studying the issue here in New Mexico. I recommend that you view the documentary, "Stealing America: Vote by Vote," to see what happened in the 2004 presidential election in Ohio and New Mexico (www.stealingamerica.org).

Now you have another chapter to write in this story. **Please hold the voting machine vendors accountable.** They have KNOWINGLY allowed substandard products to be used by the voting public. They must be held accountable for seriously tainting our elections.

Please stay strong and stand up to the corporations. We are with you. We will stand with you and do whatever is needed. The entire nation needs you now more than ever.

The vendors should be "fired." Their machines should be completely decertified. They should not be rewarded for their criminality -- They should be punished. Please hang in there and let us know what we can do to help.

I would like to see you un-privatize our elections and go to hand-counted paper ballots. It absolutely can be done, and now is the ideal time.

Earnestly and with Deep Gratitude,

Patricia A. Leahan, Director
Las Vegas Peace & Justice Center

08/01/2007

From: Brad Green
Sent: Wednesday, August 01, 2007 8:13 AM
To: Voting Systems
Subject: Computer Based Voting System Input

Please find attached a graphic I prepared. It contains a schematic of a system that provides for a programmable computer based graphical "front end". But does not have the drawbacks of the current systems. I hope you'll a take minute to view and transmit to the appropriate person's.

From: Harvey Vlahos
Sent: Wednesday, August 01, 2007 8:23 AM
To: Voting Systems
Subject: Voting machine review

Dear Ms. Bowen

While I'm writing from NY, the safeguarding of voting is the very foundation of our nation and is of concern to every American, regardless of state. Please, please make sure there is an infallible paper trail to verify results. If we can't be 100% certain, we really have no democracy. I am particularly infuriated at those who say it would be too expensive. What is more important than securing the right to vote? What is more important and deserves more money? Without accurate elections we don't have a democracy.

The very premise that we are trusting our democracy to corporations is fundamentally flawed. Privatization of voting systems is one of the biggest frauds perpetrated on the American people under the name of free market in all of US history. I am of the belief that the government should own and operate the voting systems. Independent companies could do the work under contract, but ALL, and I do mean ALL machines, software, systems etc., are owned by the government... period. That way the systems and elected officials are subject to the will of the voters. Think about other government purchases. If the state of California buys autos, are they required to have them serviced by the manufacturer's dealer only, because the on-board computers are "proprietary." The same fundamental concept should apply to voting machines. The taxpayer buys them, they own them. If the manufacturers don't like it, go somewhere else.

Thank you.

Harvey Vlahos

From: Monica Barraza
Sent: Wednesday, August 01, 2007 8:33 AM
To: Voting Systems
Subject: Voting Systems

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 30, 2007

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new, more accessible, machines are available. We cannot deprive the disabled community from practicing their right to vote.

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,

Monica Barraza

Operations Supervisor
Access to Independence (a2i)
(formerly The Access Center of San Diego)
New Web Address: www.a2isd.org

08/01/2007

From: William B. Cushman PhD.
Sent: Wednesday, August 01, 2007 8:59 AM
To: Voting Systems
Subject: Red team review of voting machines

Dear Ms. Bowen,

Thank you from the bottom of my heart for finally getting some reality into our electoral process. I personally believe that our last several elections were completely fraudulent, and the mere fact that I and so many others believe this is a very bad thing for our country. Moreover, this belief is completely unnecessary.

I would like to suggest that this overall problem is exceedingly simple to solve: Use whatever voting machine is convenient to print out human readable ballots which are then reviewed by the voter and taken by the voter him or herself to a ballot box and dropped in with many witnesses observing. Then count these ballots by hand, using only humans, and with lots of witnesses. This sort of system completely eliminates the myriad paths for fraud that the electronic "labor savors" provide, and restores visible integrity to our elections --- a feature that has been notably lacking of recent.

Hand counting sounds daunting, but our neighbors to the north seem to be able to do exactly this in about four hours. Are their precinct sizes so much smaller than ours that this is possible? If so, then make ours smaller!

Finally, post the results of every precinct count on the door to the precinct, in the newspaper, and online so that anyone with the interest can add these results up themselves, and the workers at individual precincts can verify that the numbers used in the tallies are, in fact, the numbers they report.

The fact that such a simple system is clearly possible and at the same time assiduously avoided speaks volumes about our elections, and those volumes contain nothing compatible with the notion of "Democracy," and everything compatible with the notion of Fascism or some other dictatorial system.

We have become the horror of the world of recent, and our subverted electoral system is clearly a foundational cause of this. Thank you again for your good work fighting for what our country once was, and could be again.

Respectfully,

William B. Cushman, Ph.D.

From: Betty Manock [mailto:bettymanock@comcast.net]
Sent: Wednesday, August 01, 2007 8:39 AM
To: Voting Systems
Subject: What to do!

You certainly have our sympathy and support in making your decision about what to do about the insecure voting machines. Cost is going to play a major factor in your decision but trust of the people has to be uppermost in your mind also. Did the folks that made the declaration that they were not secure from hacking give you any suggestions? If not, perhaps they could help you out. There must be a program available that could secure these machines without having to replace them. I would also contact the companies, which I'm sure you have or will, and strongly suggest to them that they hold some responsibility in this matter. We certainly have public officials that would "fix" an election if they had the opportunity. I'm afraid that this problem is nationwide and has been abused in the past and will be again if it is not addressed.

"Kudo's" to you for caring about the public that you serve.

Good luck and may the Lord bless you in making your decision.

Betty Ann
In God We Trust!
God Bless America!

[i'm making a difference. Make every IM count for the cause of your choice. Join Now.](#)

From: Gail Davis-Fradet [gdavis-fradet@a2isd.org]
Sent: Wednesday, August 01, 2007 8:47 AM
To: Voting Systems
Cc: Mark Carlson; Connie Soucy
Subject: Accessible Voting Systems

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 31, 2007

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,

Gail Davis-Fradet

Independent Living Manager
Access to Independence (a2i)
(Formerly The Access Center of San Diego, Inc.)
New Web Address: www.a2isd.org

08/01/2007

From: Clark Labitan
Sent: Wednesday, August 01, 2007 8:49 AM
To: Voting Systems
Subject: Voting and Disabilities

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 30, 2007

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,

Clark Labitan

Access to Independence (a2i)
(formerly The Access Center of San Diego)
New Web Address: www.a2isd.org

NAME CHANGE: Please note: Beginning 1-1-07, the Access Center will become:

08/01/2007

From: Caroline
Sent: Wednesday, August 01, 2007 8:36 AM
To: Voting Systems
Subject: voting machines

Dear Ms. Bowen --

THANK YOU, on behalf of all Americans....indeed, on behalf of democracy itself....for conducting the Red Review and making public what many of us knew....that the vast majority of electronic voting machines out there are NOT secure, and cannot be made secure without measures that the manufacturers do not want to agree to....

NOW...PLEASE, please, PLEASE....be strong! Do not back down! Ban all those machines! You KNOW that when all the threatening has blown past you, and all the dust has settled, all those manufacturers will either get out of the voting machine business or do what is necessary to make them secure, INCLUDING publicly held escrow of the source code. They're just going to try to bully you, scare you, and generally intimidate you into NOT defending democracy.

So go ahead and BE a Hero...we need a few of those....this could be a pivotal moment in the history of our country: if you don't ban those machines, most other states will not do so, either, and GUESS what could happen to the 2008 election? All candidates with no moral standards will be able to be in their with their techies, hacking elections one way or another.....and gradually that will become apparent as people investigate....and once there is no confidence in our elections, we are NO LONGER a viable democracy. Cynicism and apathy become even worse; we become a government of people with money, not of laws.

PLEASE do the right thing for democracy. I personally pledge to contribute to your re-election campaign if doing the right thing threatens to cost you your office. THIS IS REALLY IMPORTANT.

Thank you so much for being a REAL citizen.

Caroline Rider, Esq.

Caroline Rider

From: EPLinda
Sent: Thursday, August 02, 2007 2:36 PM
To: Voting Systems
Subject: No vote-by-mail!

August 2, 2007

To Whom it May Concern:

In light of the findings of the Top-to-Bottom review of voting systems, I am very concerned that Secretary Bowen is going to advocate vote-by-mail as the solution, temporary or not. For the reasons outlined below and in the attached white paper, vote-by-mail poses very serious security risks due (at least in part) to centralized government control and lack of secrecy of the ballot. A vote-by-mail "solution" could be MORE RISKY than using insecure voting equipment at the polls. PLEASE, PLEASE do not advocate a move toward vote-by-mail in California elections! Instead, please advocate for the most secure solution: voting at the polls with a mandatory 10% hand-count of the ballots, in public view, before they leave the poll site. This audit mechanism, called the Universal Precinct Sample, is outlined in more detailed on the website of the Election Defense Alliance, <http://www.electiondefensealliance.org/?q=hr550auditflaws>. Those who could not vote at the poll site on election day can vote early in person at the county early voting site.

Please let me know what you intend to do. Thank you very much for your consideration.

Sincerely,
Linda Bagneschi Dorrance

Rumor has it the Bowen's big Plan B be to get out of the horrendous lack of equipment will be to declare vote by mail. even if only temporary.

Many Oregon and Washington activists have been working overtime in recent months to inform people why this can NOT be the solution. Oregonians got this foisted upon them as a "temporary fix" and it became permanent. And why not? It's clean, convenient and efficient. Precincts and citizen control are admittedly a messy business.

But convenience and efficiency come with a huge price: a bona fide democracy.

For some reason people can understand the vulnerabilities of internet voting, but they fail to grasp that the issues are IDENTICAL for vote by mail. It is a trust based, government controlled system that (as Bush's signing statement against U.S. Post privacy proves) that postal privacy, including ballots, may be sacrificed without notice despite assurances to the contrary.

California Election Protection Network has just approved bylaws that feature three basic core principles:

1. Minimum of 99% Accuracy. With elections increasingly won by slim margins, we cannot accept less than 99% accuracy. Please keep in mind, that even if we were to afford armored trucks with 24 hour surveillance to oversee the transportation of our vote by mail ballots,

08/02/2007

we could NOT affirm that same assurance that the ballots cast are indeed the ballots tabulated with statistical confidence as when we count 30 to 50 ballots at the precinct BEFORE they embark upon their anonymous journey to the centralized government site.

2. Citizen-Controlled Purview (e.g., not spot checking during office hours and not based on "two people" complying with a book full of regulations (particularly since we can't get people like Conny McCormack to comply with the most basic of election observation laws--even when witnessed by the public).

3. Hostile Government Test. If we wouldn't recommend it for a third-world nation pretending to be a democracy, then we shouldn't recommend it for ourselves. Because we need a governance that will sustain us through our worst days not our best days.

YES, it's true that precincts have been commandeered. But when you have 1 person, such as Conny McCormack with oversight control of nearly 40% of the California vote "entrusted" to follow laws and regulations versus the oversight of the many eyes of the 5,000 precincts, it is obvious that these two methods do not have equal vulnerabilities. Just like the "retail vs. wholesale" metaphor for DREs vs. paper ballots, the same is true for centralized vs. decentralized vote tabulation.

Finally, just to re-cap, once the paper evidence of the ballots leave the precinct without examination, there is no way--except for a "faith in our institutions" that the ballots are indeed counted as cast. This is precisely the same reason why we've fought long and hard against DREs. It's not that paper ballots can't be subverted, it's that DREs make it so much easier. Similarly, it's not that decentralized vote counting (precincts) can't be subverted, it's that centralized vote counting (vote by mail, internet voting) make it so much easier.

So goes California, so goes the nation.

Get a sneak peek of the all-new AOL.com.

Problems with Mail Ballot Elections (AB 1654) & Suggested Alternative

May 17, 2007

SUMMARY: Vote-by-mail has serious security risks that cannot be overcome through legislation. We cannot verify that we live in a democracy if we vote by mail since it is inherently insecure. The argument that vote-by-mail increases turnout is false according to academic studies, and even if it is true, election security cannot be sacrificed for convenience and cost. A far safer alternative, that would confer 99% statistical accuracy that votes tabulated precisely match the votes that were cast, is to vote at the precinct with at least a 10% hand-audit before the ballots leave the poll site. Voters who are unable to vote at the polls on election day can vote early in person at the county site(s). Mail-in voting should be a last resort reserved only for people who verify under penalty of perjury that they are physically unable to vote at their local precinct on election day nor at the county early voting location(s).

I. PROBLEMS WITH VOTE-BY-MAIL / ABSENTEE VOTING

1. Forces us to trust county election officials without sufficient public oversight.

- a. Impractical for members of the public to observe all aspects of vote-by-mail/absentee process.
 - i. Starts 45? days before election.
 - ii. Continues 28? days after election (post-election canvass).
 - iii. Multiple locations to oversee: county election offices and storage warehouses/facilities, subcontractors (printers, mail houses), post office and its subcontractors. Example: Fairfax (in Marin County) Nov. 2005 Town Council race. Mail house mailed absentee ballots out late, reducing absentee turnout and possibly impacting election result.
 - iv. Public can't physically ensure that all ballots coming in are legitimate, not forged by election officials who "stuffed the ballot box" or otherwise tampered with the ballots.
- b. Marin County Registrar of Voters, Elaine Ginnold, acknowledged the only ones who could rig an election are the local election officials, although she says they wouldn't do that.
- c. While we hope we can trust most local election officials most of the time, it would be naïve to think we can trust all of them all of the time. A single rigged county can throw an election. Problem of consolidated power without adequate public oversight.
- d. A total of 1,213 public officials had been federally charged with corruption in 2004, 1,020 of them had been convicted of corruption, and 419 cases remained pending. Source: The Department of Justice in its *Report to Congress on the Activities and Operations of the Public Integrity for 2004*.
- e. Local election officials can see and/or print absentee vote totals to-date before Election Day. Very risky to give them this power.
- f. Example: The Public Monitor appointed by Cuyahoga County's (Cleveland) Board of Elections has issued a report that identifies significant security breaches and "points of possible legal non-compliance" by the Board and its staff in their

conduct of the November 2006 elections. The report identifies several areas of non-compliant procedures associated with the tabulation of results and technical security which could have compromised the security of the election totals. Analysis of the election tabulation system log indicated that reports may have been printed summarizing the absentee ballot totals prior to Election Day. Printing vote totals before the end of Election Day would violate a State directive issued in response to a court order specifying that “at no time, any person has any access to the count or any portion of the count before the polling places close”. The report notes “This concern is especially acute where the proportion of the votes cast by absentee ballot is extremely high, such as was the case in the November, 2006 election in which nearly 25% of votes were cast via absentee ballot.” Source: *Public Monitor Reports Serious, Possibly Illegal, Security Breaches During Ohio Mid-term Elections*, by VoteTrustUSA - February 23, 2007.

2. Violates secrecy of the ballot. Susceptible to coerced voting, voter fraud, and selling votes. Examples:

- a. In 1998, former congressman Austin Murphy of Pennsylvania, a Democrat, was convicted of absentee-ballot fraud in a nursing home, where residents’ failing mental capacities make them an easy mark. “In this area there’s a pattern of nursing home administrators frequently forging ballots under residents’ names,” said Sean Cavanagh, a former Democratic county supervisor from the area. Source: *Absent Without Leave*, Wall Street Journal, 10-30-06, <http://www.opinionjournal.com/diary/?id=110009167&ojrss=wsj>.
- b. In East Chicago’s Ind.’s 2003 mayoral race, challenger George Pabey defeated Robert Patrick, the eight-term incumbent, among Election Day voters but lost by 278 votes after some 2,000 absentee votes were tabulated. Investigators for Mr. Pabey turned up repeated instances of coercion and vote-buying. Source: *Absent Without Leave*, Wall Street Journal, 10-30-06.
- c. Jeffrey Garfield, executive director of Connecticut’s Election Enforcement Commission, notes that absentee ballot fraud has been a persistent problem in his state for years and in Hartford alone has resulted in the arrest of at least eight city politicians. Source: *Absent Without Leave*, Wall Street Journal, 10-30-06.
- d. Employers could pressure vulnerable employees (immigrants, low-income, non-English speakers, and others) to vote a certain way or lose their job.
- e. Local labor union leaders could exert undue pressure to vote a certain way.

3. The 2001 National Commission on Federal Election Reform, a bipartisan group co-chaired by Gerald Ford and Jimmy Carter, concluded that absentee ballots do not satisfy five essential criteria for sound and honest elections, including:

- a. Assure the privacy of the secret ballot and protection against coerced voting.
- b. Verify that only duly registered voters cast ballots.
- c. Safeguard ballots against loss or alteration.
 - i. Example: Prior to the November 7, 2006 election, a political consultant found tens of thousands of campaign fliers in a dumpster behind a Fremont post office. The post office admitted that nothing was wrong with some of the fliers and that they should have been delivered. Source:

4. Many other problems exist.

- a. For example, vote-by-mail does not pass the “hostile government” test. That is, since the voter’s signature or other identification accompanies his ballot (on the envelope or elsewhere), a hostile government can link the voter with how he voted and subject voters to persecution.
- b. Even if you tried to legislate remedies to the many problems associated with vote-by-mail, enforcement is uneven and not always available. Better to adopt a voting system that: 1) is inherently as secure as possible by design, and 2) results in the least possible impact if fraud occurs.

II. ISSUES DRIVING VOTE-BY-MAIL

1. Turnout may not actually increase with mail-in voting.

- a. “Academic studies all show that easy absentee voting decreases or has no effect on turnout,” said Curtis Gans, the director of the Committee for the Study of the American Electorate, with the 2004 election a slight exception. This is because “you are diffusing the mobilizing focus away from a single day and having to mobilize voters over a period of time.” Mr. Gans notes that the people who really are helped by absentee voting are those who cast ballots anyway. Source: *Absent Without Leave*, Wall Street Journal, 10-30-06.
- b. The Task Force on the Federal Election System (part of the 2001 Ford-Carter Commission report) found that unrestricted absentee voting by and large has not boosted voter turnout, or if it has only by a small amount and it’s unclear if the gains will endure.

2. Even if turnout is greater, it cannot be justified if security is reduced.

3. Cost-savings evidence is mixed.

- a. The Task Force on the Federal Election System (part of the 2001 Ford-Carter Commission report) found mixed results on cost-savings. A 1994 FEC study of early voting in Texas found that early voting actually increased election costs in the largest counties, which offered extended hours and satellite locations, but maintained or decreased costs in counties that did not have to make such accommodations. A 1987 FEC report notes that per-vote processing costs for absentee ballots are several times the expense for ballots cast at the polls.

4. Even if costs are lower, it cannot be justified if security is reduced.

5. Costs can be reduced by:

- a. Stop using taxpayer money to encourage vote-by-mail/absentee voting.
- b. Return to precinct-based voting, with vote-by-mail only an option for those who verify under penalty of perjury they are physically unable to go to the poll site on

election day or to early voting locations. (Do away with no-excuse absentee voting.)

- 6. Security cannot be sacrificed for convenience and cost.**
- 7. Difficulty recruiting pollworkers can be overcome through successful efforts such as Pollworkers for Democracy.**
- 8. Make election day a national holiday.**
 - a. Move an existing holiday (Veteran's Day or Memorial Day) to election day.
- 9. Oregon vote-by-mail experience does not justify use in California.**
 - a. Election integrity advocates in Oregon say their vote-by-mail system has not been tested against a hand-audit of the ballots to verify there is no tampering. (HB 3270 was recently introduced in the Oregon House to institute a verification procedure involving a manually counted random sample of the paper ballots to compare with the machine-tallied results. Source: *Why we need HB 3270 to verify elections in Oregon*, Statesman Journal, 4-3-07.)
 - b. Election integrity advocates in Oregon also say vote-by-mail is not appropriate for places with Jim Crow issues or a history of election fraud, nor in large states.
- 10. City/County Clerks have shown they are willing to sacrifice election security for cost and convenience.**
 - a. One major constituency promoting vote-by-mail is local election officials (city and county clerks/ROVs). However, they also opposed a voter verified paper trail for paperless touchscreen voting machines, showing they are willing to sacrifice election security for cost and convenience.

III. SOLUTION

- 1. Reduce the trend toward vote-by-mail and improve checks and balances as follows:**
 - a. The primary voting method should be the most secure voting method: voting at the local precinct on election day with the provisions outlined below. This method lends itself to public oversight during all phases, including set-up and the closing of the polls.
 - i. Marin County has established written procedures for deployment and chain of custody of ballots and voting equipment for poll site voting. All counties should be required to prepare such procedures (if not already mandatory.)
 - ii. Ballots should be hand-cast on paper and optically scanned. This method is preferable to touchscreens (DREs) for many reasons, including but not limited to: 1) studies show that most voters who use touchscreens don't check the paper trail to confirm accuracy, and that; 2) voters who do check the paper trail from the touchscreens miss most inaccuracies; 3) touchscreens can result in longer wait times to vote; 4) power outages or

- malfunctioning machines could halt voting on touchscreens; and 5) optical scan systems are cheaper than touchscreens.
- iii. A mandatory hand-audit of 10% of randomly selected ballots should take place at the poll site after polls close and before the ballots leave the poll site. This would confer 99% statistical accuracy that votes tabulated precisely match the votes that were cast.
 - iv. A 10% hand-audit would not be prohibitively time-consuming, consisting of approximately 50-60 ballots (assuming 50-60% turnout) taking about 3.7 to 4.4 minutes per race (based on observations of Marin County's Nov. 2006 post-election 1% hand tally). (In Marin County it took an average of about 7.3 minutes per 100 ballots to hand-count one race.) High school students could be recruited to assist with the 10% hand-count if necessary.
 - v. Retain the existing mandatory 1% (or more) post-election hand-count of randomly selected precincts at the county site. This would serve as a check and balance against the 10% poll site hand-audit, and would include early voting, mail-in/absentee, and provisional ballots that are not included in the 10% poll site hand-audit.
 - vi. It's worth noting that Bev Harris of Black Box Voting has said that paper ballots, hand-counted in public view have perhaps five or six "attack vectors," whereas elections conducted with electronic equipment have about 50 or 60. See <http://coalition4visibleballots.homestead.com/index.html>.
- b. Voters unable to vote at the polls on election day can vote early in person at the county early voting site(s). This option should be reserved for voters who verify under penalty of perjury they are physically unable to vote at their local precinct on election day. Early voting sites should be as secure as possible, with public oversight allowed during all phases and written procedures specifying strict chain-of-custody and other security measures.
 - c. Mail-in voting should be a last resort reserved only for people who verify under penalty of perjury that they are physically unable to vote at their local precinct on election day nor at the county's early voting site(s).
 - d. Suspend the use of tax dollars to promote vote-by-mail.
 - e. Require that all mail-in ballots and their corresponding tallies be kept, tabulated, and reported by precinct separately from ballots cast at the precinct. Similarly, ballots cast during early voting should also be kept, tabulated, and reported separately. This would enable the public to analyze the results by voting method to check for anomalies suggesting error or fraud.
 - f. Enact other measures to better secure mail-in voting. For example, John Fortier, a scholar at the American Enterprise Institute and author of "Absentee and Early Voting," suggests ways to retain the convenience of pre-Election Day voting but with a lower risk of fraud and intimidation. He suggests:

- i. States could expand hours at polling places for early voting, but only during the 10 days before the election.
- ii. New computer software can be used to match signatures on absentee ballots with registration records and flag those that raise concerns. (Note: a signature should never be deemed invalid until human eyes have physically reviewed the signature and compared it with the registration record, and a log kept as to why the signature was not accepted, who made the final determination, and when. The process should be open to public observers.)
- iii. States could require that every mail-in voter enclose a fingerprint or photocopy of some form of identification, not necessarily a photo ID.
- iv. States should hire independent investigators to interview a sample of voters about potential coercion or intimidation.

From: Connie Pracht
Sent: Friday, August 03, 2007 1:06 PM
To: Voting Systems
Subject: IMPERATIVE----VIEW IMMEDIATELY!!!!

Dear Ms. Bowen,

Attached is a compilation of materials that I have been researching for the last 8 years. Please look closely at the first 2 pages before making your decision today regarding our voting equipment. I am also doing a copy paste of some points here:

Diebold Election Systems

Diebold Elections Systems is run by [Bob Urosevich](#), who has been working in the election systems industry since 1976. In 1979, Mr. Urosevich founded [American Information Systems](#). He served as the President of AIS from 1979 through 1992, and that company, now known as [Election Systems & Software, Inc.](#), counted over 100 million ballots in the U.S. 2000 General Election. Bob's brother, [Todd Urosevich](#), is Vice President, Aftermarket Sales with ES&S. In 1995, Bob Urosevich started [I-Mark Systems](#), whose product was a touch screen voting system utilizing a smart card and biometric encryption authorization technology. [Global Election Systems, Inc.](#) acquired I-Mark in 1997, and on July 31, 2000 Mr. Urosevich was promoted from Vice President of Sales and Marketing and New Business Development to President and Chief Operating Officer. On January 22, 2002, Diebold announced the acquisition of GES, then a manufacturer and supplier of electronic voting terminals and solutions. The total purchase price, in stock and cash, was \$24.7 million. Global Election Systems subsequently changed its name to Diebold Election Systems, Inc.

Accusations & criticism

Together Election Systems & Software, Inc. and Diebold Election Systems, Inc. are responsible for tallying around 80% of votes cast in the United States. The [software architecture](#) common to both is a creation of Mr. Urosevich's company [I-Mark](#). Some critics claim that this structure is easily compromised, in part due to its reliance on [Microsoft Access](#) databases. [Britain J. Williams](#), responsible for certification of voting machines for the state of [Georgia](#) has provided a negative assessment based on her accounting of potential exploits.

In August [2003](#), [Walden O'Dell](#), chief executive of Diebold, announced that he had been a top fund-raiser for [President George W. Bush](#) and had sent a get-out-the-funds letter to [Ohio Republicans](#). When assailed by critics for the perceived conflict of interest, he pointed out that the company's election machines division is run out of [Texas](#) by a registered [Democrat](#). Nonetheless, he vowed to lower his political profile lest his personal actions harm the company.

Thank you for your protection of our vote--without it's protection and reliability we don't have a Republic.

Please contact me at:

Connie Pracht

562-421-5259

Diebold

From Wikipedia, the free encyclopedia.

Diebold, Incorporated is a security systems company which is engaged primarily in the sale, manufacture, installation and service of self-service transaction systems (such as [ATMs](#)), electronic and physical security products (including vaults and currency processing systems), and software and integrated systems for global financial and commercial markets. It has recently entered the business of creating [electronic voting](#) terminals and solutions for government entities. Diebold was incorporated

under the laws of the State of [Ohio](#) in August, 1876, and is headquartered in [North Canton, Ohio](#).

Table of contents

- [1 Diebold Election Systems](#)
- [1.1 Accusations & criticism](#)
- [2 Current controversy](#)
- [3 External links](#)

Diebold Election Systems

Diebold Elections Systems is run by [Bob Urosevich](#), who has been working in the election systems industry since 1976. In 1979, Mr. Urosevich founded [American Information Systems](#). He served as the President of AIS from 1979 through 1992, and that company, now known as [Election Systems & Software, Inc.](#), counted over 100 million ballots in the U.S. 2000 General Election. Bob's brother, [Todd Urosevich](#), is Vice President, Aftermarket Sales with ES&S. In 1995, Bob Urosevich started [I-Mark Systems](#), whose product was a touch screen voting system utilizing a smart card and biometric encryption authorization technology. [Global Election Systems, Inc.](#) acquired I-Mark in 1997, and on July 31, 2000 Mr. Urosevich was promoted from Vice President of Sales and Marketing and New Business Development to President and Chief Operating Officer. On January 22, 2002, Diebold announced the acquisition of GES, then a manufacturer and supplier of electronic voting terminals and solutions. The total purchase price, in stock and cash, was \$24.7 million. Global Election Systems subsequently changed its name to Diebold Election Systems, Inc.

Accusations & criticism

Together Election Systems & Software, Inc. and Diebold Election Systems, Inc. are responsible for tallying around 80% of votes cast in the

United States. The [software architecture](#) common to both is a creation of Mr. Urosevich's company [I-Mark](#). Some critics claim that this structure is easily compromised, in part due to its reliance on [Microsoft Access](#) databases. [Britain J. Williams](#), responsible for certification of voting machines for the state of [Georgia](#) has provided a negative assessment based on her accounting of potential exploits.

In August [2003](#), [Walden O'Dell](#), chief executive of Diebold, announced that he had been a top fund-raiser for [President George W. Bush](#) and had sent a get-out-the-funds letter to [Ohio Republicans](#). When assailed by critics for the perceived conflict of interest, he pointed out that the company's election machines division is run out of [Texas](#) by a registered [Democrat](#). Nonetheless, he vowed to lower his political profile lest his personal actions harm the company.

DES claims its systems provide strong immunity to [ballot tampering](#) and other [vote rigging](#) attempts. These claims have been challenged, notably by [Bev Harris](#) on her website, [Blackboxvoting.com](#), and book by the same name.

According to critics, the I-Mark and Microsoft software each represent a [single point of failure](#) for the vote counting process, from which 80% of votes can be compromised via the exploit of a single line of code in either subsystem. Harris and [C. D. Sludge](#), an [Internet journalist](#), both claim there is also evidence that the Diebold systems have been exploited to tamper with American elections—a claim Harris expands in her book [Black Box Voting](#).

Sludge further cites [Votewatch](#) for evidence that suggests a pattern of compromised voting machine exploits throughout the 1990s, and specifically involving the Diebold machines in the 2002 election.

Current controversy

Its [voting machines](#), which are made by its subsidiary **Diebold Election Systems** (DES), have caused a public uproar among some opponents, some of which are engaged in "electronic civil disobedience" against legal attempts by Diebold to stop the release and publication of a number of internal memos.

In September [2003](#), a large number of internal Diebold memos, dating back to mid-[2001](#), were posted to the Web by the website organizations [Why War?](#) and the [Swarthmore Coalition for the Digital Commons](#), a group of student activists at [Swarthmore College](#). Diebold's critics believe that these memos reflect badly on Diebold's voting machines and business practices. Diebold has since reportedly sent [takedown requests](#) to sites hosting these documents demanding that they be removed in violation of the [Online Copyright Infringement Liability Limitation Act](#) provisions of the [DMCA](#) found in § 512 of the United States Copyright Act.

In December [2003](#), an internal Diebold memo was leaked to the press, sparking controversy in Maryland. Maryland officials requested that Diebold add the functionality of printing voting receipts. The leaked memo said, "As a business, I hope we're smart enough to charge them up the wazoo [for this feature]".

External links

- [Official site](#)
- [Diebold Election Systems](#) by [Disinfopedia](#)
- [Diebold memos Wiki](#)
- [Why War documents archive](#)
- [Swarthmore Coalition for the Digital Commons](#)
- [Electronic Frontier Foundation case archive](#)
- [SF Indymedia report](#)
- [Wired.com Story](#)

- [Wired story: New Security Woes for E-Vote Firm](#)
 - [Salon story on the controversy](#)
 - [The Inquirer story on the Diebold documents story](#)
 - [investigative report](#) C. D. Sludge summary; Bev Harris on Diebold audit log
 - [evidence of method](#) by Bev Harris - how an [election hacker](#) can exploit Diebold weaknesses
 - [Diebold - the face of modern ballot tampering](#)
 - [Senate Ethics Director resigns](#); Senator [Chuck Hagel](#) admits owning [voting machine](#) company [McCarthy Group](#)
 - [News article concerning O'Dell's political activities](#)
 - [A Metafilter](#) posting that collects a large number of links on the Diebold affair
-

This description is from [Wikipedia](#). It is available under the terms of the [GNU Free Documentation License](#).

An investigation into the serious election problems that occurred in various state primaries and the behind the scenes difficulties with our voting system.

By Elaine Kitchel

This is a follow-up to Ms. Kitchel's earlier article, [Today Indiana, Tomorrow Your State](#)

Tangled does not even begin to describe the messy web made of our voting system. It's not only tangled; it's matted, convoluted, and it stinks to high heaven. And dead center in the web is a dangerous little "black box" with a red hourglass on it. The black box is inside each and every voting machine, and it holds the source code for every function of encoding, decoding, identification, authentication, and tallying of votes put into it. And the source code belongs to the two companies which manufacture and sell the

electronic voting machines that could be responsible for counting roughly 80% of the votes in November's election.

What else does the black box hold? Ah, that's the sixty-four-thousand-dollar question. In the case of Diebold, which has sold electronic voting machines all over the country, including twenty counties in Ohio, a key state, the box holds a nifty little piece of code that can be opened without a password using Microsoft Access. According to Bev Harris, activist and author of [Black Box Voting](#), this code makes three ledgers. The first ledger is the actual vote and tally. This can be sent off from a precinct to the state's central election location. But the second ledger can be manipulated to reflect any votes and tallies one wishes. The results from this ledger can be sent instead of the first, with no one being the wiser. It's so simple, anyone who can read can do it. Now isn't that handy? No one knows what the third ledger does, except Diebold, and probably ES&S. Read more about this here: [Inside a U.S. Election Vote Counting Program](#).

Another big player in election machines is ES&S. What would you say if you knew that the founders of Diebold and ES&S were brothers? That's right; Todd and Bob Urosevich are top dogs in each of these companies. Bob Urosevich, the CEO and founder of ES&S, oversaw the development of the software that is now used in his brother's Diebold machines. I'm betting both have a similar code inside the black boxes. Cozy, isn't it? Both are Republicans and have influential Republicans Walden O'Dell and Chuck Hagel in the upper reaches of their corporate structures, and these men have promised to "deliver" the election to George Bush. It's easy to see how that could happen, now that we know what's in the black boxes. And what's more, neither company will declare that what comes out of its machines represents the actual vote. Even so, states just keep buying the machines.

Some states have had trial runs of their ES&S/Diebold machines already. In its

primaries, California had numerous problems with its Diebolds. Some estimates of failure rates of the machines go as high as twenty-five percent. Many of California's voters were not able to vote at all. As a result, California's election oversight committee has decertified the machines and recommended to the state's Attorney General that Diebold be criminally charged for violation of California's election law. Diebold is scrambling to repair sections of the code and get re-certified.

Arkansas has some of the same problems. Lisa Burks, an election activist, writes, "Unfortunately Arkansas still uses the ES&S machines sold by the corrupt vendor in our elections. We have had major problems with their optical scanners, including misprogrammed computer chips during our recent May 18th primary." Even so, some of Arkansas' machines were "reconditioned" and sold to Florida, where they remain still.

Burks continues to say that there are shenanigans aplenty. Here's just one. "A local printer I spoke to told me that he was told to print infrared sensitive numbers on the backs of ballots, not by election officials, but by the vendors. ES&S in our case. We have their machines in 55 of our 75 counties. That printer knew I was active on the voting machine issue and asked me why they would have him do such a thing. He said he questioned the infrared numbers being printed on the backs of the ballots, but did it because 'they told him to.' He did this for a period of time, did not say how long, then the vendors suddenly told him to stop doing it." Burks states that she could find no one related to the elections who knew what the infrared numbers were used for.

Remember, in 2002, Arkansas Secretary of State Bill McCuen pleaded guilty to felony charges that he took bribes, evaded taxes, and accepted kickbacks. According to the *Baton Rouge Advocate*, "Part of the case involved Business Records Corporation, which has now merged to become Election Systems &

Software. Arkansas officials said the scheme involved Tom Eschberger, an employee of BRC. Eschberger got immunity from prosecution for his cooperation. Today, he's a top executive of ES&S."

And don't forget Florida. There's no way to give you a real sense of how messed up Florida is. An entire book would not be enough. But here are a few things to consider:

- DBT On-Line of Boca Raton has now admitted wrongdoing after being sued by the NAACP for violating Floridians' civil rights in the 2000 election. They have turned over to the NAACP's lawyers a report indicating that the state, under the supervision of Katharine Harris, ordered the purge of 94,000 voters and, according to the company's data, no more than 3,000 would have been illegal voters. Most, though not all, of the purged names belonged to black Democrats.
- Sandra Mortham, a Republican, was responsible for bringing ES&S machines into Florida as a lobbyist for the company. The funny thing was, she was also a lobbyist for the Florida Association of Counties, which was purchasing the machines. Mortham has admitted taking kickbacks from ES&S for every machine sold to the Association.
- Ed Kast resigned his post last Tuesday as Florida's election chief. Kast's resignation comes as scrutiny of the 2004 election process intensifies, and after some voting machines in the primaries failed to respond to voters' input.
- Jeb Bush recently signed into law a bill doing away with the witness signature previously required on absentee ballots. Absentee ballot fraud has been an ongoing problem in South Florida, with candidates often buying ballots or stealing them from unsuspecting senior citizens in nursing homes and condominiums. In 1997, a Miami election was overturned for this kind of fraud.

Don't hold your breath for a fair election in Florida. In fact, don't hold it for a fair election anywhere. Without a paper trail, votes simply cannot be verified, and

that's what unscrupulous politicians and their accomplices in the voting machine industry are depending on. How hard is it to make a paper trail? Here's what a Diebold spokesman had to say: "While Diebold is certainly capable of producing receipt printers, we currently have no plans to manufacture receipt printers primarily because our customers haven't requested it." Some states are beginning to request it since that statement was made, but not many.

Every voter has the right to expect his vote to be counted. And every voter has the right to make his election officials PROVE that a fair election has taken place in his state. But without a paper trail that verifies each vote, no election official can prove the reliability of the vote. This opens the door for litigation to improve the system. Ed Kast won't be the only official resigning this year.

So if the picture for a fair election is so bleak, why should you vote? Here are a few reasons:

- Most election officials are decent folk. You may live in a county or precinct where officials take great care and do their jobs. Your vote may get counted.
- If you don't vote, you have no right to complain. Can you really keep your mouth shut for four more years?
- If you do vote, and your party's vote is skewed or manipulated, you can help fix the problem by joining in a suit against the offenders. Often, this is the only way to change things.

So why isn't Kerry worried? Why isn't he holding his nose? We've heard nothing from him on this issue. We know why Bush isn't complaining. Is John Kerry confident there will be more talented hackers on the Democratic side? Does he know something we don't? I'm puzzled. Aren't you?

Here's [John Kerry's website](#), where you can find an address if you would like to write to ask him.

Read more about the paperless vote: [Count the Vote](#), as well as Ms. Kitchel's earlier article, [Today Indiana, Tomorrow Your State](#).

Elaine Kitchel lives in Indiana where she is a research scientist. She closely watches the political scene and writes about it, instead of jumping from her 4th floor office window in disgust. You can email Elaine at

Elaine@interventionmag.com

Posted Sunday, June 13, 2004

Report Raises Electronic Vote Security Issues

John Schwartz | **New York Times** | **September 25, 2003**

"Electronic voting machine technology used nationwide is 'at high risk of compromise' because of software flaws that could make them vulnerable to computer hackers and voting fraud."

Electronic voting machine technology used nationwide is "at high risk of compromise" because of software flaws that could make them vulnerable to computer hackers and voting fraud, according to a review released yesterday. The report also said, though, that proper safeguards could help to mitigate the risk.

The new report, the second concerning voting machines from Diebold Election Systems, was conducted for the state of Maryland after researchers warned this summer that the Diebold AccuVote-TS voting machines, more than 33,000 of which are used in 38 states, may be vulnerable to manipulation. Maryland is adopting the machines for elections.

Diebold executives and Maryland officials said the report vindicated their view that the machines could be used reliably.

The new report, said Mark Radke, a Diebold executive, "really confirms our stance that our equipment is as secure, if not more secure, than any other electronic system in the marketplace." The company is working to improve the security even further, he added.

In a letter yesterday, James C. DiPaula, secretary of the state's Department of Management and Budget, recommended to Gov. Robert L. Ehrlich Jr. that the state advance a plan which he said "will correct specific risk factors and ensure reliability of the election process."

The [earlier study](#), released in July, said Diebold software contained numerous security gaps that could be exploited to let people vote many times or to change votes after the fact. Aviel D. Rubin, a computer security researcher, and colleagues analyzed Diebold source codes that had been leaked to the Internet by critics of electronic voting systems.

Yesterday's report, by the Science Applications International Corporation, said that Mr. Rubin's conclusions about the company's software were "technically correct," but that the researchers "did not have a complete understanding" of Maryland's use of the system.

In an interview yesterday, Mr. Rubin said he was mystified to see that the state planned to use Diebold machines despite the report.

"It almost seems as though the people writing the Maryland action plan either did not read or did not understand the S.A.I.C. report," he said. "What they should say is, 'We're going to put these systems on hold until they say that these things are safe to use.' "

James T. Smith, the Baltimore County executive, who has opposed the move to electronic voting, said the new report should stop the state from using the machines.

"For two years, Baltimore County has warned, 'Iceberg ahead!' and now independent experts have warned that it's a gigantic iceberg," Mr. Smith said.

"Maryland should not say, 'Damn the iceberg, full speed ahead.' "

www.nytimes.com/2003/09/25/technology/25VOTE.html?ex=1066795200&en=98d975f47510c

Test of Electronic Balloting System Finds Major Security Flaws

John Schwartz | New York Times | January 30, 2004

A report presented to the Maryland state legislature indicated that Diebold voting systems, which have been purchased by many states, are not tamper-proof.

Electronic voting machines from [Diebold Inc.](#) have computer security and physical security problems that might allow corrupt insiders or determined outsiders to disrupt or even steal an election, according to a report presented yesterday to Maryland state legislators.

But authors of the report — which described the first official effort to hack Diebold voting systems under election conditions — were careful to say the machines, if not hacked, count votes correctly. And they said the vulnerabilities the exercise found could be addressed in a preliminary way in time for the state's primaries in March.

"I don't want to beat people up," said Michael Wertheimer, a security expert for RABA Technologies in Columbia, Md., who oversaw the exercise. "I want to get an election that people can feel good about."

Further steps could be taken to ensure a safe general election in November, the report concluded. But ultimately, it said, Diebold election software had to be rewritten to meet industry security standards and limited use of paper receipts to verify votes would be needed.

A spokesman for Diebold, which is based in North Canton, Ohio, emphasized the report's positive elements. "There is nothing that has not been, or can't be, mitigated" before the election, David Bear, the spokesman, said.

In a statement, Bob Urosevich, president of the Diebold election-systems unit, said that this report and another by the Science Applications International Corporation "confirm the accuracy and security of Maryland's voting procedures and our voting systems as they exist today."

Maryland has spent more than \$55 million for the machines. Georgia has chosen Diebold for elections statewide, and major counties in California and Ohio, among other states, have picked the machines.

The report's authors said they had expected a higher degree of security. "We were genuinely surprised at the basic level of the exploits" that allowed tampering, said Mr. Wertheimer, a former security expert for the National Security Agency.

The report supports the findings of a study released in July, by academic security experts at Johns Hopkins and Rice universities, that found Diebold software lacked the level of security needed to safeguard elections. Diebold stated that the code used by the researchers, which had been taken from a company Internet site and circulated online, was outdated. A subsequent report by Science Applications International found some similar problems.

Aviel D. Rubin, who led the Johns Hopkins effort, said, "If our report was unable to convince Maryland that the Diebold machines were vulnerable, then surely this work will set them straight."

The latest study found that some problems identified in the Hopkins study had not been corrected, and discussed other issues it found equally troubling.

Security experts found that the touch-screen voting machines all used the same key to two locks that protect them from tampering. With handheld computers and a little sleight of hand, they also found, the touch screens could be reprogrammed to make a vote for one candidate count for another, or results could be fouled so that a precinct's vote could not be used.

Communications between the terminals and the larger server computers that tabulate results from many precincts do not require that machines on either end of the line prove they are legitimate, which could let someone grab information that could be used to falsify whole precincts' worth of votes.

The group also found that the server computers did not have the latest protection against the security holes in the Microsoft operating systems, and were vulnerable to hacker attacks that would allow an outsider to change software.

www.nytimes.com/2004/01/30/politics/campaign/30SECU.html

Civil Rights Groups Sue Diebold Over Threats

Rachel Konrad | **Associated Press** | **November 4, 2003**

"Many groups are refusing to remove from their Web sites internal Diebold documents that they claim raise serious security questions and threaten the U.S. elections process."

SAN JOSE, Calif. — Attorneys specializing in free speech on the Internet filed suit Tuesday against Diebold Inc., demanding the voting equipment company stop sending legal threats to organizations that publish its leaked documents.

The Electronic Frontier Foundation and Stanford University's Cyberlaw Clinic filed for a temporary restraining order in federal court. Judge Jeremy Fogel in San Jose is expected to issue a decision this week.

Computer programmers, Internet service providers and students from at least 20 universities, including the University of California, Berkeley, and the Massachusetts Institute of Technology, have received the cease-and-desist orders from Diebold.

Many groups are refusing to remove from their Web sites internal Diebold documents that they claim raise serious security questions and threaten the U.S. elections process.

Diebold executives could not be reached Tuesday, but spokesman Mike Jacobsen said in late October that the cease-and-desist orders do not mean the documents are authentic — nor do they give credence to advocates who claim lax Diebold security could allow hackers to rig machines. Jacobsen warned that some of the 13,000 pages of stolen documents may have been altered after they were stolen from the company's central server.

In March, a hacker broke into Diebold's servers using an employee's ID number, and copied company announcements, software bulletins and internal e-mails dating back to January 1999, Jacobsen said.

The vast majority of the 1.8 gigabits of data contain little more than banal employee e-mails, routine software manuals and old voter record files. But several items seem to raise security concerns.

In one series of e-mails, a senior engineer dismisses concern from a lower-level programmer who questions why the company lacked certification for a customized operating system used in touch-screen voting machines. The Federal Election Commission requires voting software to be certified by an independent research lab.

In another e-mail, a Diebold executive scolded programmers for leaving software files on an Internet site without password protection.

"This potentially gives the software away to whomever wants it," the manager wrote in the e-mail.

In August, the hacker e-mailed the data to voting activists, some of whom published stories on their Web logs. A freelance journalist at *Wired News* also received data and wrote about it in an [online story](#).

The data was further distributed in digital form online, and it can still be found at [dozens of sites](#) — including some in Australia, New Zealand, Canada and Italy. It's unclear how many sites link to the data.

EFF staff attorney Wendy Seltzer said activists are trying to publicize alleged security breaches at Diebold, which has more than 50,000 touch-screen voting terminals nationwide. Publishing stolen documents from one of the nation's largest election equipment vendors, she says, is more important than honoring copyrights.

"People are using these documents to talk about how the votes are counted," Seltzer said. "The First Amendment protects them."

San Francisco-based EFF represents Online Policy Group, a nonprofit ISP that hosts the San Francisco Bay Area Independent Media Center.

www.miami.com/mld/miamiherald/business/7182111.htm

New Security Woes for E-Vote Firm

[Brian McWilliams](#) | [Wired News](#) | [August 7, 2003](#)

"The archive of internal Diebold Election Systems mailing lists taken from the staff site includes thousands of messages dating from January 1999 through March 2003. ... Diebold's Internet security problems necessitate that the company hire a 'Big Five-caliber' firm to conduct a thorough inspection of its software code, and to insure that malicious outsiders have not tampered with it."

Following an embarrassing leak of its proprietary software over a file transfer protocol site last January, the inner workings of Diebold Election Systems have again been laid bare.

A hacker has come forward with evidence that he broke the security of a private Web server operated by the embattled e-vote vendor, and made off last spring with Diebold's internal discussion-list archives, a software bug database and more software.

The unidentified attacker provided *Wired News* with an archive containing 1.8 GB of files apparently taken March 2 from a site referred to by the Ohio-based company as its "staff website."

Representatives of Diebold Election Systems, one of the largest electronic voting systems vendors with more than 33,000 machines in service around the country, said the company is still investigating the security breach and reviewing the contents of the archive.

Director of Communications John Kristoff said the stolen files contained "sensitive" information, but he said Diebold is confident that the company's electronic voting system software has not been tampered with.

"Thus far we haven't seen anything that would be of use to anyone trying to affect the outcome of an election," he said.

But experts said the appearance of the archive of purloined files from the staff site raises new questions about Diebold's attention to the security of its intellectual property.

"They claim they keep everything secure, but this shows the lax nature of their procedures. This just blatantly flies in the face of good security," said Rebecca Mercuri, a computer science professor at Bryn Mawr College who opposes the use of electronic voting systems.

The anonymous attacker said he broke into the Diebold staff site, which was located at <https://staff.dieboldes.com>, after reading in January about how unauthorized outsiders had copied source code and documentation from an insecure FTP site operated by the company at the Internet address <ftp://ftp.gesn.com>.

"In a few short minutes I had access to their replacement for the FTP site, their 'secure' web," wrote the hacker.

Last month, researchers at Johns Hopkins University used source code from the FTP site to publish an analysis of what they claimed were serious security problems in Diebold's AccuVote-TS voting terminal. Diebold attempted last week to rebut the researchers' charges.

The archive of internal Diebold Election Systems mailing lists taken from the staff site includes thousands of messages dating from January 1999 through March 2003. The lists contained internal company discussions of product support issues, new software announcements and general company announcements.

"We do not believe there is any real security threat, but perception matters a great deal in this business!" wrote Pat Green, Diebold Election Systems' director of research and development, in a Feb. 7 message to the company's "support"

discussion list. Green was announcing the temporary shutdown of the Diebold staff site.

Two days before, on Feb. 5, activist Bev Harris detailed in an article at New Zealand news site called *Scoop* how she had freely accessed thousands of files from Diebold's FTP server.

The hacker did not reveal how he subsequently breached the security of the Diebold staff site, which used SSL encryption. The file archive included source code to a login page that included a March 2 welcome message to one of the firm's election support specialists, suggesting the attacker may have compromised the employee's account.

Judging from internal mailing list discussions, Diebold management was either unaware of proper information security practices, or chose to ignore them out of expediency, experts said.

"There is no sane reason to put the corporate jewels on an Internet-facing server. They were basically asking to be hacked," said Jeff Stutzman, CEO of ZNQ3, a provider of information security services. "This is the kind of behavior you expect of a startup company that's only concerned about selling their first product."

But Kristoff said the staff server housed only compiled, executable programs, and not the raw source code to Diebold's election systems. He said it was "an oversight" that source code was available to the public from the FTP server in January.

The Diebold discussion-list archives included other warnings of potential security problems. In May 2000, Diebold Election Systems' systems engineer manager Talbot Iredale posted a message to the support list chiding employees for placing software files on the special "customer" section of the FTP site without password-

protecting them. That section of the site was created for delivering program updates and other files to election officials and other customers.

"This potentially gives the software away to whom ever (*sic*) wants it," wrote Iredale.

On Dec. 2 last year, Diebold Election Systems' webmaster Joshua Gardner announced to the list that the FTP site finally was being eliminated and replaced by the staff site. Gardner explained that the FTP site had been "accessible to the outside world with no restrictions on access, and no provisions for logging user activity. FTP was a security risk, and I have shut it down for this reason."

Yet nearly eight weeks later, Internet users apparently still were able to access the FTP site without a password and to download proprietary software and manuals.

Kristoff said Diebold has shut down the FTP and staff sites, and the company no longer provides customers or field personnel with access to Diebold software over the Internet. Instead, software and proprietary data has been distributed by CD-ROM since January, he said.

Even if unauthorized individuals were able to access and modify voting system source code, some e-voting experts downplay the impact of such theoretical threats. After the earlier problems at Diebold's FTP site, Brit Williams of the Center for Election Systems at Kennesaw State University published a report last April noting that some states, such as Georgia, carefully review source code prior to use in electronic voting systems.

But Stutzman said Diebold's Internet security problems necessitate that the company hire a "Big Five-caliber" firm to conduct a thorough inspection of its software code, and to insure that malicious outsiders have not tampered with it.

"To gain credibility back, they ... have to do a line-by-line audit to make sure that their intellectual property is still sound," said Stutzman.

www.wired.com/news/privacy/0,1848,59925,00.html

Voting Machine Controversy

[Julie Carr Smyth](#) | [Cleveland Plain Dealer](#) | [August 28, 2003](#)

"[A] letter from Walden O'Dell, chief executive of Diebold Inc. — who has become active in the re-election effort of President Bush — prompted Democrats this week to question the propriety of allowing O'Dell's company to calculate votes in the 2004 presidential election."

COLUMBUS — The head of a company vying to sell voting machines in Ohio told Republicans in a recent fund-raising letter that he is "committed to helping Ohio deliver its electoral votes to the president next year."

The Aug. 14 letter from Walden O'Dell, chief executive of Diebold Inc. — who has become active in the re-election effort of President Bush — prompted Democrats this week to question the propriety of allowing O'Dell's company to calculate votes in the 2004 presidential election.

O'Dell attended a strategy pow-wow with wealthy Bush benefactors — known as Rangers and Pioneers — at the president's Crawford, Texas, ranch earlier this month. The next week, he penned invitations to a \$1,000-a-plate fund-raiser to benefit the Ohio Republican Party's federal campaign fund — partially benefiting Bush — at his mansion in the Columbus suburb of Upper Arlington.

The letter went out the day before Ohio Secretary of State Ken Blackwell, also a Republican, was set to qualify Diebold as one of three firms eligible to sell upgraded electronic voting machines to Ohio counties in time for the 2004 election.

Blackwell's announcement is still in limbo because of a court challenge over the fairness of the selection process by a disqualified bidder, Sequoia Voting Systems.

In his invitation letter, O'Dell asked guests to consider donating or raising up to \$10,000 each for the federal account that the state GOP will use to help Bush and other federal candidates — money that legislative Democratic leaders charged could come back to benefit Blackwell.

They urged Blackwell to remove Diebold from the field of voting-machine companies eligible to sell to Ohio counties.

This is the second such request in as many months. State Sen. Jeff Jacobson, a Dayton-area Republican, asked Blackwell in July to disqualify Diebold after security concerns arose over its equipment.

"Ordinary Ohioans may infer that Blackwell's office is looking past Diebold's security issues because its CEO is seeking \$10,000 donations for Blackwell's party — donations that could be made with statewide elected officials right there in the same room," said Senate Democratic Leader Greg DiDonato.

Diebold spokeswoman Michelle Griggy said O'Dell — who was unavailable to comment personally — has held fund-raisers in his home for many causes, including the Columbus Zoo, Opera Columbus, Catholic Social Services and Ohio State University.

Ohio GOP spokesman Jason Mauk said the party approached O'Dell about hosting the event at his home, the historic Cotswold Manor, and not the other way around. Mauk said that under federal campaign finance rules, the party cannot use any money from its federal account for state-level candidates.

"To think that Diebold is somehow tainted because they have a couple folks on their board who support the president is just unfair," Mauk said.

Griggy said in an e-mail statement that Diebold could not comment on the political contributions of individual company employees.

Blackwell said Diebold is not the only company with political connections — noting that lobbyists for voting-machine makers read like a who's who of Columbus' powerful and politically connected.

"Let me put it to you this way: If there was one person uniquely involved in the political process, that might be troubling," he said. "But there's no one that hasn't used every legitimate avenue and bit of leverage that they could legally use to get their product looked at. Believe me, if there is a political lever to be pulled, all of them have pulled it."

Blackwell said he stands by the process used for selecting voting machine vendors as fair, thorough and impartial.

As of yesterday, however, that determination lay with Ohio Court of Claims Judge Fred Shoemaker.

He heard closing arguments yesterday over whether Sequoia was unfairly eliminated by Blackwell midway through the final phase of negotiations.

Shoemaker extended a temporary restraining order in the case for 14 days, but said he hopes to issue his opinion sooner than that.

Students Fight E-Vote Firm

[Kim Zetter](#) | [Wired News](#) | [October 21, 2003](#)

"We're advocating freedom of information and open-source standards," Smith said. "If there's anything the public has an inherent right to look in on, it's voting technology. That's why we're pushing this.' "

A group of students at Swarthmore College in Pennsylvania has launched an "electronic civil disobedience" campaign against voting machine maker Diebold Election Systems.

The students are protesting efforts by Diebold to prevent them and other website owners from linking to some 15,000 internal company memos that reveal the company was aware of security flaws in its e-voting software for years but sold the faulty systems to states anyway. The memos were leaked to voting activists and journalists by a hacker who broke into an insecure Diebold FTP server in March.

Diebold has been sending out cease-and-desist letters to force websites and ISPs to take down the memos, which the company says were stolen from its server in violation of copyright law. It has been using the Digital Millennium Copyright Act, or DMCA, to force ISPs to take down sites hosting the memos or sites containing links to the memos.

Diebold did not respond to *Wired News'* requests for comment.

Bev Harris, owner of the Black Box Voting site and author of a book on the electronic voting industry, was one of the first people to post the memos before a letter from Diebold threatened her with litigation.

Half a dozen other people hosting the memos in the United States, Canada, Italy and New Zealand also have received letters forcing them to take the material down.

Why War?, a nonprofit student organization at Swarthmore, and the Swarthmore Coalition for the Digital Commons, also composed of Swarthmore students, announced plans to defy Diebold and their college ISP.

Why War? posted the memos on its website about two weeks ago but moved them to a student's computer after the college ISP received a cease-and-desist letter.

The college notified the student, who wishes to remain anonymous, that it would disconnect his Internet service if he didn't remove the memos. But Luke Smith, a sophomore, said students are planning to bypass that threat by hosting the memos on different machines. Each time one machine is shut down by Diebold, they will move the memos to another machine, passing them from student to student.

"They're using copyright law as a means of suppressing information that needs to be public," Smith said. "It's a great example of how copyright law can be against the public good rather than for it, as it was originally intended."

He added, "It's not like people are reading these memos in order to steal Diebold's election system. [The company is] trying to use this law, and specifically the mandatory take-down section, to conceal flaws that directly affect the validity of election results. This is a threat to our democracy."

The DMCA, passed by Congress in 1998, includes a "safe harbor" provision that allows ISPs to remove material from the Web that allegedly violates a copyright without suffering legal repercussions from the person who posted the material. The law allows the ISP to remove the content for a minimum of 10 days.

Will Doherty, media relations director for the Electronic Frontier Foundation, said companies have been using the safe-harbor provision to stifle free speech online, and ISPs have caved in to the threats rather than risk facing legal action from the copyright holder.

"We support the right of Swarthmore students or anyone for that matter to link to or to publish information about electronic voting systems that is vital to debate over democratic process," Doherty said.

Doherty and the EFF launched their own resistance campaign last week after a news site, the Independent Media Center, and its Internet provider, the Online Policy Group, received a cease-and-desist letter from Diebold. In addition to his position at EFF, Doherty is executive director of the Online Policy Group, a nonprofit organization that focuses on digital privacy and rights issues.

The Independent Media Center didn't actually post the Diebold memos on its site. However, Diebold objected when a contributor to the news service posted links to other sites that were hosting the memos.

Even if the Independent Media Center had posted the memos, Doherty said the Online Policy Group still would support its right to do so.

"These documents indicate the potential for widespread election fraud in the U.S. or wherever else Diebold voting machines are being used," he said.

The Diebold memos contain a trove of information about the internal workings of the electronic voting machine manufacturer, which has been criticized for poor programming practices.

Among the revelations in the memos was news that the Microsoft Access database used by the Diebold system to count votes was not protected by a password. This means anyone could alter votes by entering the database through an insecure backdoor, via physical access to the machine or remotely, via the phone system.

The memos also reveal that the audit log, which records any activity in the Access database, could be easily altered so that an intruder could erase a record of the intrusion.

These security flaws were pointed out to Diebold in 2001 in memos from a firm that was being paid to audit and certify the software. A Diebold engineer responded by saying the company preferred not to password-protect the database because it was easier for them (presumably Diebold employees) to go into the software and do "end-runs" in the system — a term that describes when someone changes software to fix or work around coding problems.

Other memos indicate that patches were installed in systems after the systems already were certified and delivered to states.

In a January 2002 memo, Ken Clark, a Diebold engineer, discussed modifying voting software designed for machines in California. Because the state was likely to reject a change so late in the game, he proposed making the change as a bug fix to pass muster with election officials rather than undergoing lengthy certification procedures.

Smith, who plans to major in computational linguistics, said members of the public wouldn't have to fight to expose Diebold's business practices if election officials were doing their job.

"It would be great if they were more rigorous but apparently they've dropped the ball because these systems have already been implemented," he said. "There's a definite need to make this info public."

Smith said he's surprised by Diebold's stance regarding the memos.

"If I were Diebold I wouldn't claim copyright protection; I'd claim I hadn't written the memos," he said. "They knowingly created a system that doesn't even have a semblance of security. And then they pass it off on the American public in the name of modernization."

Smith said his group plans to launch a campaign this week to recruit more students to participate in the revolt.

"We're advocating freedom of information and open-source standards," he said. "If there's anything the public has an inherent right to look in on, it's voting technology. That's why we're pushing this."

www.wired.com/news/print/0,1294,60927,00.html

Swarthmore Shuts Down Web Sites of Students Publicizing Company's Voting-Machine Memos

Andrea Foster | Chronicle of Higher Education | October 27, 2003

"Diebold will continue to send copyright-infringement notices to Internet service providers that host the company documents, including the four other institutions — the Massachusetts Institute of Technology, Purdue University, the University of Southern California, and the University of Texas-Pan American."

Swarthmore College last week temporarily shut down the network connections of two students who used the Internet to publicize internal company memos that the students say reveal insecurities in a commercial electronic-voting system.

Calling their exploits an act of civil disobedience, the two have inspired students at four other institutions to help disseminate the documents.

At issue are memos and other materials from Diebold Inc., a producer of electronic-voting machines that is based in North Canton, Ohio. According to the Swarthmore students, and the writer who first obtained the company memos, they reveal that people can tamper with Diebold's vote-counting database and change votes.

But Joseph Richardson, a spokesman for Diebold, said the materials that the students have been distributing were stolen from Diebold, and contain company software and employee correspondence. The company considers the posting of

the materials online to be copyright infringement under the Digital Millennium Copyright Act, he said.

The Swarthmore students who first distributed the memos online are Micah White, a senior, and Andrew Main, a junior. They are affiliated with a liberal student-activist group on the campus called Why War. The students say that distributing the documents is an act of free speech that could lead to fairer elections.

Earlier this month, the Why War Web site, hosted by a commercial Internet service provider, contained links to the Diebold documents. After Diebold told the provider that it was breaking the law by hosting the Web site, Why War moved its site to Swarthmore's server.

Swarthmore then received a letter from Diebold demanding that the college take down the site. The students moved the Why War site to another provider, and also publicized the Diebold documents on their personal Web pages, which are hosted by Swarthmore.

That action is what prompted Swarthmore administrators to sever the students' Internet connections on Thursday. The students then removed the references from their Web sites and their Internet connections were restored the same day, said Mr. White.

He said he was disappointed that the college thwarted Why War's efforts to distribute the documents, particularly since the college was founded by Quakers and encourages students to stand up for their political beliefs.

"There's tremendous support on this campus for Swarthmore taking a stronger stance on this issue," he said. "By them saying, 'It's a copyright violation,' they're weaseling out of their responsibility as a major institution of higher learning that happens to be founded on Quaker principles of truth and civil disobedience."

A spokesman for Swarthmore said the college is proud that the students are acting on their beliefs, but that it cannot support them because that would require the college to support every student political movement on campus. "There are students here pursuing all sorts of political initiatives," said Tom Krattenmaker, a spokesman for Swarthmore. "All of them want the college to commit their resources to their causes."

Apart from Swarthmore, dozens of other Internet service providers that are unaffiliated with colleges have hosted the Diebold documents, including the Online Policy Group, a nonprofit policy-research group. The Electronic Frontier Foundation, a group that promotes civil liberties online, is now representing the Online Policy Group in its fight to keep the documents on its computer server.

Mr. Richardson said Diebold will continue to send copyright-infringement notices to Internet service providers that host the company documents, including the four other institutions — the Massachusetts Institute of Technology, Purdue University, the University of Southern California, and the University of Texas–Pan American. The materials were first obtained by Bev Harris, who is writing a book about modern-day ballot-tampering. According to published accounts, she found the materials on an unprotected Web site while doing a Google search.

chronicle.com/prm/daily/2003/10/2003102703n.htm

Diebold Threatens Publishers of Leaked Documents

Rachel Konrad | Associated Press | October 27, 2003

"Diebold spokesman Mike Jacobsen said the fact that the company sent the cease-and-desist letters does not mean the documents are authentic — or give credence to advocates who claim lax Diebold security could allow hackers to rig machines. But the activists say the mere fact that Diebold was hacked shows that the company's technology cannot be trusted."

SAN JOSE, Calif. — Despite lawsuit threats from one of the nation's largest electronic voting machine suppliers, some activists are refusing to remove from Web sites internal company documents that they claim raise serious security questions.

Diebold Inc. sent "cease and desist" letters after the documents and internal e-mails, allegedly stolen by a hacker, were distributed on the Internet. Recipients of the letters included computer programmers, students at colleges including Swarthmore and at least one Internet provider.

Most of the 13,000 pages of documents are little more than banal employee e-mails, routine software manuals and old voter record files. But several items appear to raise security concerns.

Diebold refused to discuss the documents' contents. Company spokesman Mike Jacobsen said the fact that the company sent the cease-and-desist letters does not mean the documents are authentic — or give credence to advocates who claim lax Diebold security could allow hackers to rig machines.

"We're cautioning anyone from drawing wrong or incomplete conclusions about any of those documents or files purporting to be authentic," Jacobsen said.

But the activists say the mere fact that Diebold was hacked shows that the company's technology cannot be trusted.

"These legal threats are an acknowledgment of the horrific security risks of electronic voting," said Sacramento-based programmer Jim March, who received a cease and desist order last month but continues to publish the documents on his [personal Web site](#).

In one series of e-mails, a senior engineer dismisses concern from a lower-level programmer who questions why the company lacked certification for a customized operating system used in touch-screen voting machines.

The Federal Election Commission requires voting software to be certified by an independent research lab.

In another e-mail, a Diebold executive scolded programmers for leaving software files on an Internet site without password protection.

"This potentially gives the software away to whomever wants it," the manager wrote in the e-mail.

March contends the public has a right to know about Diebold security problems.

"The cease-and-desist orders are like a drug dealer saying, 'Hey, cop, give me back my crack.' It's an incredible tactical blunder," he said.

The documents began appearing online in August, six months after a hacker broke into the North Canton, Ohio-based company's servers using an employee's ID number, Jacobsen said. The hacker copied company announcements, software bulletins and internal e-mails dating back to January 1999, Jacobsen said.

In August, someone e-mailed the data to electronic-voting activists, many of whom published stories on their Web logs and personal sites. A freelance journalist at *Wired News*, Brian McWilliams, also received data and [wrote about it](#) in an online story.

The data was further distributed in digital form around the Internet and it is not known how many copies exist.

Wendy Seltzer, an attorney for the Electronic Frontier Foundation, said she has been contacted by about a dozen groups that received cease-and-desist letters. Among them is Online Policy Group, a nonprofit ISP that hosts the [San Francisco Bay Area Independent Media Center](#), which published links to the data.

Seltzer encouraged them to defy the Diebold cease-and-desist letters.

"There is a strong fair-use defense," Seltzer said. "People are using these documents to talk about the very mechanism of democracy — how the votes are counted. It's at the heart of what the First Amendment protects."

Although Seltzer believes Diebold's legal case to be weak, she worries about a chilling effect.

Angered last week after Swarthmore College told them they could not link to the documents from college-sponsored sites, some students at the liberal arts school near Philadelphia found Internet providers abroad to [host the content](#). Others took down the offending material at their dean's request, but they promised to put the documents back online if Diebold doesn't provide a more detailed explanation within two weeks. Branen Salmon, 22, president of the Swarthmore College Computer Society, said Diebold's threats put the documents in the spotlight.

"A week ago, this was still a murmur," Salmon said last Thursday. "Now this is front page stuff that people are talking about."

seattlepi.nwsourc.com/business/aptech_story.asp?category=1700&slug=Electronic%2

Swarthmore groups told to nix links

Firm says memos were stolen by hacker

By DON RUSSELL

russeld@phillynews.com

Swarthmore College, a school with a history of passive resistance, is drawing the line at "electronic civil disobedience."

Yesterday, the Delaware County school's dean, Robert Gross, asked a pair of student groups to remove Internet links at their Web sites to a trove of damning memos that activists believe reveal potential security flaws in new electronic voting machines.

"The administration explained that we are obliged, according to the law, to advise them to take the memos off the network, and to pursue the legal recourse that is available to them," said Tom Krattenmaker, Swarthmore's director of news and information.

The dispute centers on a widening scandal over new touch-screen voting machines that, critics say, encourage voter fraud and could affect the outcome of local and national elections.

The machines, now installed in 37 states, are being tested for use in some Pennsylvania counties.

The apparent flaws are detailed in a set of 15,000 internal e-mail memos between employees at Diebold Inc., the Ohio voting-machine manufacturer.

Diebold says a hacker illegally copied the memos from its Web site last March.

In recent weeks, the e-mails have surfaced at several Internet sites. In each case, Diebold sent "cease and desist" letters to the computer hosts, demanding them to remove the material.

"It's stolen property," said Diebold spokesman Mike Jacobsen. "The company has taken steps to protect its property."

According to Wired News, the half-dozen other sites that had posted the memos removed them after receiving the letters.

Why War?, a nonprofit student organization at Swarthmore, and a second group, the Swarthmore Coalition for the Digital Commons, posted the memos online about two weeks ago, then announced they would defy Diebold's removal demands as an act of "electronic civil disobedience."

Luke Smith, a Swarthmore sophomore and co-founder of SCDC, said his group would remove the memos, but then seek to re-post them after a mandated 14-day waiting period.

"The way we see it, the college is giving in," Smith said.

"We were actually hoping for a little more understanding and tolerance."

Why War? is expected to maintain links to the memos at a Web site hosted off campus.

Voting Machine Showdown

[Farhad Manjoo](#) | [Salon](#) | [February 10, 2004](#)

"A leading maker of computer election equipment defends itself in court against charges that it overreached itself in trying to stifle critics."

Diebold, one of the nation's leading manufacturers of computerized voting machines, faced off against some of its critics on Monday in U.S. District Court. But this time, the question at issue wasn't whether [the machines could be hacked](#), but whether Diebold was abusing the principles of free speech in an attempt to quash the critics.

Late in the summer of 2003, Diebold found itself at the center of a white-hot controversy over the trustworthiness of the American democratic process. For several months, activists and academics concerned about the security of touch-

screen voting systems had closely scrutinized the company, and they'd found much to worry about: Diebold's voting machines were said to be full of security flaws, and its CEO turned out to be a major supporter of George W. Bush. Then, activists found what they called the smoking gun — a stash of thousands of internal e-mail messages that appeared to prove that Diebold was up to no good.

In the [e-mail messages](#), which were quickly posted on left-leaning sites across the Web, Diebold engineers seem to acknowledge that their products aren't very secure, and they appear to discuss methods of [hiding the problems](#) rather than fixing them. The documents were, naturally, extremely embarrassing to Diebold, which had always maintained that its engineers were the paragon of professionalism, and the firm moved quickly to stifle their publication.

The company claimed that its internal messages were property protected by the Digital Millennium Copyright Act, and it sent out dozens of cease-and-desist letters to Web sites and Internet service providers (ISPs) involved in the publication of the documents. The company targeted not only ISPs that hosted sites that posted the messages but also ISPs that hosted sites that merely linked to the documents, and even ISPs that provided Internet service to *other* ISPs that hosted sites that linked to documents.

In court on Monday, the Electronic Frontier Foundation and other guardians of digital civil liberties argued that Diebold went too far. By hastily sending out cease-and-desist letters, Diebold abused the powers of the DMCA, EFF attorneys said. Even though Diebold ultimately [withdrew](#) its threatening letter to ISPs and promised not to sue anyone "for copyright infringement for the non-commercial use of the materials posted to date," the plaintiffs argued that Diebold ought to be punished for initially attempting use copyright law to stifle speech. "We think it's important that the court make it clear that if you misuse the powers the DMCA has granted copyright holders, there are going to be serious

consequences," said Cindy Cohn, EFF's legal director, in an interview before the hearing.

For critics of the long reach of the DMCA, the EFF's argument is an attractive one. In recent years, copyright law has been used to "chill" many instances of seemingly legitimate, First Amendment-protected speech — everything from [research papers showing the vulnerabilities in music copy-protection schemes](#) to Harry Potter-inspired [erotic fan fiction](#). (The [Chilling Effects Clearinghouse](#), run by the EFF and several universities, documents this trend.)

But Diebold argued at the hearing that its actions were not obviously beyond the pale. Temporarily chilling speech, it suggested, is a right that Congress has sanctioned in copyright legislation, and Diebold acted well within the DMCA when it sent takedown notices to ISPs. Under the law, said Robert Mittelstaedt, Diebold's attorney, a firm can ask providers to remove content as long as they have a reasonable sense that the content is copyrighted. Because Diebold did not "make a knowing misrepresentation" that its content was protected by the DMCA, it should not be liable for any damages stemming from its letters, he said.

In the case, the EFF is representing the Online Policy Group, a San Francisco ISP that provides Internet services to hundreds of nonprofit groups, including the [San Francisco Indymedia](#) site, which published several links to other sites hosting the Diebold memos last fall. On Oct. 10, Diebold sent OPG a letter demanding that it remove the links. For technical reasons, OPG could not just remove the links — it could only pull down the entire Indymedia site, which officials at OPG thought was an overreaction to a simple link. Diebold also sent a cease-and-desist letter to Hurricane Electric, a firm that provides what's known as "upstream" Internet access to OPG — meaning that Hurricane is essentially OPG's ISP. For similar technical reasons, Hurricane also could not force Indymedia to remove the offending link; it could only block Internet access to

OPG, meaning that Indymedia as well as every other site hosted by OPG would go dark, all for a simple link.

The EFF argues that because Diebold was never going to publish and sell its internal discussions, the company's copyright claims on the e-mails were obviously weak, and that the activists who published the e-mails were acting within their "fair use" rights. Diebold ought to have investigated whether the activists had a legitimate fair-use claim before it sent out the takedown notices, Cohn argued; its rash action suggested that it was more interested in stifling speech than in pursuing a legitimate DMCA claim.

"What happened at Diebold was, they said, 'Hey, there's this embarrassing stuff online,'" Cohn said in an interview. "So their lawyers said, 'Here's this easy way to get them down — we don't have to go to a judge, we just say they're copyrighted.' Diebold says, 'Sure, that's cheaper.' What we'd like to have interjected in that conversation is a lawyer saying, 'Wait a minute, we don't have a valid copyright claim.'" EFF asked the judge to make Diebold pay the OPG's attorneys fees and other damages as a way to deter other firms from too quickly reaching for the DMCA.

At the center of this case is the question of whether it should have been obvious to Diebold that its copyright claim was weak. Diebold argues that it isn't obvious that the people who posted the material online had a fair-use right to do so. There is, for instance, no fair-use right to publish documents that are judged especially important to the public good, and publishing all of the e-mails (rather than excerpts from them) might also have run afoul of fair-use doctrines. Diebold's claim was not frivolous, Mittelstaedt said, "therefore no damages."

Diebold could very well be right. The firm might reasonably have decided that activists had no fair-use right to publish the company's internal discussions — but if Diebold is correct, and it turns out that the DMCA does, as the company asserts, give a company the right to shut down hundreds of Web sites just to get

at one hyperlink, that by itself would be a damning commentary on current copyright law.

The judge in the case, Jeremy Fogel, seemed troubled by this prospect but was also deferential to Diebold's view that what it did was within the law. Fogel said he'd try to issue his decision within a month or two.

www.salon.com/tech/feature/2004/02/10/diebold_copyright/print.html

Analysis: Black Box Voting Blues

Steven Levy | Newsweek | November 3, 2003

"The best minds in the computer-security world contend that [electronic] voting terminals can't be trusted."

After the traumas of butterfly ballots and hanging chad, election officials are embracing a brave new ballot: sleek, touch-screen terminals known as direct recording electronic voting systems (DRE). States are starting to replace their Rube Goldbergesque technology with digital devices like the Diebold Accu-Vote voting terminal. Georgia uses Diebolds exclusively, and other states have spent millions on such machines, funded in part by the 2002 federal Help America Vote Act. Many more terminals are on the way.

Unfortunately, the machines have "a fatal disadvantage," says Rep. Rush Holt of New Jersey, who's sponsoring [legislation](#) on the issue. "They're unverifiable. When a voter votes, he or she has no way of knowing whether the vote is recorded." After you punch the buttons to choose your candidates, you may get a final screen that reflects your choices—but there's no way to tell that those choices are the ones that ultimately get reported in the final tally. You simply have to trust that the software inside the machine is doing its job.

It gets scarier. The best minds in the computer-security world contend that the voting terminals can't be trusted. Listen, for example, to Avi Rubin, a computer-

security expert and professor at Johns Hopkins University who was slipped a copy of Diebold's source code earlier this year. After he and his students examined it, he [concluded](#) that the protections against fraud and tampering were strictly amateur hour. "Anyone in my basic security classes would have done better," he says. The cryptography was weak and poorly implemented, and the smart-card system that supposedly increased security actually created new vulnerabilities. Rubin's paper concluded that the Diebold system was "far below even the most minimal security standards." Naturally, Diebold disagrees with Rubin. "We're very confident of accuracy and security in our system," says director of Diebold Election Systems Mark Radke.

After Rubin's paper appeared, Maryland officials—who were about to drop \$57 million on Diebold devices—commissioned an outside firm to look at the problem. The resulting [report](#) confirmed many of Rubin's findings and found that the machines did not meet the state's security standards. However, the study also said that in practice some problems were mitigated, and others could be fixed, an attitude Rubin considers overly optimistic. "You'd have to start with a fresh design to make the devices secure," he says.

In the past few months, the computer-security community has been increasingly vocal on the problems of DRE terminals. "I think the risk [of a stolen election] is extremely high," says David Dill, a Stanford computer scientist. The devices are certified, scientists say, but the process focuses more on making sure that the machines don't break down than on testing computer code for Trojan horses and susceptibility to tampering. While there's no evidence that the political establishment actually wants vulnerable machines, the Internet is buzzing with conspiracy theories centering on these "[black box](#)" voting devices. (The biggest buzz focuses on the [2002 Georgia gubernatorial election](#), won by a Republican underdog whose win confounded pollsters.) Suspicions run even higher when people learn that some of those in charge of voting technology are themselves partisan. Walden O'Dell, the CEO of Diebold, is a major fund-raiser for the Bush

re-election campaign who recently [wrote to contributors](#) that he was “committed to helping Ohio deliver its electoral votes for the president next year.” (He later clarified that he wasn’t talking about rigging the machines. Whew.)

To remedy the problem, technologists and allies are rallying around a scheme called [verifiable voting](#). This supplements electronic voting systems with a print-out that affirms the voter’s choices. The printout goes immediately into a secure lockbox. If there’s a need for a recount, the paper ballots are tallied. It’s not a perfect system, but it could keep the machines honest. If Representative Holt’s proposed [Voter Confidence Act](#) is passed, verification will be the law of the land by the 2004 election, but prospects are dim, as the committee chairman, Bob Ney of Ohio, is against it.

Critics of verifiable voting do have a point when they note that the printouts are susceptible to some of the same kinds of tricks once played with paper ballots. But there’s a promise of more elegant [solutions](#) for electronic voting that are private, verifiable and virtually tamperproof. Mathematician David Chaum has been working on an [ingenious scheme](#) based on encrypted receipts. But whatever we wind up using, it’s time for politicians to start listening to the geeks. They start from the premise that democracy deserves no less than the best election technology possible, so that the vote of every citizen will count. Can anyone possibly argue with that?

www.msnbc.com/news/985033.asp?cp1=1

[How to Hack an Election](#)

EDITORIAL | [New York Times](#) | [January 31, 2004](#)

"When the State of Maryland hired a computer security firm to test its new machines, these paid hackers had little trouble casting multiple votes and taking over the machines' vote-recording mechanisms. The Maryland study shows convincingly that more security is needed for electronic voting, starting with voter-verified paper trails."

Concerned citizens [have been warning](#) that new electronic voting technology being rolled out nationwide can be used to steal elections. Now there is proof. When the State of Maryland hired a computer security firm to test its new machines, these paid hackers had little trouble casting multiple votes and taking over the machines' vote-recording mechanisms. The [Maryland study](#) shows convincingly that more security is needed for electronic voting, starting with voter-verified paper trails.

When Maryland decided to buy 16,000 AccuVote-TS voting machines, there was considerable opposition. [Critics charged](#) that the new touch-screen machines, which [do not create a paper record](#) of votes cast, were vulnerable to vote theft. The state commissioned a staged attack on the machines, in which computer-security experts would try to foil the safeguards and interfere with an election.

They were disturbingly successful. It was an "easy matter," they reported, to reprogram the access cards used by voters and vote multiple times. They were able to attach a keyboard to a voting terminal and change its vote count. And by exploiting a software flaw and using a modem, they were able to change votes from a remote location.

Critics of new voting technology are often accused of being alarmist, but this state-sponsored study contains vulnerabilities that seem almost too bad to be true. Maryland's 16,000 machines all have identical locks on two sensitive mechanisms, which can be opened by any one of 32,000 keys. The security team had no trouble making duplicates of the keys at local hardware stores, although that proved unnecessary since one team member picked the lock in "approximately 10 seconds."

[Diebold](#), the machines' manufacturer, rushed to issue a self-congratulatory press release with the headline "Maryland Security Study Validates Diebold Election Systems Equipment for March Primary." The study's authors were shocked to see their findings spun so positively. Their report said that if flaws they identified

were fixed, the machines could be used in Maryland's March 2 primary. But in the long run, they said, an extensive overhaul of the machines and at least a limited paper trail are necessary.

The Maryland study confirms concerns about electronic voting that are rapidly accumulating from [actual elections](#). In Boone County, Ind., last fall, in a particularly colorful example of unreliability, an electronic system initially recorded more than 144,000 votes in an election with fewer than 19,000 registered voters, County Clerk Lisa Garofolo said. Given the [growing body of evidence](#), it is clear that electronic voting machines cannot be trusted until more safeguards are in place.

www.nytimes.com/2004/01/31/opinion/31SAT1.html

Touch-Screen Voting 'Disaster' with a 'Myriad of Problems'

Larry Carson | Baltimore Sun | September 26, 2003

"Maryland's rush to convert 19 counties to touch-screen voting before the March 6 primary election will impose a tough deadline, local officials say, leading Howard County's elections administrator to warn yesterday that the pressure could create 'the combination for disaster' on election day."

Maryland's rush to convert 19 counties to touch-screen voting before the March 6 primary election will impose a tough deadline, local officials say, leading Howard County's elections administrator to warn yesterday that the pressure could create "the combination for disaster" on election day.

"I feel very uneasy about it. There are too many loose ends," said administrator Robert J. Antonetti, who has a staff of seven and 33 years of experience running election boards in Prince George's and Howard counties.

Baltimore County Executive James T. Smith asked the state to delay using the new machines in his county until 2006, to give the county time to ensure that

technical questions about the security of voting results can be resolved. State officials rejected the request.

"We can't afford to be on the leading edge of technology when it comes to elections. They have a myriad of problems to fix, which we knew were going to be the case," Smith said, calling the March deadline "an arbitrary timetable that is totally unnecessary."

Anne Arundel County Executive Janet Owens said that although she is confident of her county board's abilities, she is concerned about the short time frame, especially when it comes to educating voters, said her spokesman, Matt Diehl.

An independent review of the proposed voting system concluded there is a "high risk of compromise" by outsiders, though state officials say they can fix the problems.

The 16,500 new Diebold, Inc. machines are waiting in Maryland warehouses, said Jim Petit, spokesman for the state board, who added: "As far as the state Board of Elections goes, it's full speed ahead."

State officials rejected the option of waiting until the November 2004 presidential election to use the machines — which was Antonetti's choice — because they didn't want to break in a new system with a higher voter turnout.

Better to work out any bugs with fewer voters in a primary, Petit said.

Federal funds totaling \$22 million will pay most of the cost.

Other county election administrators, however, said yesterday that the job can and must be done despite the short lead time.

"Yes, it will be tight. I think we're all nervous," said Rita Dather, Harford County's election director.

"It will be difficult, hard work, but I don't see any major problems," said Gail Carter, deputy elections administrator in Carroll County.

Jackie McDaniel, Baltimore County's elections administrator, said "it's a short amount of time, but I feel confident we can do it." She did acknowledge, though, "this is cutting it close."

Guy Harriman, chairman of Howard's election board, also disagreed with Antonetti.

"We go with what the state dictates we do," he said, adding that "I personally believe we will have it done."

Mark Radke, director of voter industry for Diebold Election Systems, said the company should have no problem meeting Maryland's deadline.

He pointed to the November elections last year in Georgia, when "we had about the same time period to provide 22,000 machines for the entire state."

Kimbell Brace, president of Election Data Services, a Washington elections research firm, said the vital question is how much support and training Diebold — the company supplying the machines — will provide.

"The problem we've always had is that the [election] judges tend to be older individuals who are less inclined electronically. Training is the most critical thing," he said.

The machines were used last year in four counties. Montgomery County experienced problems in the September primary that year — the machines' debut — that delayed vote counts until 2 a.m. Baltimore has a separate electronic system.

Still, Margaret Jurgensen, Montgomery County elections director, said there is enough time now to change the rest of the state, using what was learned from the first counties to make the conversion.

"The state [election board] learned quite a bit working with the various-sized jurisdictions — the timeline and how important teamwork is. I believe that everyone is building toward success," she said.

Robin Downs, Prince George's County elections administrator and president of the Maryland Association of Election Officials, said:

"Of course there is going to be a learning curve. We've done it before. We're professionals. Not to say it is not going to be horrendous, because it usually is."

But Antonetti has serious doubts.

"There are 161 days before the primary," Antonetti said. Subtracting weekends, holidays and the 10 days before the election — when everything must be certified as ready — "there are only 109 working days. It's a pretty close call. When you have to rush things, it opens the door to possible errors," he said.

Overseas absentee ballots must be ready, and election judge training must begin by the end of January, he said. "I don't want to be an alarmist, but I don't feel very comfortable."

Others are muting their fears, he said.

Sun staff writer David Nitkin contributed to this article.

www.sunspot.net/news/local/howard/bal-ho.elect26sep26,0,4741774.story?coll=bal-1

Analysis: A Better Ballot?

Mary Wiltenburg | Christian Science Monitor | November 3, 2003

"A growing number of computer scientists are now warning that [electronic voting], far from solving America's voting problems, may actually make things worse. 'If you look at the consequences for democracy, it's terrifying,' says David Dill, a Stanford University computer-science professor."

When voters head to the polls Tuesday, those using punch-card ballots — notorious for their role in the 2000 presidential election recount — may do so with a lingering unease that their votes could go uncounted. Others will enter sleek new electronic voting booths bought at great price by a patchwork of states and counties trying to guard against butterfly ballots and hanging chads.

But a growing number of computer scientists are now warning that the new technology, far from solving America's voting problems, may actually make things worse. Electronic ballots can be miscounted too, they say — or the machines that tally them tampered with and traces of sabotage erased.

"If you look at the consequences for democracy, it's terrifying," says David Dill, a Stanford University computer-science professor who has led the charge to raise awareness about the machines' potential security flaws. "If we had a way to make [computerized voting] safe, believe me, we would. There's no way to run a reliable election without a verifiable paper trail — that's what these machines don't have."

Others, including makers of the electronic systems and politicians who tout them, argue that democracy always has been a messy process and that no technology is foolproof. As long as there's been a vote, they say, there have been ballots destroyed, misread, and counterfeited; machines worn out or sabotaged; officials bribed; voters bullied or denied their rights. Some disabled citizens have been unable to vote privately, illiterates have been unable to vote knowingly, and voters with limited English have not understood how to cast ballots that count. Electronic voting is the latest in a long line of imperfect solutions, its proponents say, but it's the best option there is.

Voting was a matter of assessing shouts and shows of hands back in Colonial days. In the 1770s, these unverifiable counts were replaced by ballots written longhand, which left a paper trail but took a long time to tally. In 1892, self-tallying lever machines sped up the process, but again left no paper record. When punch-card ballots hit the scene in the 1960s, jurisdictions began to replace the old lever machines. But the punch-card system had its own weaknesses. Even before the 2000 Florida fiasco, some states had switched to the mark-sense or optical-scan ballots, which are much like fill-in-the-bubble standardized tests.

After the recount debacle, officials scrambled to ensure that no future chads would be left hanging. Congress passed the Help America Vote Act of 2002 (HAVA), but has so far supplied only \$664.5 million to fund it. So solutions have come in fits and starts, with counties adopting a hodgepodge of systems ([see map](#)). Last November, Georgia became the first state to install touch-screen machines at all its polling stations, under a \$54 million contract with Diebold Election Systems, a supplier of Direct Recording Electronic voting systems (DREs).

Many Georgia voters were impressed. Kim Hullett, who used a new model in Fayette County's latest election, says the machines — which work much like automatic teller machines — were easy to understand, kept lines moving, and meant she and her husband could track election results on the Web as they heard about them on the TV news.

But Professor Dill, at Stanford, had doubts. A concerned activist had sent him a copy of the Diebold system's source code — the road map to its computer voting software — which the company had been storing on a publicly accessible server. Diebold says this code was partial and outdated. Dill gave the code to a team of computer security experts led by Avi Rubin, technical director of the Information Security Institute at Johns Hopkins University.

The team's [report](#), released in July, marked the first time any company's voting-system software has been publicly evaluated by an academic team. Over 24 pages, it details what Dr. Rubin describes as system-security flaws the average teenager today would be computer-savvy enough to exploit.

Two big flaws, Rubin says, could give rise to any number of nightmare scenarios. The first: The machines' software is encrypted in only the most basic ways, so people with access to a machine before Election Day could easily get into it and, for instance, change the program so that all votes for one candidate go to an opponent. The second: Diebold machines, like comparable machines sold by Sequoia Voting Systems and Election Systems & Software, produce no paper record of a vote, making recounts impossible. A computer science professor, Rubin says he's all in favor of computerizing needless paperwork — but sometimes, in the interest of democracy, you need to kill a few trees.

Diebold rebutted the team's report, arguing it failed to take into account all the checks and balances that ensure election security. Rubin's team argued back that poll workers cannot be expected to make up for security flaws in election machines.

Caught in the crossfire, Maryland put on hold a \$55.6 million contract with Diebold to outfit the entire state, and asked Scientific Applications International Corp., an independent research firm, to investigate. Though the firm's report cautiously confirmed some of the Rubin team's findings, it said many flaws could be corrected, and Maryland decided to go ahead with the purchase. Last month, two lawmakers requested a further review of the matter by an independent state agency.

Meanwhile, states are in limbo — awaiting word on the security of DRE machines before spending more on them, as well as late-arriving HAVA funding. The 2002 act mandates numerous state and county reforms, such as establishing reliable voter rolls (many African-Americans were mistakenly cut from Florida's 2000

eligible-voter lists, and in Denver last month, nearly 200 deceased voters were invited to cast absentee ballots).

The law does not require states to install electronic systems, but the technology holds appeal because of its flexibility, says Roy Saltman, a private election-technology consultant. DREs can give instructions in many languages, and can be adapted for visually impaired voters. HAVA requires that all new systems and safeguards be in place by January 2006, a deadline many states expect to miss.

Critics and some proponents of DREs agree on one thing: the need for a paper audit trail so votes can be recounted. A [bill](#) now before Congress would add that requirement.

www.csmonitor.com/2003/1103/p11s02-uspo.html

The Tyranny of Copyright?

Robert S. Boynton | New York Times | January 25, 2004

"The question of whether the students were within their rights to post the [politically embarrassing] memos was essentially moot: thanks to the Digital Millennium Copyright Act, their speech could be silenced without the benefit of actual lawsuits, public hearings, judges or other niceties of due process."

Last fall, a group of civic-minded students at Swarthmore College received a sobering lesson in the future of political protest. They had come into possession of some 15,000 e-mail messages and memos — presumably leaked or stolen — from Diebold Election Systems, the largest maker of electronic voting machines in the country. The memos featured Diebold employees' candid discussion of flaws in the company's software and warnings that the computer network was poorly protected from hackers. In light of the chaotic 2000 presidential election, the Swarthmore students decided that this information shouldn't be kept from the public. Like aspiring Daniel Ellsbergs with their would-be Pentagon Papers, they posted the files on the Internet, declaring the act a form of electronic whistleblowing.

Unfortunately for the students, their actions ran afoul of the 1998 Digital Millennium Copyright Act (D.M.C.A.), one of several recent laws that regulate intellectual property and are quietly reshaping the culture. Designed to protect copyrighted material on the Web, the act makes it possible for an Internet service provider to be liable for the material posted by its users — an extraordinary burden that providers of phone service, by contrast, do not share. Under the law, if an aggrieved party (Diebold, say) threatens to sue an Internet service provider over the content of a subscriber's Web site, the provider can avoid liability simply by removing the offending material. Since the mere threat of a lawsuit is usually enough to scare most providers into submission, the law effectively gives private parties veto power over much of the information published online — as the Swarthmore students would soon learn.

Not long after the students posted the memos, Diebold sent letters to Swarthmore charging the students with copyright infringement and demanding that the material be removed from the students' Web page, which was hosted on the college's server. Swarthmore complied. The question of whether the students were within their rights to post the memos was essentially moot: thanks to the Digital Millennium Copyright Act, their speech could be silenced without the benefit of actual lawsuits, public hearings, judges or other niceties of due process.

After persistent challenges by the students — and a considerable amount of negative publicity for Diebold — in November the company agreed not to sue. To the delight of the students' supporters, the memos are now back on their Web site. But to proponents of free speech on the Internet, the story remains a chilling one.

Siva Vaidhyanathan, a media scholar at New York University, calls anecdotes like this "copyright horror stories," and there have been a growing number of them over the past few years. Once a dry and seemingly mechanical area of the

American legal system, intellectual property law can now be found at the center of major disputes in the arts, sciences and — as in the Diebold case — politics. Recent cases have involved everything from attempts to force the Girl Scouts to pay royalties for singing songs around campfires to the infringement suit brought by the estate of Margaret Mitchell against the publishers of Alice Randall's book "The Wind Done Gone" (which tells the story of Mitchell's "Gone With the Wind" from a slave's perspective) to corporations like Celera Genomics filing for patents for human genes. The most publicized development came in September, when the Recording Industry Association of America began suing music downloaders for copyright infringement, reaching out-of-court settlements for thousands of dollars with defendants as young as 12. And in November, a group of independent film producers went to court to fight a ban, imposed this year by the Motion Picture Association of America, on sending DVD's to those who vote for annual film awards.

Not long ago, the Internet's ability to provide instant, inexpensive and perfect copies of text, sound and images was heralded with the phrase "information wants to be free." Yet the implications of this freedom have frightened some creators — particularly those in the recording, publishing and movie industries — who argue that the greater ease of copying and distribution increases the need for more stringent intellectual property laws. The movie and music industries have succeeded in lobbying lawmakers to allow them to tighten their grips on their creations by lengthening copyright terms. The law has also extended the scope of copyright protection, creating what critics have called a "paracopyright," which prohibits not only duplicating protected material but in some cases even gaining access to it in the first place. In addition to the Digital Millennium Copyright Act, the most significant piece of new legislation is the 1998 Copyright Term Extension Act, which added 20 years of protection to past and present copyrighted works and was upheld by the Supreme Court a year ago. In less than a decade, the much-ballyhooed liberating potential of the Internet seems to

have given way to something of an intellectual land grab, presided over by legislators and lawyers for the media industries.

In response to these developments, a protest movement is forming, made up of lawyers, scholars and activists who fear that bolstering copyright protection in the name of foiling "piracy" will have disastrous consequences for society — hindering the ability to experiment and create and eroding our democratic freedoms. This group of reformers, which Lawrence Lessig, a professor at Stanford Law School, calls the "free culture movement," might also be thought of as the "Copy Left" (to borrow a term originally used by software programmers to signal that their product bore fewer than the usual amount of copyright restrictions). Lawyers and professors at the nation's top universities and law schools, the members of the Copy Left aren't wild-eyed radicals opposed to the use of copyright, though they do object fiercely to the way copyright has been distorted by recent legislation and manipulated by companies like Diebold. Nor do they share a coherent political ideology. What they do share is a fear that the United States is becoming less free and ultimately less creative. While the American copyright system was designed to encourage innovation, it is now, they contend, being used to squelch it. They see themselves as fighting for a traditional understanding of intellectual property in the face of a radical effort to turn copyright law into a tool for hoarding ideas. "The notion that intellectual property rights should never expire, and works never enter the public domain — this is the truly fanatical and unconstitutional position," says Jonathan Zittrain, a co-founder of the Berkman Center for Internet and Society at Harvard Law School, the intellectual hub of the Copy Left.

Thinkers like Lessig and Zittrain promote a vision of a world in which copyright law gives individual creators the exclusive right to profit from their intellectual property for a brief, limited period — thus providing an incentive to create while still allowing successive generations of creators to draw freely on earlier ideas. They stress that borrowing and collaboration are essential components of all

creation and caution against being seduced by the romantic myth of "the author": the lone garret-dwelling poet, creating masterpieces out of thin air. "No one writes from nothing," says Yochai Benkler, a professor at Yale Law School. "We all take the world as it is and use it, remix it."

Where does the Copy Left believe a creation ought to go once its copyright has lapsed? Into the public domain, or the "cultural commons" — a shared stockpile of ideas where the majority of America's music and literature would reside, from which anyone could partake without having to pay or ask permission. James Boyle, a professor at Duke Law School, notes that the public domain is a necessity for social and cultural progress, not some sort of socialist luxury. "Our art, our culture, our science depend on this public domain," he has written, "every bit as much as they depend on intellectual property."

In opposition to the cultural commons stands the "permission culture," an epithet the Copy Left uses to describe the world it fears our current copyright law is creating. Whereas you used to own the CD or book you purchased, in the permission culture it is more likely that you'll lease (or "license") a song, video or e-book, and even then only under restrictive conditions: read your e-book, but don't copy and paste any selections; listen to music on your MP3 player, but don't burn it onto a CD or transfer it to your stereo. The Copy Left sees innovations like iTunes, Apple's popular online music store, as the first step toward a society in which much of the cultural activity that we currently take for granted — reading an encyclopedia in the public library, selling a geometry textbook to a friend, copying a song for a sibling — will be rerouted through a system of micropayments in return for which the rights to ever smaller pieces of our culture are doled out. "Sooner or later," predicts Miriam Nisbet, the legislative counsel for the American Library Association, "you'll get to the point where you say, 'Well, I guess that 25 cents isn't too much to pay for this sentence,' and then there's no hope and no going back."

There is a growing sense of urgency among the members of the Copy Left. They worry that if they do not raise awareness of what is happening to copyright law, Americans will be stuck forever with the consequences of decisions now being made — and laws being passed — in the name of preventing piracy. "We are at a moment in our history at which the terms of freedom and justice are up for grabs," Benkler says. He notes that each major innovation in the history of communications — the printing press, radio, telephone — was followed by a brief period of openness before the rules of its usage were determined and alternatives eliminated. "The Internet," he says, "is in that space right now."

America has always had an ambivalent attitude toward the notion of intellectual property. Thomas Jefferson, for one, considered copyright a necessary evil: he favored providing just enough incentive to create, nothing more, and thereafter allowing ideas to flow freely as nature intended. "If nature has made any one thing less susceptible than all others of exclusive property," he wrote, "it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of everyone." His conception of copyright was enshrined in Article 1, Section 8 of the Constitution, which gives Congress the authority to "promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."

But Jefferson's vision has not fared well. As the country's economy developed from agrarian to industrial to "information," ideas took on greater importance, and the demand increased for stronger copyright laws. In 1790, copyright protection lasted for 14 years and could be renewed just once before the work entered the public domain. Between 1831 and 1909, the maximum term was increased from 28 to 56 years. Today, copyright protection for individuals lasts for 70 years after the death of the author; for corporations, it's 95 years after publication. Over the past three decades, the flow of material entering the public domain has slowed to

a trickle: in 1973, according to Lessig, more than 85 percent of copyright owners chose not to renew their copyrights, allowing their ideas to become common coin; since the 1998 Copyright Term Extension Act lengthened present and past copyrights for an additional 20 years, little material will enter the public domain any time soon.

Some of the changes that expanded copyright protection were made with an understanding of their effects; what also troubles the Copy Left, however, are the unintended consequences of seemingly innocuous tweaks in copyright legislation. In particular, two laws that were passed years before the creation of the Internet helped set the stage for today's copyright bonanza. Before the 1909 Copyright Act, copyright was construed as the exclusive right to "publish" a creation; but the 1909 law changed the wording to prohibit others from "copying" one's creation — a seemingly minor change that thereafter linked copyright protection to the copying technology of the day, whether that was the pen, the photocopy machine, the VCR or the Internet. In 1976, a revision to the law dispensed with the requirement of formally registering or renewing a copyright in order to comply with international copyright standards. Henceforth, everything — from e-mail messages to doodles on a napkin — was automatically copyrighted the moment it was "fixed in a tangible medium."

The true significance of these two laws didn't become apparent until the arrival of the Internet, when every work became automatically protected by copyright and every use of a work via the Internet constituted a new copy. "Nobody realized that eliminating those requirements would create a nightmare of uncertainty and confusion about what content is available to use," Lessig explains, "which is a crucial question now that the Internet is the way we gain access to so much content. It was a kind of oil spill in the free culture."

Lessig is one of the most prominent and eloquent defenders of the Copy Left's belief that copyright law should return to its Jeffersonian roots. "We are invoking

ideas that should be central to the American tradition, such as that a free society is richer than a control society," he says. "But in the cultural sphere, big media wants to build a new Soviet empire where you need permission from the central party to do anything." He complains that Americans have been reduced to "an Oliver Twist-like position," in which they have to ask, "Please, sir, may I?" every time we want to use something under copyright — and then only if we are fortunate enough to have the assistance of a high-priced lawyer.

In October 2002, Lessig argued before the Supreme Court in *Eldred v. Ashcroft*, which concerned a challenge to the Copyright Term Extension Act. On behalf of the plaintiffs, Lessig argued that perpetually extending the term of copyright was a violation of the Constitution's requirement that copyright exist for "a limited time." The court responded that although perhaps unwise on policy grounds, granting such extensions was within Congress's power. It was a major setback for the Copy Left. Given the *Eldred* decision, there is nothing to stop a future Congress from extending copyright's term again and again.

Lessig's efforts haven't been limited to the courtroom. In 2001, he was part of a group that founded an organization called Creative Commons, which offers individual creators the ability to carefully calibrate the level of control they wish to maintain over their works. The organization services the needs of, say, musicians who want rappers and D.J.'s to be able to download and remix their music without legal trouble or of writers who want their works republished without charge, but only by nonprofit publications. The Commons has developed a software application for the Web that allows copyright holders who do not want to exercise all of the restrictions of copyright law to dedicate their work to the public domain or license it on terms that allow copying and creative reuses. The aim of Creative Commons is not only to increase the sum of raw source material online but also to make it cheaper and easier for other creators to locate and access that material. This will enable people to use the Internet to find, for example, photographs that are free to be altered or reused or texts that may be copied,

distributed or sampled — all by their authors' permission. The Creative Commons now has a presence in 10 countries, including Brazil, whose minister of culture, the musician Gilberto Gil, plans to release some of his songs under the Creative Commons license so that others may freely borrow from them. Creative Commons is currently talking to Amazon and others about a plan to release out-of-print books under Creative Commons licenses.

One of the central ideas of the Copy Left is that the Internet has been a catalyst for re-engaging with the culture — for interacting with the things we read and watch and listen to, as opposed to just sitting back and absorbing them. This vision of how culture works stands in contrast to what the Copy Left calls the "broadcast model" — the arrangement in which a small group of content producers disseminate their creations (television, movies, music) through controlled routes (cable, theaters, radio-TV stations) to passive consumers. Yochai Benkler, the law professor at Yale, argues that people want to be more engaged in their culture, despite the broadcast technology, like television, that he says has narcotized us. "People are users," he says. "They are producers, storytellers, consumers, interactors — complex, varied beings, not just people who go to the store, buy a packaged good off the shelf and consume."

A few weeks ago, I met Benkler in his loft in downtown New York. He stroked his beard while explicating his ideas with the care of a man parsing a particularly knotty question of Scripture. Benkler was born in Tel Aviv in 1964, and while in his 20's, he helped found a remote desert kibbutz in an attempt to recapture the Zionist movement's original socialist spirit. The challenges of creating a community in isolation from the rest of society ultimately proved overwhelming. "After a few years," he said, "we realized that at the rate we were going we wouldn't attend college until we were in our 50's." It was a hard lesson in the difficulty of producing anything — a community, a work of art — in isolation.

But Benkler's belief in the importance of creating things in common rests on more than anecdotal evidence. What makes his argument more than wishful thinking, he said, is that he has some economic evidence for his view. "Let's compare a few numbers," he said. "How much do people pay the recording industry to listen to music versus how much people pay the telephone industry to talk to their friends and family? The recording industry is a \$12 billion a year business, compared with the telephone business, which is a more than \$250 billion a year business. That is what economists call a 'revealed willingness to pay,' a clear preference for a technology that allows you to participate in work, socializing and interaction in general, over a technology that allows you to be a passive consumer of a packaged good. Is that a study of human nature? No. Is it an economic measure that would suggest there is a lot of demand out there for speaking and listening to others? Yes."

According to Benkler, the cultural commons not only offers a better model for creativity; it makes good economic sense. Like Lessig and other members of the Copy Left, he takes his bearings from the free software movement and views the success of products like Linux and services like Google as evidence of a viable collaborative (or "peer to peer") model for producing and sharing ideas — a model that will augment and, in some cases, replace the current model. (He concedes that some products, like novels and blockbuster movies, will never be produced peer to peer, though they will draw on the work of artists before them.)

Benkler predicts that the recording industry will be one of the first businesses to go. "All it does is package and sell goods," he said, "which is technically an unfeasible way of continuing. They are trying their best to legislate the environment to change, but that doesn't mean we have to let them."

The battle between the Copy Left and its opponents is as much a clash of worldviews as of legal doctrine. Aligned against the Copy Left are those who sympathize with the romantic notion of authorship and view the culture as a

market in which everything of value should be owned by someone or other. Jane Ginsburg, a professor at Columbia Law School who specializes in copyright law, fears that in the Copy Left's rush to secure the public domain, it gives short shrift to the author. A self-described "copyright enthusiast," Ginsburg considers the author the moral center of copyright law and questions equating copyright control with corporate greed. "Copyright cannot be understood merely as a grudgingly tolerated way station on the road to the public domain," she writes in a recent article titled "The Concept of Authorship in Comparative Copyright Law." "Because copyright arises out of the act of creating a work, authors have moral claims that neither corporate intermediaries nor consumer end-users can (straightfacedly) assert."

Ginsburg and others embrace many elements of the "permission society" demonized by the Copy Left and cite developments like the iTunes store as a sign of greater consumer choice and freedom. In his book "Copyright's Highway," Paul Goldstein, a professor at Stanford Law School, writes that "the logic of property rights dictates their extension into every corner in which people derive enjoyment and value from literary and artistic works." He characterizes the permission society as a "celestial jukebox" in which access to every creation — music, literature, movies, art — is available to anyone for a price.

An entire "digital rights management" industry has arisen to bring this vision to fruition, each company calibrating a particular license through a system of micropayments — play a song on your computer for one price; transfer it to your MP3 player for a slightly higher fee. Goldstein argues that the scheme of a business like iTunes is actually more efficient and democratic than the commons model championed by the Copy Left. "The problem with the commons is that it doesn't take into consideration the direction of the payment; it doesn't reveal what kind of culture gets used and what kind doesn't," he says. "I think it is good to have a price tag attached to each use because it tells producers what

consumers want; it lets them vote with their purchase for the kinds of culture they want."

But the Copy Left is convinced that there is a better way for the entertainment industry to adapt to the Internet age while still paying its artists their due. William Fisher, director of the Berkman Center, has spent the last three years devising an alternative compensation system that would enable the entertainment industry to restructure its business model without resorting to cumbersome micropayments. He has worked out a modified version of the system that artists' advocacy groups currently use to make sure that composers are paid when their music is performed or recorded. According to Fisher's plan, all works capable of being transmitted online would be registered with a central office (whether government or independent is unclear). The central office would then monitor how frequently a work is used and compensate the creators on that basis. The money would come from a tax on various content-related devices, like DVD burners, blank CD's or digital recorders. It is a brave proposal in a political culture that is allergic to taxes and uncomfortable with complex solutions. Still, if his numbers do indeed add up, Fisher's proposal might be the best thing that ever happened to the cultural commons: the creators would be paid, while every individual would have unlimited access to every cultural creation.

Fisher and Charles Nesson, his colleague at Harvard Law School, have showed this proposal to movie executives and lawyers for several media conglomerates. Fisher says that his ideas have been received with great interest by the very industries — music, home video — that see their business models disintegrating before their eyes.

When asked whether he thinks his ambitious scheme has a chance, Fisher says that the likeliest possibility would be for it to be adopted in countries that are neither so developed that they have signed on to international copyright protocols nor so undeveloped that they are desperate to do so. Only second-world

countries, like Croatia or Brazil, he speculates, are unfettered enough to try something new. "The hope is in the rain forest," he says, in countries that "are more like the United States was before 1890, when we were a 'pirate' nation."

And in the United States, is there any future for this sort of payment system? Perhaps when the various current schemes fail, Fisher's plan will seem more attractive, he says. "What is involved here is nothing less than the shape of our culture and the way we think of ourselves as citizens," he adds. He describes a recent letter he received from a supporter of his work. "When they come for my guns and my music, they'd better bring an army," it read. "People are used to being creatively engaged with the culture," Fisher explains. "They won't let someone legislate that away."

The future of the Copy Left's efforts is still an open question. James Boyle has likened the movement's efforts to establish a cultural commons to those of the environmental movement in its infancy. Like Rachel Carson in the years before Earth Day, the Copy Left today is trying to raise awareness of the intellectual "land" to which they believe we ought to feel entitled and to propose policies and laws that will preserve it. Just as the idea of environmentalism became viable in the wake of the last century's advances in industrial production, the growth of this century's information technologies, Boyle argues, will force the country to address the erosion of the cultural commons. "The environmentalists helped us to see the world differently," he writes, "to see that there was such a thing as 'the environment' rather than just my pond, your forest, his canal. We need to do the same thing in the information environment. We have to 'invent' the public domain before we can save it."

www.nytimes.com/2004/01/25/magazine/25COPYRIGHT.html

Will the Election Be Hacked?

[Farhad Manjoo](#) | [Salon](#) | [February 9, 2004](#)

"If there's an upset in a close presidential race, will we be able to trust it? Ironically, the paperless systems were supposed to restore trust in a democracy that saw the presidency hang by a few thousand chads in Florida three years ago. In Georgia, and increasingly across the nation, they're in danger of doing quite the opposite."

A few weeks after Election Night 2002, Roxanne Jekot, a computer programmer who lives in Cumming, Ga., began fearing demons lingering in the state's voting machines. The midterm election had been a historic one: Georgia became the first state to use electronic touch-screen voting machines in every one of its precincts. The 51-year-old Jekot, who has a grandmotherly bearing but describes herself as a "typical computer geek," was initially excited about the new system.

"I thought it was the coolest thing we could have done," she says.

But the election also brought sweeping victories for Republicans, including, most stunningly, one for Sonny Perdue, who defeated Roy Barnes, the incumbent Democrat, to become Georgia's first Republican governor in 135 years, while Rep. Saxby Chambliss upset Vietnam veteran Sen. Max Cleland. The convergence of these two developments — the introduction of new voting machines and the surprising GOP wins — began to eat away at Roxanne Jekot. Like many of her fellow angry Democrats on the Internet discussion forums she frequented, she had a hard time believing the Republicans won legitimately. Instead, Jekot began searching for her explanation in the source code used in the new voting machines.

What she found alarmed her. The machines were state-of-the-art products from an Ohio company called Diebold. But the code — which a friend of Jekot's had found on the Internet — was anything but flawless, Jekot says. It was amateurish and pocked with security problems. "I expected sophistication and some fairly difficult to understand advanced coding," Jekot said one evening this fall at a restaurant near her home. But she saw "a hodgepodge of commands thrown all over the source code," an indication, she said, that the programmers were careless. Along with technical commands, Diebold's engineers had written

English comments documenting the various functions their software performed — and these comments "made my hair stand on end," Jekot said. The programmers would say things like "this doesn't work because that doesn't work and neither one of them work together." They seemed to know that their software was flawed.

To Jekot, there appeared to be method in the incompetence. Professional programmers could not be so sloppy; it had to be deliberate. "They specifically opened doors that need not be opened," Jekot said, suggesting the possibility that Diebold *wanted* to leave its voting machines open to fraud. And, ominously, the electronic voting systems used in Georgia, like most of the new machines installed in the United States since the 2000 election, do not produce a "[paper trail](#)" — every vote cast in the state's midterm election was recorded, tabulated, checked and stored by computers whose internal workings are owned by Diebold, a private corporation.

Jekot was particularly alarmed — and outraged — to learn that company CEO Walden O'Dell is one of the GOP's biggest fundraisers in his home state of Ohio and nationally. Right after the Georgia elections, an O'Dell e-mail began making the rounds of Web logs and other Internet sites that were tracking the Diebold security flaws, [in which the CEO bragged](#) that he's "committed to helping Ohio deliver its electoral votes to the president next year." What better way to deliver electoral votes for President Bush, some reasoned, than to control the equipment Americans use to cast their ballots?

"I believe that the 2002 election in Georgia was rigged," Jekot insists today. "I don't believe that Saxby Chambliss or Sonny Perdue won their races legally."

Despite Jekot's technical expertise, officials in Georgia consider her theories baseless. Roy Barnes, the defeated Democratic governor, says that blaming his loss on voting machines is "ridiculous." And, to be sure, there is no evidence proving malfeasance, and there probably never will be. The only trouble is, the

state cannot furnish any definitive evidence to show that the 2002 election *was not* fraudulent. Proving that the machines didn't malfunction, or that they weren't hacked, is impossible. And since scores of computer scientists say that voting systems are vulnerable to attack, and because activists have raised legitimate concerns about election equipment vendors' politics and processes, Jekot's fears have come to seem, to many, entirely reasonable.

Even a self-described Christian arch-conservative, former Diebold systems manager Rob Behler, says the company failed to adequately test its troubled equipment — and balked when he warned them of widespread problems with the machines. Last summer, computer scientists at Johns Hopkins University and Rice University found [major security flaws](#) in the Diebold machines, concluding that the Georgia system falls "far below even the most minimal security standards." And in January, experts at RABA Technologies, a consulting firm in Maryland, discovered [additional failures](#) [pdf] in that state's Diebold systems. Internal Diebold e-mail shows that company engineers knew about the problems and in some instances chose to ignore them.

Some elections officials are beginning to see the profound dangers inherent in this process; California Secretary of State Kevin Shelley has ordered that all systems in his state implement a paper record by 2006. Activists hailed Shelley's decision as evidence that he understands the fundamental principle at stake: Elections should be sacrosanct.

But on Election Day this November, more than 20 percent of American voters will cast their ballots on paperless electronic machines; voters across the nation will encounter them during the primaries. Critics of touch-screen systems point to the controversy surrounding the vote in Georgia as a sign of things to come nationally. If there's an upset in a close presidential race, will we be able to trust it? Ironically, the paperless systems were supposed to restore trust in a democracy that saw the presidency hang by a few thousand chads in Florida

three years ago. In Georgia, and increasingly across the nation, they're in danger of doing quite the opposite.

Many in Georgia dismiss Jekot and her Web-based acolytes as blinded partisans, conspiracy nuts, or even "wack-jobs."

But if you dismiss Roxanne Jekot as a wack-job, you still have to deal with her friends. Jekot represents only the most strident quarter of an emerging national movement aimed at slowing the spread of the kind of touch-screen systems that were first used in Georgia. While the movement counts as members some of the most shrill partisans on the Web, it also includes some of the most well-regarded computer scientists in the world — and together, these groups have been unexpectedly successful in changing the national perceptions of touch-screen machines.

Until just about a year ago, these systems were considered the natural replacement to the punch-card machines that so roiled the last presidential election. The new machines are easy to maintain, they can accommodate multiple languages, they can be used by people with disabilities, and they have the backing of influential groups like the League of Women Voters and the ACLU. The Help America Vote Act of 2002, which doles out a total of \$650 million in federal money to state and local officials who upgrade their aging voting systems, has already prompted dozens of counties and a handful of states to deploy the touch-screen systems.

The activists have upended the process. Fear of the voting machines is now a red-meat issue not just for online lefties but also for libertarians, for many on the right, and, increasingly, for the establishment. National newspapers run Op-Eds on the issue, network news shows feature the movement's proponents, and officials like Shelley, in California, have been pressed to change their positions on the systems.

If you spend much time in the world of the activists, you'll understand why. In the fall, I sat with [Jim March](#), an anti-Diebold tech expert in Sacramento, Calif., while he showed me on his home PC how to steal an election. March, an ardent libertarian whose apartment is decorated with political posters — "Politicians Prefer an Unarmed Populace," one announces — spent months investigating security flaws in touch-screen systems. Thanks to his network of fellow geek-activists, he'd found flaws in the system Diebold used to tally election results, a program called GEMS. The GEMS software runs on a standard PC that's usually housed in a county election office. The system stores its votes in a format recognizable by Microsoft Access, a common office database program. If you've got a copy of Access and can get physical access to the county machine — or, some activists say, if you discover the county's number and call into the machine over a phone line — the vote is yours to steal.

While I sat at his computer, March helped me open a file containing actual results from a March 2002 primary election held in San Luis Obispo County, Calif. — a file that March says would be accessible to anyone who worked in the county elections office on Election Day. Following March's direction, I changed the vote count with a few clicks. Then, he explained how to alter the "audit log," erasing all evidence that we'd tampered with the results. I saved the file. If it had been a real election, I would have been carrying out an electronic coup. It was a chilling realization.

The person who discovered the problems with the GEMS program — she's singularly responsible for almost every bit of attention recently paid to electronic voting machines, and for almost every juicy detail uncovered about the vote in Georgia — is a middle-aged publicist-turned-[investigative-journalist](#) in Seattle named [Bev Harris](#). Harris began thinking about voting machines in late 2002, when, after reading some claims on the Web that the election equipment firms were being infiltrated by foreign nationals, she decided, almost on a lark, to investigate the matter.

Harris had no journalistic experience, but she'd always harbored fantasies of uncovering something big. She turned out to be exceptionally talented at reporting. Within a few weeks of her investigation, she'd dug up many compelling nuggets. She found, for instance, that in the early 1990s, before he was elected to office, Sen. Chuck Hagel, the Nebraska Republican, served as the president of American Information Systems, the company that built most of the voting machines used in his state. Harris also discovered that Diebold, the firm that produced the machines used in Georgia, had left the software used to run its systems on a public server online. Harris downloaded these files and looked through them. She saw that she had the company's source code as well as several other curiously named files — one, for example, was called "rob-georgia.zip."

Before Bev Harris found the files used in Georgia, the software in the machines had essentially been secret. Although the code had been reviewed by government testing authorities, nobody outside those labs had been allowed to see the programs, which is a standard provision in most electronic voting systems. When the computing public got a peek at the files Harris found, experts were not kind.

In July, a team of four computer scientists at Johns Hopkins University and Rice University announced that they'd [uncovered major security flaws](#) in the machines used in Georgia's elections. "Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts," the team wrote. Diebold has long boasted that votes in its system are stored in an encrypted manner, hidden to anyone who didn't have a valid password; the computer scientists found that Diebold's programmers left the "key" to decrypt the votes written into the code, which is a bit like locking your door and placing the key *on* the welcome mat. The Hopkins/Rice scientists also said that they saw no adequate mechanism to prevent voters from casting multiple ballots, viewing partial election results, or terminating an election early.

On Jan. 19, a team of computer scientists working with RABA Technologies set up a red-team exercise — a one-day attempt to hack into Diebold machines configured as they would be on Election Day. [They were successful](#). In a short time, the hackers managed to guess the passwords securing the voting system, allowing them to cast multiple ballots. They found that with a standard lock-pick set, they could inconspicuously open up each machine — sometimes in less than 10 seconds — and remove or attach various pieces of hardware, letting them erase or change electronic ballots. They concluded that Diebold's touch-screen machines contain "considerable security risks," and they suggested that Maryland put in place stringent safeguards before its March 2 primary, and that the state overhaul the system before the presidential election.

Diebold fiercely disputes that its technology is vulnerable to attacks. Mark Radke, a spokesman for Diebold, says that the RABA study pointed out some areas in which Maryland could improve its voting procedures, and he's pleased that Maryland is instituting those changes. As for the Hopkins study, Radke says the scientists who looked at the system erred in their assessment by examining only a small bit of the code and by neglecting the "checks and balances" that occur in an actual election. He pointed to a study of the company's system that was performed by Science Applications International Corp., a consulting firm, at the behest of the state of Maryland. The SAIC report gives Diebold a clean bill of health, and Georgia officials say it proves their system is safe. (The study is available [here](#) in PDF format.)

There is no evidence that someone tampered with the votes in Georgia. But certainly it is not beyond the bounds of possibility that someone could do so in the future. The history of American democracy is replete with allegations of vote fixing and stolen elections — from Rutherford Hayes' disputed victory over Samuel Tilden in 1876 to Illinois in 1960 (there were vote fraud allegations against both Richard Nixon and John F. Kennedy) to the Florida debacle in 2000. Leaving the security of such a crucial government function in the hands of private

companies motivated primarily by a desire to make a quick buck seems like a loopy idea to many people. And the more one listens to the activists' complaints about how Diebold does business, the more one comes to understand their worries about election security.

Bev Harris says that in August, a former employee at Diebold handed her a trove of documents from the company, representing years of discussions on an internal company Web site. In [the memos](#), Diebold programmers seem to acknowledge security holes in their system, and they appear to discuss methods of evading testing authorities. In one e-mail, Ken Clark, a programmer at the company, acknowledges that vote data can be viewed with Microsoft Access, but he says that fixing the problem will be difficult, and it would be easier to feel out the testing labs and "find out what it is going to take to make them happy." In another e-mail, Clark recommends to his co-workers that if the state of Maryland — which has also purchased the company's touch-screen machines — decides to require a paper trail in its voting systems, the company should exact a high price for the required upgrades. Diebold should charge Maryland "out the yin," Clark wrote. In yet another e-mail, Clark does an impression of how voters in Georgia might react to touch-screen machines: "Yer votin thingamajig sure looks purdy," he writes. (Calls to Clark were routed to Diebold's P.R. office. While the company concedes that the memos are authentic, it disputes Harris' claim that the files came from a Diebold employee. Instead, says Mark Radke, Diebold's computers were hacked. The firm initially threatened to sue people who posted the files on the Web, but it has [backed off](#) that threat.)

In the spring of 2003, Harris received an e-mail that read, "I think I may be the Rob in rob-georgia." The message was from Rob Behler, a laid-off telecom worker who found a contract job at Diebold's Atlanta warehouse in the summer before the midterm election. Behler, a friendly fellow in his 30s who speaks with a disarming Southern drawl, paints a disastrously unflattering picture of the company that provided his state with its voting equipment. He told Harris that his

time at Diebold was marked by confusion and chaos, a month of 16-hour days in which he did nothing but fix broken machines, broken management techniques, and deal with incompetent people.

On his first day on the job, Behler, who had never worked on election systems before, was promoted to a manager's position and put in charge of the team assembling, testing and deploying all of the voting machines in the state. He says that when he checked the machines that employees had been assembling for months, he discovered that large numbers of them were defective.

During the few weeks that followed, Behler spent his time fixing the machines. He says that each time he discovered a new problem with the systems, he would call up the tech experts at Diebold, and they would determine a way to fix it. The programmers would put a file on the company server — a file like rob-georgia.zip — and Behler would download it to his laptop, store it on a memory card, then install the memory card on the touch-screen machines. The process steered clear of any certification authorities; no independent body was checking to see what was being installed on the system.

Indeed, Behler remembers a conference call with Diebold executives in which they specifically discussed what to tell Georgia authorities if Diebold engineers were caught installing software on the machines. "Can't we just tell them we're updating?" Behler wondered in the meeting. "They're like, 'No, no, no, no, no, you can't do that. It has to be certified.' And I say, 'Oh? So we don't want them to know that we're fixing a problem?' So I was like, 'OK — we can tell them that we're doing a quality check and that we're making sure that they're all the same.' And that's exactly what we did."

Mark Radke of Diebold says, "All I can tell you about these situations is that before the units are deployed they are fully tested, and that final testing was proof-positive about how those units were going to function."

The Georgia secretary of state's office dismisses most of Behler's claims. Chris Riggall, press secretary to Cathy Cox, the secretary of state, says that at some point before the 2002 election, Diebold did discover that Windows CE, the version of the Microsoft Windows operating system that runs on the touch-screen machines, needed to be upgraded. But this was a one-time fix that Cox was fully aware of, he said. This fix was not formally certified by state and federal testing authorities, as Georgia law requires. But Riggall says that the state's testing experts determined that because the upgrade was only to the Windows operating system and not to the other software in the touch-screen machine, it did not need to be certified. The election was fast approaching, Riggall said, and there simply was no time for certification. Doing it this way was "not our preferred best option," he wrote in an e-mail, "but nevertheless justifiable under the circumstances." As for Behler's claim that the software was downloaded from Diebold's publicly accessible server, Riggall says that's not true. "No, we never used that site during any aspect of the 2002 elections."

Behler, who has seven children, is an arch-conservative. One night this fall, standing outside his five-bedroom house in one of Atlanta's affluent northern suburbs, he described his politics in detail — why he favored the ban on late-term abortions, why he considers the minimum wage a foolish idea, why he prefers George W. Bush to Bill Clinton, and why, despite what he knows of working at Diebold, he does not believe that the 2002 election in his state was rigged. For one thing, he doesn't consider the GOP's wins very surprising; to him, the Republicans running that year were fine candidates. But he does believe the Diebold flaws are an open invitation to election mischief.

The transition to touch-screen machines in Georgia was proposed and championed by Democrats, and the state's elected Democrats remain the machines' fiercest defenders. It is an irony of this story, then, that while Roxanne Jekot and her friends claim that Republicans rigged the 2002 election, it is for Democrats — or, for one Democrat in particular, Georgia's secretary of state,

Cathy Cox — that they reserve their contempt. Cox, a former journalist and attorney who was first elected to office in 1998, is the nation's leading proponent of electronic voting systems. After the 2000 election, Cox grasped, long before her peers in other states, that electronic voting would be the future of elections. It was a future that she was determined to bring to her state.

Georgia has 159 counties, more than any state except Texas, and, before the new machines were installed, there were nearly as many different voting systems in use — old-school lever machines (which also produce no paper trail), punch-card machines, and optical scan systems (which use SAT-style fill-in-the-bubble ballots), all of varying makes and models. Shortly after the 2000 election, Cox commissioned a study on the accuracy of these systems, looking at one measure in particular, the presidential-race undervote. (The undervote in a given race is the number of ballots on which voters failed to register any choice for a candidate.) Cox found that the highest undervote rates occurred in neighborhoods where there were large groups of minorities.

In a sample of predominantly black precincts Cox examined, for instance, she found that the undervote was an alarming 8.1 percent. What was mysterious was that optical scan voting systems — which are really the only alternative to touch-screen machines still available for sale — did not seem to greatly improve the undervote rate among minorities. While the undervote rate on optical scan machines in white neighborhoods was just 2.2 percent, in black neighborhoods it was 7.6 percent. The situation in Georgia was so obviously discriminatory that in 2001, the ACLU sued Cox to force her to upgrade the state's elections systems. Cox says that she chose touch-screen systems because, among other attributes, they had the best chance of reducing the undervote. She was right: In the 2002 election, using the new machines, the undervote rate in Georgia was less than 1 percent.

In the online forums where voting-machine critics assert that Republicans fixed the 2002 election in Georgia, it's often said that the results in the state surprised everybody. This isn't exactly the case. The Senate race, which pitted the incumbent Democrat Max Cleland against Saxby Chambliss, a Republican, was widely considered a tossup by Election Day.

The big surprise, perhaps the largest upset anywhere in the country that night, was in the governor's race. Roy Barnes had been all but assured a win. He had everything on his side, including money (Barnes outspent Sonny Perdue by a margin of 6 to 1), history (Georgia is the only state in the nation that did not elect a Republican governor in all of the 20th century) and a commanding lead in the polls.

But when Barnes eventually lost (with 46 percent to Perdue's 51 percent), his campaign did not suspect the voting machines, not even for a second. According to Bobby Kahn, Barnes' chief of staff and an old-time political hand in Georgia, there was an obvious political reason for the defeat — the Confederate flag. In an e-mail, Roy Barnes wrote that "you will see that the dominant factor in my defeat in 2002 was anger over my actions in changing the Georgia flag to reduce the size of the Confederate battle emblem. I knew from my travels around the state that there was a lot of anger over the change — I had believed, or at least hoped, I could overcome the anger, but I couldn't." Voter turnout among white Georgians in 2002 was unexpectedly high, much higher than in the 1998 race.

In his office this fall, Chris Riggall, Cox's press secretary, said that many of the computer scientists who have questioned electronic voting systems have little firsthand experience in elections, and are therefore unqualified to judge a voting system's security. And those who say there was something amiss with the 2002 election don't have a clue about how politics works in Georgia, he said. "When I see the Independent" — the London newspaper — "[saying](#) the only way Max Cleland could have lost was because of the voting machines, I have to laugh.

What in the hell do you know about Georgia political history? The last time he won with [just] 30,000 votes!"

"Our system is not perfect," says Riggall. "Our system is vulnerable, but we believe it's less so than all of the alternatives. So our frustration is the lack of context, perspective and knowledge of what happens in Georgia."

But the movement to challenge electronic voting is not confined to Georgia, or to those who worry about the 2002 election results. David Dill, a computer scientist at Stanford University, has been among the one or two activists [most responsible for the shift](#). Dill says that when he first heard that systems were being installed in Georgia and in some of California's largest counties — including his own, Santa Clara — he initially figured "that somebody was minding the store and making sure that the equipment is somehow trustworthy."

Then he did some research into how the systems were designed and implemented, and "I began to feel that maybe that wasn't true," he says. Dill says that he was particularly annoyed that election officials seemed to ignore the concerns of computer security experts, who've warned of the dangers of electronic voting for decades. So early in 2003, Dill posted a petition online demanding that all computerized voting equipment produce what he called a "voter-verifiable audit trail."

The audit trail (an idea that was first developed by [Rebecca Mercuri](#), a computer scientist who has long studied the voting systems and is now a research fellow studying transparency in computational systems at Harvard's Kennedy School) works as follows: When a voter casts a ballot on a touch-screen machine, she'll be presented with a paper version of her votes to look over. Once she approves this paper ballot, it becomes the official record of her vote (she is not allowed to remove the paper ballot from the voting precinct). If there is a question about the accuracy of the electronic count, election officials would be required to manually count the paper ballots; if there's a discrepancy between the two counts, the

manual count would be considered the official result of the election. Thousands of computer scientists have signed Dill's demand; attaining it nationally has become the paramount goal for the critics of the touch-screen systems.

"It's not just one computer scientist whining about this," Dill says. "It's a lot of very reputable people who are willing to say that as far as they can see this voter-verifiable audit trail idea is the only way you can conceive the necessary level of confidence in the equipment."

Kevin Shelley's decision, in late November, to require a paper trail in California's electronic voting machines was gutsy — and some say precipitous. No paper-equipped touch-screen system has ever been used in a real election in the state, and a few election experts have expressed serious concerns about the viability of such a machine. Ted Selker, a computer scientist at MIT who has studied election procedures, fears that the paper trail would be prone to accidents and attacks: Paper ballots are tricky to count accurately by machine, are almost impossible and time-consuming to count by hand, and, of course, they can easily be tampered with. It's not clear how the paper ballots would be made accessible to the blind, either, and nobody knows how much upgrading to the paper system would cost. Selker, who worked on a landmark study of the 2000 election, says that millions of votes each year are lost because of faulty registration databases, flawed ballot design, and poorly trained poll workers. Spending money on a paper trail rather than to fix these known problems, he says, is a waste.

Officials in Shelley's office acknowledge the concerns with paper, but they insist that voting firms will overcome them. Most major voting companies, including Diebold, already say they can build systems that include a paper trail. "Our perspective is that voter confidence is paramount in terms of the election process," Tony Miller, an attorney in Shelley's office, says. "Even if this costs a few thousand dollars, the cost of democracy is not necessarily cheap and it shouldn't be the determining factor."

David Dill describes Shelley's decision as "the biggest breakthrough that the paper trail movement has had to date," and he says that he's certain "it will affect the attitude of people in other states." He was right: In December, Nevada also acted to require paper receipts. Dill also has high hopes for the [Voter Confidence and Increased Accessibility Act of 2003](#), a bill introduced in Congress by Rep. Rush Holt, a New Jersey Democrat, which would require a paper trail nationally. Three Democrats in the Senate — Barbara Boxer, Hillary Clinton and Bob Graham — have each proposed companion legislation.

But officials who've already invested in paperless machines will have a hard time joining the paper-trail bandwagon. In Georgia, for instance, Cathy Cox is sticking by her decision. In a speech to the state's political scientists in November, she assailed the critics who've lately attacked touch-screen voting systems, saying they "approach the issue of election technology as if on a mission to save humanity from the scourge of a worldwide conspiracy." But Cox, it should be noted, is massively invested in the reliability of the Diebold systems she purchased, having staked her political career — and the millions it cost to purchase them — on the new system.

The people who insist that Georgia's 2002 election was stolen may well be wrong. But the attention that they are focusing on voting machines is anything but misplaced. An election has to be above suspicion, even above the suspicion of some of the most suspicious people in a democracy. Says California's Tony Miller: "If people don't have confidence in the voting systems being used, then they lose faith in the voting process itself."

www.salon.com/tech/feature/2004/02/09/voting_machines/print.html

The Problem with 'Anyone But Bush'

T. Patrick Donovan | **Dissident Voice** | **February 4, 2004**

"For progressives to submerge ourselves within the ABB tidal wave is a complete abdication of our responsibility as global citizens to agitate around the issues facing this

country and the world, rather than once again believing that our work is limited to simply voting for the president every four years."

Following the strategy of "Anybody But Bush" in the upcoming presidential election is equally as dangerous as Bush getting re-elected.

Why? There are two basic reasons.

First, the "Anybody But Bush" (ABB) movement is predicated on the mistaken and illusory belief that Bush & Co. is an aberration from the American political system, rather than extensions of it.

Second, for progressives to submerge ourselves within the ABB tidal wave is a complete abdication of our responsibility as global citizens to agitate around the issues facing this country and the world, rather than once again believing that our work is limited to simply voting for the president every four years.

"These are the times that try men's souls," wrote Tom Paine, a seminal thinker during the birth of America. Today, these are times when the very souls of America and the entire planet are at stake. To think that in this post-9/11 reality we can go on with business as usual, believing that who is in the White House is the only cutting-edge issue, is patently absurd.

Given the debacle in Florida in 2000, the fact that the U.S. Supreme Court intervened in the last election, and the fact that [suspect computerized voting machines](#) are on their way, how much faith can we seriously have in the election process as a whole?

More importantly, though, we face today issues wherein the future of the planet is at stake. We know it and the powers-that-be know it too. Bush's election in 2000 was a reflection of the extent and depth of these fundamental problems. Bush's time in office and the policies flowing forth from his tenure — most dramatically

the invasion and occupation of Iraq — are attempts to stem the tide of America's decline.

With the world's oil reserves passing peak production capacities, the beachhead in Iraq is the keystone for both control of the majority of these reserves and the maintenance of our American lifestyle, such as it is these days. I cannot emphasize enough that this occupation (and eventual expansion) is a fundamental part of American global aspirations, and this WILL NOT change whether a Democrat is elected or Bush is re-elected!

Why? Because it cannot be reversed unless a complete re-evaluation and reassessment of America's ambitions toward empire is undertaken. What the ABB movement fails to recognize is that neither Dean nor Kerry nor Gephardt nor Clark are up to the task of dissecting the inner workings of American capitalism and its engine of globalization.

The likeliest scenario, given a Democrat being elected in November, is that they will spin the continued occupation of Iraq as "necessary" and "humane" because America needs to rebuild the country that it destroyed.

So, unlike Vietnam, where "stopping communism" was the rationale, this time the rationale will be "fixing the mess that Bush left us." Different storyline, but the result will be years of continued occupation and control of the region's oil.

The extremism that is the Bush regime is really a mirror into the extreme nature of the situation facing us all. Below all the political machinations, all the dire warnings of economic collapse, renewed plans for nuclear wars, global warming, etc., is the fact that the system that brought us all the benefits of modernity has now revealed its darkest shadow: the absolute commodification of every aspect of our lives, our relationships to each other and our environment.

The American Way has brought us to the ultimate precipice.

Despite the extreme difficulty that we humans have in breaking the bonds of habit, inertia, and mesmerization with the status quo, it is time for we, the people, to begin the deep soul-searching, soul-wrenching inquiry and debate over how we reclaim our humanity.

Ultimately, it is NOT the economy, stupid; NOT the environment; NOT foreign policy; NOT even the occupation of Iraq that demands our deepest attention. And it is certainly NOT about uncritically "taking back America."

Important as some of these may be, these are but the symptoms of a greater and more deadly infection: our complete dissociation from our world, each other, and even our own hearts.

This election year could be an amazing opportunity to take a hard look at where humankind has come from and where we are heading. This is the orientation that our elected representatives need to have as well. To drown the nascent potential that these next few months could offer in the staid waters of "Anybody But Bush" is one more crime we inflict on ourselves and on the planet.

And we inflict it at our own peril.

www.dissidentvoice.org/Feb04/Donovan0212.htm

Analysis: Pentagon E-Voting Plan Scrapped

Cynthia Webb | Washington Post | February 6, 2004

"It's worth noting that the announcement came from an anonymous official, *The Associated Press* reported, a sign that the Pentagon wants its backpedaling to be done with as much secrecy as the American citizen gets inside the voting booth."

The Internet's role in campaigns and elections continues to grow, but security snags continue to mar e-voting efforts. Amid a public outcry over security, the

Pentagon said it would pull the plug on its plan to let U.S. citizens living abroad cast their votes online in the upcoming presidential election.

The news is an about-face for the Defense Department, which had virulently defended an expansion of its e-voting program, despite a recent report by computer security experts that called for it to be tanked because of the potential for security problems and hacker attacks that could change votes or taint information.

Seems the Pentagon brass finally listened to the criticism, mostly from four computer scientists who were part of a group that reviewed the merits — and pitfalls — of the test system, called the Secure Electronic Registration and Voting Experiment. The idea of e-voting is a good one in theory, but so is the shelving of this plan for now since the security holes experts identified could allow someone to monkey around with real votes — not exactly the foundation on which the United States was built.

"The cancellation of the system is the latest set back for Internet and electronic voting amid ongoing concerns over the security and reporting features of e-voting machines. The criticism has mounted to the point that the makers of e-voting machines have formed a lobbying group to take their case to Washington, D.C. The Defense Department hasn't indicated what the next step is for Internet voting, except that the United States is still interested," CNET's News.com reported.

The government's e-voting Web site, part of the Federal Voting Assistance Program, apparently hasn't caught wind of the cancellation order. It still bears the headline: "Vote Using the Internet In 2004!" The program was supposed to go live for the primaries this past Tuesday. It's worth noting that the announcement came from an anonymous official, *The Associated Press* reported, a sign that the Pentagon wants its backpedaling to be done with as much secrecy as the American citizen gets inside the voting booth. "The official, who requested

anonymity, said Deputy Defense Secretary Paul Wolfowitz made the decision to scrap the system because Pentagon officials were not certain they could 'assure the legitimacy of votes that would be cast,'" The AP wrote.

The New York Times provides more details on where the stop order came from. "The decision was announced in a memorandum from Deputy Defense Secretary Paul D. Wolfowitz to David S. C. Chu, under secretary of defense for personnel and readiness. Paraphrasing the memorandum, a Department of Defense spokeswoman said: 'The department has decided not to use Serve in the November 2004 elections. We made this decision in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election results.' The memorandum says efforts will continue to find ways to cast ballots electronically for Americans overseas and to use Serve for testing and development."

Don't discount the possibility that President Bush might want to do whatever he can to avoid mention of controversial votes this time around, especially after the, uh, uncertainties that marked Florida's vote-counting operation in 2000. More on the cancellation of the program: "The \$22 million pilot project was intended to be used by about 100,000 voters from 50 counties in seven states. State election officials said they were told late Wednesday that it would not be used to count votes included in election results," *The Washington Post* reported. "Overseas voters will be able to cast Internet ballots as part of a test intended to learn more about online voting. But to cast an actual vote in the presidential election, they will have to fill out and return the traditional paper absentee ballots. The greatest security concern is the personal computer of the individual voter, said Paul W. Craft, an election official from Florida, one of the participating states. A virus or other hidden program in a voter's computer could monitor keystrokes and intercept — or change — votes. 'They decided they could not mitigate that risk sufficiently for the 2004 election. We would not have used it unless they addressed that risk,' he said."

The same article noted that the decision came after the report and a call to stop the program from the Republican and Democratic party groups for citizens living overseas.

The two groups banded together, likely spurred by the release of the scathing report, which listed a number of concerns including this particularly troubling contention about hacker attacks on the system: "Such attacks could occur on a large scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law. These attacks could result in large-scale, selective voter disenfranchisement, and/or privacy violation, and/or vote buying and selling, and/or vote switching even to the extent of reversing the outcome of many elections at once, including the presidential election. With care in the design, some of the attacks could succeed and yet go completely undetected."

GovExec.com reported yesterday that a "Pentagon spokeswoman said that she could not comment on whether the report led directly to the cancellation decision. According to the spokeswoman, the Pentagon is not focused completely on the SERVE program. Defense officials are currently investigating other technology that would allow military personnel overseas to securely cast their votes online, the spokeswoman said." Stay tuned.

E-Vote Rocked

Security concerns are affecting states' e-voting efforts as well. California Secretary of State Kevin Shelley is trying to improve the security of e-voting machines after a separate report indicated the systems can be compromised. Shelley wants Diebold Election Systems, which makes e-voting machine software, "to turn over its software code so it could be evaluated by independent experts chosen by the state. Shelley also is requiring random state testing of all electronic voting systems on election day to ensure ballots are accurately recorded," The San Jose Mercury News reported. "One in four California voters,

including those in Alameda County, are expected to cast ballots in next month's presidential primary on electronic voting systems made by Diebold Election Systems. Last week, computer scientists hired by the state of Maryland to hack its Diebold voting system announced they had successfully changed vote tallies on touch-screen voting machines, altered ballots and seized control of a central vote-counting computer ... The report, which was prepared by Raba Technologies for the Maryland legislature, comes on the heels of an audit of California Diebold systems conducted by Shelley's office in December. That study found Diebold had installed unapproved software in 17 California counties in violation of state law."

E-Vote Rolled

Michigan, however, has fully embraced e-voting for this weekend's caucus. "Anyone who requested to vote absentee received a paper ballot that could be mailed in; that ballot included directions and passwords to vote on the Internet. As of last Saturday's deadline, 123,000 people had requested the mail-or-Internet ballots, a huge leap for caucuses that had 20,000 voters four years ago," *The Washington Post* wrote. "We're holding the most accessible election ever in the United States — five weeks of voting by mail and five weeks of voting by Internet," Mark Brewer, the state party's executive chairman, told the paper. "Plus you can vote in person Saturday. We're taking the election to the voters."

In an opinion piece in today's *Detroit News*, George Weeks wrote: "Saturday's Democratic presidential caucus is a test not only of candidates. It also tests a process that will be watched by both parties and by election officials across the land: voting by Internet. By late Thursday, more people — 21,200 — already had voted by Internet than the 20,000 people who voted in Michigan's 2000 Democratic caucus." More from the article: "Arizona had Internet voting in 2000, but Michigan is the only state to use it this year in the nominating process. Terry McAuliffe, chairman of the Democratic National Committee (DNC), has touted it

as a process for the future that is being honed by Michigan Democrats. The DNC rejected a challenge by some Michigan Democrats — supported by Kerry and all other Democratic contenders except Dean and retired Gen. Wesley Clark — that Internet voting would disadvantage the poor and minorities who lack Internet access. ... The Internet also is being used to help voters determine their nearest caucus site. Information is available at www.publius.org and www.mi-democrats.com."

www.washingtonpost.com/wp-dyn/articles/A18597-2004Feb6.html

From: Stuart Schy
Sent: Friday, August 03, 2007 10:58 AM
To: Voting Systems
Subject: Suggestion

I have been reading as much as I can of the documentation you have posted on your website in the last few days. The grouping of the written comments by affiliation was particularly illuminating. I noted the use of the same or similar "talking points" penned by the RoV correspondents such as "we oppose...." which echoes the points made by the vendors.

Because of my long involvement with disability issues, I was particularly interested in the communications from the organizations devoted to helping the disabled. They appear to have been convinced by the vendors and perhaps the RoVs that computerized voting was very much needed.

As suggested in my email of July 31 to you, I feel the evidence for decertification is overwhelming. But, if you do find it necessary to use electronic devices for disabled voters, please consider making them available ONLY for people with disabilities. Isn't that what we do with those blue parking spots and other accomodations?

Thank you again for a remarkable job in initiating and carrying out the Top-to-Bottom Review. Please know that you have a lot of support in your quest to getting our democracy back.

Stuart Schy

From: Harold Lecar

Sent: Friday, August 03, 2007 3:30 PM

To: Voting Systems

Cc: Michelle Gabriel; Helene Lecar; Mike Lecar; Dan Ashby; Don Goldmacher

Subject: Source Codes designed for election theft

Dear Secretary Bowen:

The corrupt state of the software codes for all three companies (Diebold, Sequoia and Hart) cannot possibly be coincidental. Nor can this be chalked off to incompetence alone. The companies have had ample time to fix their deficiencies if they wanted to. Diebold has already been decertified at least twice, and only was recertified on their own say so.

The hue and cry of some ROVs is ironic. They are exorcised about the very idea of testing the machines, but are oblivious to the fact that all the machines flunked. The very intensity of their protest would lead one to think that they themselves have something to hide.

If the machines cannot be abandoned in time for the primary election, one can use a provisional decertification to some advantage, by specifying a draconian set of election-day random checks and mandatory complete public audits. Also ballots can be recounted by open-source-coded fast counters run by state officials.

Furthermore, the previous use of these corrupted machines should provide legal justification for opening and recounting the ballots for disputed 2005 and 2006 elections. In particular, the San Diego congressional elections, which featured sleep-overs of the insecure machines, a phony premature swearing-in ceremony before the results were certified, and a denial of all legitimate requests for recounting the ballots, should be investigated.

Of course, machine manipulation is not the only vehicle for election theft. It appears that California was also a victim of the nation-wide effort to disenfranchise voters under the pretext preventing election fraud. Although former Secretary MacPherson said that HAVA made him do it, it does seem fishy that so many states use the same computer programs which selectively disenfranchise minorities (43% of new registrants is his case) and that these programs give mostly wrong results. This suggests a very thinly disguised conspiracy. If the Attorney General took up this matter, he would be doing the whole country a great service. After all, this scam is at the heart of current DOJ investigations, and appears to be one of the preferred modes of operation for the 2008 elections.

Thank you for the great service you are doing for California and for the maintenance of democracy in the United States.

Sincerely yours,

Harold Lecar

From: Richard Lyons
Sent: Friday, August 03, 2007 2:02 PM
To: Voting Systems
Subject: Re: My election/voting thoughts...

Dear Secretary Bowen,

I am deeply alarmed at the cavalier attitude of such companies as Diebold towards our voting franchise. It is not fear-mongering to be concerned over the very integrity and nature of our coveted voter franchise.

It is known that Diebold is a friend of Bush. We are seeing the damage the dubious elections in 2000 and 2004, most particularly in Ohio and Florida, have wrought. Such a mess must not be permitted to reoccur.

I have already sent an email to your office, stating in NO uncertain terms that I wish to receive ONLY paper ballots, which I mark myself, put into the ballot box and are not liable to tampering. In such an administration as this, influenced by men of such low moral character as Karl Rove, no vote is safe: that is clear. But one can try to prevent as much tampering as possible by NOT certifying the use of these pigs-in-a-poke, the electronic voting machines. Nowhere they have been introduced has the election been free from taint. The attendant voter frauds under this administration have yet to be properly addressed. I do not want in California what has happened in too many other parts of this country.

Please insist on paper ballots only, until a system so secure and certain is produced that we need not fear for the very Republic.

Thank you.

In Peace,

richard scott lyons

From: V.E. Lane
Sent: Friday, August 03, 2007 1:36 PM
To: Voting Systems
Subject: Replace all machines with paper ballots handcounted at the Precinct SAVElections Monterey County

Dear Debra:

We commend you and suport you. Dr. Judith Alter spoke for SAVElections Monterey County in her testimony. We have demanded the removal of our Sequoia machines and have called upon the BOS to hear our grievances. We are awaiting their scheduling of a public hearing so that we can provide testimony to support our position. Paul Lehto,esq. and Rebecca Mercuri have advised you of their opinions which we fully support.

Perhaps most important is the simple fact that citizens do not trust these machines and have thanked us for speaking up on their behalf. They are ready, willing and able to hand count the vote. We do not belive that the optical scan tabulators should be used to count the paper ballots because they are counting our vote behind closed doors. We are not permitted to have any meaningful oversight of the election procedures.

On election nite laptops downloading results and tabulating screens are turned away from our view.

The one percent audit is conducted by the same people who have run the elections. Again we are unable to view ballots or records during the audit. We must not interrupt except by written question to the ROV.

The poll closing tapes were not posted in our June 2007 election because our ROV Linda Tulett informed us in writing that this procedure is "obsolete and not possible due to security restrictions related to the VVPAT's." Dr Alter has just delivered documents from your office to us which in fact are copies of an e-mail to Clerks from SOS McPherson to counties which have Sequoia DRE's, instructing them in the correct procedure to create poll closing tapes to insure that they adhere to the CA election Code.

It is really quite simple, it is insider tampering which cannot be protected against. Citizens should not have the burden to prove tampering which may leave no evidence..

PLEASE DECERTIFY ALL THE VOTING SYSTEMS. RESTORE OUR DEMOCRACY>

THANKYOU,

Valerie Lane

From: Susan & Noel
Sent: Friday, August 03, 2007 1:27 PM
To: Voting Systems
Subject: Decertify the voting machines

Below is what I sent to the Democratic Party because Howard Dean (chairman) sent out a letter saying that the Democrats are right now going out to be sure that the election is fair. How, I don't know. They just asked for money. What I wrote back (whether they get it or not, is another question.) follows:

Is the Party aware of the struggles going on in some states, California in particular, regarding decertifying electronic voting machines? The Secretary of State had the machines provided by the three electronic voting machine companies whose machines are used in California tested against hacking. All of them failed the testing. Nevertheless, the Registrars of Voters in California (except for the one in Yolo County) are fighting to have the faulty machines accepted by the Secretary of State's office. This certainly is an issue that the Democratic Party should be very interested in and should strongly be supporting the Secretary of State of California.

Susan Kidder

From: Joe Harty
Sent: Friday, August 03, 2007 12:10 PM
To: Voting Systems
Subject: Absolutely no computer voting machines....

Secretary of State,

The mere fact that these machines are still being considered for the primary's use means that money is flooding the talking heads departments in these nefarious organizations still. Diebolt alone stands as the shining example of a new kind of criminal, a vote distorter on the pay of the gop with a track record with the GOP going back to the secretary of state/GOP hack Kathleen Harris of Florida back in 1999 and the deliberate, proven action to disenfranchise 40,000 people and tinker with the poll numbers so that for the first time the polling numbers did not match their votes.

The absentee ballots should be the only alternative to paper ballots at the polls like in Oregon, as there is no trust in any of the computer voting machines, even with paper trails because the people who are involved and own these companies are less than democratic. They are disloyal to our secular democracy. As a matter of fact I consider this a fundamentalists problem. I refer to the cult of the American Taliban, the southern christians, who just like the Taliban radicals in Afghanistan hold everyone who thinks different from them in contempt worthy of being attacked, those kind of people maybe alright to rule their cults, but have no place in our democracy.

Please shut this down, when you do it will have an instant effect in other states, also in the process of bankrupting a field unworthy instrumentations set-up to give ultimate power to corporation types over us all. This is in direct opposition to the single most dynamic democracy on the earth at any time in history. Stop the machines involvement with the vote, crush their grip on the system here, if California leads other states will follow. I believe this maybe the last chance to

stop this. Please shut them down now! Last, feel free to send whatever information that shows your research's findings.

Joseph F.P. Harty

From: Jackie Maruhashi
Sent: Friday, August 03, 2007 10:20 AM
To: Voting Systems
Subject: Top-To-Bottom Review of Voting Machines

August 2, 2007

The Honorable Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, CA 95814 /Sent via e-mail to: _votingsystems@sos.ca.gov
<<mailto:votingsystems@sos.ca.gov>>_/

/___/*RE: Top-To-Bottom Review of Voting Machines*

**Dear Secretary Bowen:

We support the August 1, 2007 letter sent to you by the Asian Pacific American Legal Center and other civil rights and civic engagement organizations. The Asian Law Alliance is a non-profit community law office that has significant experience working with new voters and those who are limited English proficient.

We oppose any decertification of the voting systems as a means of addressing the report's findings that question the security and accessibility of the voting systems. We support recommendations calling for corrective action to mitigate or eliminate the security vulnerabilities identified in the report. In addition, we believe that accessibility issues addressed in the report can be remedied without forcing counties to switch to other voting systems.

Currently, Santa Clara County voters may vote in Chinese, Spanish, Tagalog, and Vietnamese in addition to English on the Sequoia AVC Edge electronic voting machines. These machines offer increased access to the polls when compared to the paper-based voting systems. As a result, voter registration and turnout have increased tremendously in Santa Clara County.

With so little time left before the February 2008 election, we urge you to fix the problems identified in your July 27, 2007 report, but not decertify our voting system.

Sincerely,

Richard Konda,
Executive Director

From: Ouapiti Robintree
Sent: Friday, August 03, 2007 7:27 AM
To: Voting Systems
Subject: VOTING MACHINE FRAUD -- Please nip this problem in the bud!

To: Secretary of State Debra Bowen
re: validity and function of electronic voting
machines

Dear Secretary Bowen,

I am writing to share my concern about the use of electronic voting machines in recent US elections. It has been shown repeatedly that these machines are easily manipulated for fraudulent purposes, and American citizens have very serious concerns about the validity of our recent election outcomes. If there is a HINT of illegality about these machines, it is your duty to decertify them and, if at all possible, return the American populace to the use of paper-and-pencil ballots which we've used to record our votes, until such time (which I doubt) as these machines can be programmed against ANY tampering. It is imperative that you hold these companies accountable for lying and deceiving state officials. The refusal to step up and do the right thing NOW may lead to inaccurate reporting of the American people's will for government, and THAT IS A TRAITOROUS OFFENCE! How can we be a nation of informed voters, if our rights to vote are taken away by corrupted computer-voting programs?

Our founders held that voting was a citizen's right and duty; please don't let this country go down in history as crumbling under the corruption of this administration. Regardless of your party membership, surely you must see that "Those who cast the votes don't matter; those who count the votes do."
(paraphrasing Josef Stalin)

History will record your actions for posterity, and it would be a sad day if this nation crumbled because of the iniquity and vice of corrupt politicians and voting machine companies. Please do the right thing and stand up for American virtue and TRUE freedom: the right to express ourselves by voting for the men and women we trust to lead this country back into virtue and respect from the rest of the world.

Yours sincerely, one more concerned citizen,
Ms. Robin O. Robintree

From: 2005nfg
Sent: Wednesday, August 01, 2007 12:33 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mrs. Toni Kimball

From: rionido104
Sent: Wednesday, August 01, 2007 12:34 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. john andreas

From: muckd5
Sent: Wednesday, August 01, 2007 12:34 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. Dorothy McDonald

From: cbingram
Sent: Wednesday, August 01, 2007 12:34 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Paper ballots, counted slowly and carefully. Totally verifiable.
Totally recountable. Extremely difficult to alter.
Let's take 10 days to count the vote. We can wait.
What's the rush? The anticipation will be exquisite!

Mr. christopher ingram

From: susan
Sent: Wednesday, August 01, 2007 12:34 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

I am an informed citizen who has voted in EVERY election possible - local, state, federal - since turning 21 in 1971 and I'm dismayed at the prospects of allowing hackable voting machines to be used in the State of California. It is imperative, for the very sake of our democracy, that only reliable, non-hackable voting systems are allowed to be used to ensure that EVERY vote is accurately counted. No private corporate interests or voting machine vendors can be permitted to dictate how our elections are conducted. Thanks to Debra Bowen for conducting the "Red Team" review and please stand firm for for allowing only reliable, non-hackable voting systems to accurately record our votes.

Ms. Susan Longstreth

From: mwh7
Sent: Wednesday, August 01, 2007 12:34 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Democracy cannot survive without an infallible means of counting the vote. Would we trade that for mere efficiency?

Mr. Michael Henscey

From: karlsonsheila
Sent: Wednesday, August 01, 2007 12:34 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

I no longer trust the vote in California using computers. I will use absentee ballot from now on unless the state changes the system. We simply MUST have a paper trail.

Mrs. Sheila Karlson

From: susanshepard777
Sent: Wednesday, August 01, 2007 12:34 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

These machines can be easily manipulated and cannot be trusted for accuracy. Please, DECERIFY these Voting Machines.
Thank You

Mrs. Susan Shepard

From: Auditor John R Brakey
Sent: Friday, August 03, 2007 5:13 PM
To: Finley, Lowell; Voting Systems
Subject: Please, our country need leaders. Have you seen the letter to Diebold from the Sos of Florida? YES Decertification of all equipment that is not made secure ; OS only come only back when you have meanifuling handcounts

Dear Lowell,

Please, our country needs leaders, our Election System is broken

Decertification of all equipment that is not made secure; OS come back when you have meaningful hand counts per the new Brennan Center report has very good cross over players who put it together and it came at the right time.

http://www.brennancenter.org/dynamic/subpages/download_file_50089.pdf

TABLE 2. ADJUSTABLE-PERCENTAGE AUDIT MODEL:

TIERED AUDITS OF PRECINCTS IN THE MODEL CONGRESSIONAL DISTRICT					
No. of Precincts	Margin of Victory	Confidence in a 2% Audit	Confidence in a 3% Audit	Confidence in a 5% Audit	Confidence in a 10% Audit
400	0.75%	15%	22%	34%	58%
400	1.75%	31%	43%	61%	86%
400	5.00%	66%	80%	94%	99%

Have you seen the letter to Diebold from the Sos of Florida? Its attached.

All e-mail I send now have his on the bottom thanks to you and SOS Bowen.

Before August 2, 2007; Rev. DeForest Soaries, the first Chairman of the Election Assistance Commission said:

"We know more today about how to build a machine to take pictures of rocks on Mars than we know about how to build a voting machine to safeguard the American right to vote."

Read what else he has to say: <http://www.bradblog.com/?p=3491#comments>

However that has changed do to the Top-to Bottom Review by California's Secretary of State Debra Bowen. Link to the documents

http://www.sos.ca.gov/elections/elections_vsr.htm

Our ADP-EIC Chair - Dr Ted Downing wrote; "Based on the results of your Top to Bottom Review, the Arizona Democratic Party's Election Integrity Committee supports decertification of all equipment that is not made secure as outlined in your reports for the 2008 election cycle." you met Ted in Phoenix 18 months ago.

Audio links of William J. "Bill" Risner Esq. on the John C. Scott Radio Show Tucson, Arizona Ted Downing Hr 1, Bill Risner Hr 2, about litigation PCDP vs Pima County, Election Fraud, Vote Flipping. [State asked to review '06 RTA vote | www.azstarnet.com](http://www.azstarnet.com) @ 5-26-07 State asked to review '06 RTA vote. Lawyer for Dems says transport tally was possibly altered. By Andrea Kelly AZ Daily Star

Audio [John C Scott hr1 5 30 07 Dr Ted Downing.mp3](#)

Audio [John C Scott hr2 5 30 07 Bill Risner Esq.mp3](#)

William J. Risner Esq

Firm: [Risner & Graham](#)

Address:

[Arizona Election Wars: Pima County: The Gauntlet Is Thrown'](#) Time 6:57 Part 1 of Series: Powerful letter by Tucson Democratic Attorney Bill Risner to the County Manager on what's been going on with ele Part 1 of Series: Powerful letter by Tucson Democratic Attorney Bill Risner to the County Manager on what's been going on with elections in Pima County. Set to a powerful song 'MY VOTE DON'T MATTER ANYMORE' Written and performed by VICTORIA PARKS. For over 2 years we have been investigating Pima County Election Department and we don't like what we're have found. They have illegally been printing of election results up to 8 days before the election using the mail in early ballots. This has been going on since the primary of 2004. We know how the backdoor works with the GEMS/Diebold system and how it could be easily hacked using MS-Access. A lawsuit was filed shortly after letter was sent that is basics of this video.

[Arizona Election Wars: Is Our Vote Secure in Pima County?](#) Part 1 of 2 They've known about the backdoor since 1996: Several Pima County bureaucrats from the very top down have known about the backdoor in our voting system. This odd procedure is not found in the 548 page Diebold's User Guide for our voting software, nor does explain that the system is built upon Microsoft Access. Furthermore, by using MS-Access, in less than a minute; a person could switch election by changing two positions in the candidates table (in Access) flipping an election all the way down to the precinct level. This and much more was

established in depositions taken by well known Democratic Attorney William 'Bill' Risner in Tucson, Arizona. Clip explains more!

[Arizona Election Wars: Is Our Vote Secure in Pima County?](#) Part 2 of 2 Time 08:00
They've known about the backdoor since 1996: More clips coming soon.

Kimble: Does the RTA vote really add up? | www.tucsoncitizen.com ®

Published: 06.07.2007

Kimble: Does the RTA vote really add up?

[MARK KIMBLE](#)

Tucson Citizen

It is not what you want to hear about the people entrusted with counting our votes:

- * "Less security than I have on my home computer."
- * "The appearance isn't good."
- * "The facts available match an 'election hacking' incident . . . while matching no legitimate processing procedure."
- * "Dismal record in implementing reasonable computer software security measures to protect election data from improper access or change."

Those are the opinions of two computer experts who have carefully examined how Pima County runs its vote-counting operation.

And even if you don't understand the language of computer code - and I don't - there are enough questions to generate a lot of concern about how accurately your votes have been counted.

How bad is all of this? Who knows?

There is a possibility of outright fraud, with vote totals changed or totals for winners and losers flipped. Or the totals may be dead-on accurate with nothing more than unexplained idiosyncrasies in the way computer operators do their job.

The answer may be in computer records that Pima County is refusing to release. Or it may be impossible to ever know with certainty what happened in recent elections.

The poster child for concerns is the May 16, 2006, Regional Transportation Authority election.

Some significant events in the vote-counting for that election are highlighted below in excerpts from a Pima County election report.

The Pima County Democratic Party is suing for access to county databases to try to determine what happened when votes were counted in that and the 2006 fall elections. Among the issues:

- * Counting of early ballots started May 10, six days before the election. Votes were counted for about four hours, which probably meant at least 8,000 ballots counted and maybe as many as 12,000.

The tally was saved. Then it was saved again the next morning before counting resumed. Why?

William J. Risner, a lawyer and Democratic activist involved in the lawsuit, asked the county worker under oath why he did that. "He had no explanation for it," Risner said.

James March, a computer expert who has worked on elections systems, outlined one possibility. In a declaration in the Democrats' suit, March said someone could have copied the election data to a disk, taken it to another computer, used widely available software to hack it, then returned the disk with hacked data and overwritten the vote count.

The vote totals could have been changed. Or the counts for "Yes" and "No" could have been reversed.

"The facts available match an 'election hacking' incident of this sort," March's declaration said.

*** On May 11, five days before the election, reports were printed that showed early vote totals. If people on either side had known those totals, it would have been invaluable for late campaigning.**

Brad Nelson, Pima County elections director, said the reports were printed and "glimpsed at" only to make sure the total number of ballots counted matched the number fed in. The reports then were shredded, Nelson said.

*** Early vote total reports also were printed before the 2006 primary election, March wrote. In one race, a "who is winning" report was printed at 3:45 p.m. on the Saturday before the Tuesday election.**

At 8:30 p.m. that same Saturday, a "robocall" went out to voters in that race slamming one candidate, March wrote. "We cannot positively link the two actions, but the appearance isn't good," he wrote.

Risner is asking for the county database that shows all activity on the election-counting computer.

But Nelson said he doesn't want to supply that because it would compromise security. "There are passwords and modem numbers in that," he said.

Risner countered that such information has been released elsewhere and is available on the Internet without security being compromised.

So what does all this mean? Have some winners actually lost and losers won? Have invaluable early vote-counting totals been leaked, allowing a campaign to be tailored at the last minute?

Nelson says absolutely not. There is 24-hour video surveillance of election-counting equipment. There are two-part passwords, and each employee knows only one part. "The level of security in the election division is always evolving and always getting better," he said.

Risner has doubts. "I don't know why or where or if," he said. "We're not telling anyone it happened. But the way the software works, you don't see this anywhere else."

It's impossible to know who is right and whether anyone actually did anything untoward. But the county's secrecy - while apparently well-meaning - does nothing to alleviate the concerns.

And when it comes to accurately counting votes, there is no room for any concerns.

Election Summary Report

for May 16, 2006 election, with date, time, action and what it means

05/10/06, 08:21:41, Reset election: Ensures that totals are at zero.

05/10/06, 08:22:08, Printing summary report: Report showing vote totals; all should be zero. Vote counting starts.

05/10/06, 012:27:27, Backed up election to D:\Program Files/pimaconsolidated051606 EARLY DAY1.gbf: Early votes have been counted for about four hours. Totals are saved.

05/10/06, 12:27:38, Previewing Cards Cast Report: Indicates how many ballots went through the scanners.

05/10/06, 12:28:05, Closing GEMS: GEMS is the Global Election Management System software. developed by Diebold Election Systems. Vote counting is over for the day.

05/11/06, 09:55:57, User login: GEMS started.

05/11/06, 09:55:57, Open Election: Consolidated Election, May 16, 2006: Ready to start counting votes.

05/11/06, 09:56:30, Backed up election to D:\Program Files/pimaconsolidated 051606 EARLY DAY1.gbf: Appears to indicate vote totals from the previous day were overwritten.

05/11/06, 09:56:49, Printing summary report: A report showing vote totals was printed.

05/11/06, 10:06:21, Printing summary report: Another report showing vote totals was printed.

05/11/06, 12:06:48, Previewing Cards Cast Report: Looking at a report on the number of early ballots cast. Counting begins again.

05/11/06, 15:23:32, Backed up election to D:\Program Files/pimaconsolidated 051606 EARLY DAY2.gbf: Votes have been counted for about three hours. Totals are saved.

05/11/06, 15:23:46, Closing GEMS:Vote counting is over for the day.

Mark Kimble appears at 6:30 p.m. and midnight Fridays on the Roundtable segment of "Arizona Illustrated," KUAT-TV, Channel 6. Reach him at mkimble@tucsoncitizen.com and 573-4662.

[Subscribe to the Tucson Citizen](#)

Comments on this Story

[Write a letter to the Editor](#)

[27 Total Comments - See All Comments](#)

1. Comment by Mike H. (#3533) - June 7,2007 @ 9:45AM

Pima County really needs to open the doors on this investigation. Those of us who opposed the RTA were astounded to see pro-RTA forces repeatedly break campaign laws and get off with hand slaps. Now, it seems possible that they may have gone far

beyond those small irregularities. The ballots need to be recounted by an independent, non-partisan outside agency and actual results made public. As big a catastrophe as the RTA is for central city neighborhoods such as ours, the possibility that elections are being stolen and manipulated is much worse. When WE, THE PEOPLE may not actually be choosing our government or passing ballot issues that are put in force, the fundamental covenant on which this nation stands is put into doubt. That is absolutely unacceptable. Thank you, Mark Kimble, for this honest assessment.

J.M. "Mike" Hayes, President, Campbell/Grant Northeast Neighborhood Association

2. Comment by Jan F. (Janis) - June 7,2007 @ 10:22AM

Government, especially elections offices, must run with absolute transparency. Hiding behind security concerns is lame and casts doubt about the integrity of the whole election process.

If all the votes can not be counted fairly, then we need to stop the RTA and have another election.

3. Comment by Glenn M. (GLM) - June 7,2007 @ 10:23AM

Our tax dollars at work.

Debra Bowen's Voter's Bill of Rights

10 simple but powerful principles that will guide her every day as your next Secretary of State.

The ability to register to vote, to cast a ballot, and to have that ballot counted accurately is the very foundation of our democracy. To that end, every one of California's voters is entitled to the following rights:

- 1. The Right To Register To Vote.** Every Californian who is eligible to vote has a legal right to register to vote without being forced to navigate through unnecessary bureaucratic obstacles.
- 2. The Right To Vote.** Every registered voter has a right to cast a ballot. This means that Voters shouldn't show up at a polling place, only to find it closed for hours or be forced to stand in lines because the voting equipment doesn't work. In addition, essential information about voting should be readily available to all voters.
- 3. The Right To Vote In A Tamper-Proof Election.** Every voter has the right for his or her vote to count equally -- which means no one should be required to vote using machines that have been proven time and time again to lack the security necessary to ensure that people's votes are counted accurately. If a piece of voting equipment isn't secure, accurate, and auditable, it should not be used in California's electoral process.
- 4. The Right To Vote On Paper.** More and more counties are installing electronic voting equipment and doing away with the paper ballots that

voters are used to just as voter confidence in electronic machines is plummeting. Voters should have a right to cast a paper ballot, and it should be made clear to voters that they have this choice.

5. **The Right To Have Each Vote Counted Accurately.** A vote is meaningless unless it is counted as the voter intended it. In recent years, every election has brought instances of votes being inaccurately tabulated and voter confidence in the election results is at an all-time low. It's time to change that.
6. **The Right To Have Election Results Properly Audited.** Audits are the only way to ensure the accuracy of the vote. Next year, when SB 1235 (Bowen) takes effect, the current law requiring that 1% of precincts be audited will be expanded to include votes cast by absentee ballot and early voting centers, and will require full transparency of the auditing process. Audits should be statistically valid, and when there are irregularities the audit should be expanded or a full recount should be conducted.
7. **The Right To An Open, Transparent, Public Process.** While every voter's ballot is and must be private, that's the only thing in the electoral process that should stay a secret. We should have full transparency in elections procedures, all phases of the conduct of the election, the process used for testing, reviewing and buying voting systems, and all reports of errors and anomalies should be made public. Finally, voters should be entitled to watch the vote-counting process and the 1% manual audit process.
8. **The Right To Elections Officials Who Operate Free of Partisan Influence.** Anyone who is in charge of tallying the votes and certifying the results of an election, including the Secretary of State and local registrars of voters, should not endorse candidates for office in that election.
9. **The Right To Know that Elected Officials Are Free From the Influence of Campaign Contributions From Voting Machine Vendors.** The people responsible for setting the standards for voting equipment, for testing a voting system, or for deciding which system to buy should not be taking campaign contributions or gifts from voting equipment manufacturers who have a financial interest in the decisions that are made.
10. **The Right To Find Out How Money Is Being Raised And Spent In The Political Process.** Voters should be able to easily find out the true identity of any person or any entity that is contributing to campaigns, as well as how candidates and campaigns are spending their money.

Nobody, and no machine, should be counting American votes in secret.

Our ADP-EIC Chair - Dr Ted Downing wrote; "Based on the results of your Top to Bottom Review, the Arizona Democratic Party's Election Integrity Committee supports decertification of all equipment that is not made secure as outlined in your reports for the 2008 election cycle."

Hope is that SoS Debra Bowen talks the talk and walks the walk. I'm impressed with her campaign videos on youtube and Debra Bowen's Voter's Bill of Rights.

[Why Debra Bowen Run for Secretary of State?](#) Time: 01:42 Debra Bowen (D) describes her two biggest reasons for running: Florida and Ohio....bowen diebold Mcpherson California vote Florida Ohio 2000 2004

[Debra's Vision for the Future](#) Time: 02:42 a leader in election reform that will have a positive impact on increasing transparency in every state across the country....bowen diebold mcpherson california democracy

[Debra on Voting Machine Security](#) Time: 01:17 California Secretary of State candidate Debra Bowen (D) on the importance of ensuring voting machine security... bowen diebold mcpherson California

**Auditor John R Brakey, Special Task Force Leader of Arizona Democratic Party Election Integrity Committee
and
Co founder; Americans United for Democracy Integrity and Transparency in Elections - AUDIT-AZ**

Before August 2, 2007; Rev. DeForest Soaries, the first Chairman of the Election Assistance Commission said:

**"We know more today about how to build a machine to take pictures of rocks on Mars than we know about how to build a voting machine to safeguard the American right to vote."
Read what else he has to say:**

<http://www.bradblog.com/?p=3491#comments>

However that has changed do to the Top-to Bottom Review by California's Secretary of State Debra Bowen.

Link to the documents http://www.sos.ca.gov/elections/elections_vsr.htm

"Never doubt that a small group of thoughtful, committed citizens can change the world. Indeed, it is the only thing that ever has."

Margaret Mead



HBO [Hacking Democracy 8 of 9](#) Time: **09:01** this cautionary documentary that exposes the vulnerability of our computer voting systems - which count approximately 80% of America's votes in county, state and federal elections - suggesting that if our votes aren't safe, then our democracy isn't safe either. The documentary, broadcast on HBO throughout November & December 2006, exposes the dangers of voting machines used during America's mid term and presidential elections..



HBO [Hacking Democracy 9 of 9](#) Time: 09:58 On December 13, 2005, Leon County, Florida Supervisor of Elections, Ion Sancho, invited computer experts to try to breach security and hack into a Diebold optical-scan voting system described in a report published on July 4, 2005 by Blackboxvoting.org -- the exact Diebold equipment and memory cards were used in Pima and 11 other Arizona Counties.

- The test refuted specific denials by Diebold.
- Sancho set up the test environment to prove whether or not Leon County's Diebold voting system could be hacked to tamper with an election.
- The outside experts had no password access; the complete canvassing procedure was followed for 8 test ballots.
- The result was that while the 8 paper ballots had a vote tally of 2 Yes and 6 No.
- All of the official reports from the optical scanner on through to the publication of results from the GEMS Central Tabulator - showed an outcome of 7 Yes and 1 No.
- This design defect is illegal and exists on all Diebold "DRE" and "optical scanners".

Thomas W. Ryan Ph.D explained that is INTERPRETED CODE: *"This is code that is readable by humans and modifiable by humans. This is kind of code that is often used by scientists and engineers ...because it is easily modifiable, and should be used ONLY in an experimental environment. It should never be used in any device or system that requires security and [it] is explicitly prohibited by the 2002 Federal Election code."*



[Arizona Election Wars: Pima County: The Gauntlet Is Thrown'](#)

Time 6:57 Part 1 of Series: Powerful letter by Tucson Democratic Attorney Bill Risner to the County Manager on what's been going on with elections in Pima County. Set to a powerful song 'MY VOTE DON'T MATTER ANYMORE' Written and performed by VICTORIA PARKS. For over 2 years we have been investigating Pima County Election Department and we don't like what we've found. They have illegally been printing of election results up to 8

days before the election using the mail in early ballots. This has been going on since the primary of 2004. We know how the backdoor works with the GEMS/Diebold system and how it could be easily hacked using MS-Access. A lawsuit was filed shortly after letter was sent that is basics of this video.



[Arizona Election Wars: Is Our Vote Secure in Pima County?](#) Part 1 of 2 Time Clip 1 of 2: They've known about the backdoor since 1996: Several Pima County bureaucrats from the very top down have known about the backdoor in our voting system. This odd procedure is not found in the 548 page Diebold's User Guide for our voting software, nor does explain that the system is built upon Microsoft Access. Furthermore, by using MS-Access, in less than a minute; a person could switch election by changing two positions in the candidates table (in Access) flipping an election all the way down to the precinct level. This and much more was established in depositions taken by well known Democratic Attorney William 'Bill' Risner in Tucson, Arizona. Clip explains more!



[Arizona Election Wars: Is Our Vote Secure in Pima County?](#) Part 2 of 2 Time 08:00 Clip 2 of 2: They've known about the backdoor since 1996: More clips coming soon.

Auditor John R Brakey, Special Task Force Leader of Arizona Democratic Party Election Integrity Committee (ADP-EIC)
& Co-founder; Americans United for Democracy Integrity and Transparency in Elections - AUDIT-AZ
5947 S Placita Picacho El Diablo
Tucson, AZ 85706
520-578-5678
Cell 520-250-2360
AUDITAZ@cox.net

Before August 2, 2007; Rev. DeForest Soaries, the first Chairman of the Election Assistance Commission said: "We know more today about how to build a machine to take pictures of rocks on Mars than we know about how to build a voting machine to safeguard the American right to vote." Read what else he has to say: <http://www.bradblog.com/?p=3491#comments>

However, that has changed do to the Top-to Bottom Review by California's Secretary of State Debra Bowen. Link to the documents http://www.sos.ca.gov/elections/elections_vsr.htm

AUDIT-AZ's mission: Is to restore public ownership and oversight of elections, work to ensure the fundamental right of every American citizen to vote, and to have each vote counted as intended in a secure, transparent, impartial, and independently audited election process.

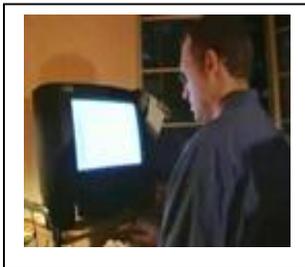
"Never doubt that a small group of thoughtful, committed citizens can change the world. Indeed, it is the only thing that ever has." Margaret Mead



[FOX News Exposes Princeton / Diebold Vote-Reversal Story](#) Time: 03:08
Views: 97,718 News exposes the Princeton report that confirms that **Diebold** machines cannot be trusted in elections....fox news Princeton **Diebold** vote votes reversal fraud hacked hack security election



[Princeton University Exposes Diebold Flaws](#) Time: 09:28 Views: 57,011
Research by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten
See <http://itpolicy.princeton.edu/voting/> for full research, FAQ, and other info. 1. Malicious software running on a single voting machine can steal votes with little if any risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss. We have constructed demonstration software...



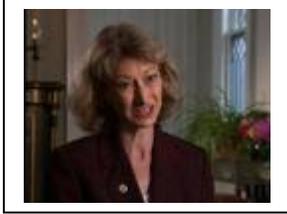
[Hack The Vote \(Part 2\)](#) Time: 04:49 " into **election** machines before an **election** was held in Georgia. A computer programmer admits before Congress he wrote programming code that would "switch" an **election**. "Hack The Vote" is an in-depth look at the still-unsolved problems with electronic voting. Reporter Carter Evans secured the first-ever exclusive on-camera interview with a former employee (now turned whistleblower) of Diebold, one of the companies making these machines. Among the revelations in this series: A whistleblower Chris Hood admits on-camera that he and a team secretly inserted...



[Hack The Vote \(Part 4\)](#) Time 03:45 "Hack The Vote" is an in-depth look at the still-unsolved problems with electronic voting. Reporter Carter Evans secured the first-ever exclusive on-camera interview with a former employee (now turned whistleblower) of Diebold, one of the companies making these machines.



[Rolling Stone : Robert F. Kennedy Jr. "Will The Next Election Be Hacked?"](#) By Robert F Kennedy Jr. Sep 21, 2006 *Fresh disasters at the polls -- and new evidence from an industry insider -- prove that electronic voting machines can't be trusted* According to Chris Hood, Diebold employees altered software in some 5,000 machines in DeKalb and Fulton counties - the state's largest Democratic strongholds. To avoid detection, Hood and others on his team entered warehouses early in the morning. "We went in at 7:30 a.m. and were out by 11," Hood says. "There was a universal key to unlock the machines, and it's easy to get access. The machines in the warehouses were unlocked. We had control of everything. The state gave us the keys to the castle, so to speak, and they stayed out of our way." Hood personally patched fifty-six machines and witnessed the patch being applied to more than 1,200 others.



[Why Debra Bowen Run for Secretary of State?](#) Time: 01:42 Debra Bowen (D) describes her two biggest reasons for running: Florida and Ohio....bowen **diebold** Mcpherson California vote Florida Ohio 2000 2004



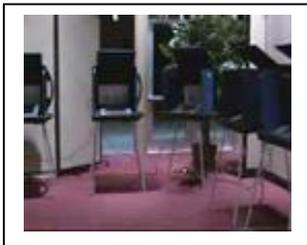
[Debra's Vision for the Future](#) Time: 02:42 a leader in election reform that will have a positive impact on increasing transparency in every state across the country....bowen **diebold** mcpherson california democracy

security...bowen diebold



[Debra on Voting Machine Security](#)
Time: 01:17

California Secretary of State candidate **Debra Bowen (D)** on the importance of ensuring **voting machine** mcpherson California



[Sarasota Elections 2006](#) Time: 04:50 22 showing anomalies in numbers before elections and after elections....Sarasota Florida elections electronic voting machine paper trail black box ES&S **diebold** vote printout Christine Jennings The new Sub SOS of California Lowell Finley was handling this case.



[Election Rigging - how to hack Diebold w/ Howard Dean](#) Time: 02:35 From the HBO movie, Hacking Democracy - Bev Harris of blackboxvoting.org shows Howard Dean how it is possible for anyone with access to the central tabulator computer From the HBO movie, Hacking Democracy - Bev Harris of BlackBoxVoting.org shows Howard Dean how it is possible for anyone with access to the central tabulator computer to alter an election. We need to make sure that this can never happen! Be aware!



[How To Steal An Election](#) Time: 00:46 Do you know what REALLY happened on Election Night 2004? You have no idea. We received this never-before-released promotional video from our good friends at Diebold. It's time to celebrate! Don't think it could happen? Check out these news stories: "Washington Post: It's easier to rig an electronic voting..."



[Another Example of the 1 Minute E Voting Machine Hack](#) CNN Lou Dobbs Time: 03:08 It only takes a minute to steal a US Election!...Vote Voting Fraud Election Elections Scandal GOP Republican Democrat House Senate

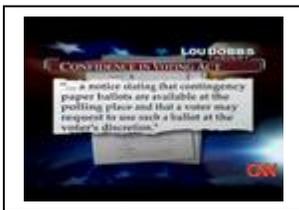


[Lou Dobbs: The dangers of computer voting machines](#) Time: 05:36 Dr. Avi Rubin appears to discuss how computer voting machines (dres) threaten democracy....e-voting computer voting dre diebold avi rubin

be outlawed, and why? have any confidence in electronic voting machines here. Would you make the belonging to the political party you are *not* affiliated with,



[Should e-voting machines be outlawed?](#) Time: 01:16 still have any confidence in these machines. Should electronic voting machines Leave Jack Cafferty, on CNN, asks if we still these machines. <http://www.cnn.com/CaffertyFile> Should be outlawed, and why? Leave your comments same choice if you knew a malicious hacker, knew how to alter the outcome?



[Want to Vote on Paper on November, 2006?](#) CNN Lou Dobbs Time: 01:55 gives voters the option of using paper ballots on November 2006....Dodd Holt Boxer Feingold Kerry amendments HAVA Legislation Senate Congress ballot paper election **Diebold**



[Diebold Ballot Boxes Will Be 100% Hackable](#) CNN Lou Dobbs Time: 00:32 Princeton University studied **the security** a popular electronic voting machine by **Diebold**. Their study, titled "**Security Analysis of the Diebold Accuvote-TS Voting Machine**" A new study e-voting finds results the midterm elections can not be trusted. The Center for Information Technology Policy at Princeton University studied the security a popular electronic voting machine by Diebold. Their study, titled "Security Analysis of the Diebold AccuVote-TS Voting Machine", and...



FLORIDA DEPARTMENT OF STATE

CHARLIE CRIST
Governor

KURT S. BROWNING
Secretary of State

July 31, 2007

Mr. David Byrd
Diebold Election Systems
PO Box 1019
Allen, Texas 750133

Dear Mr. Byrd:

As Chief Elections Officer, it is my responsibility to insure fair, accurate, secure, and uniform elections in Florida. On May 15, 2007, the Department of State contracted with Security and Assurance in Information Technology (SAIT) Laboratory at Florida State University to review documented, published issues with the Diebold Accuvote OS and the TSx, currently in the voting systems certification process in Florida.

SAIT Lab released its findings in a report to the Department of State on Friday, July 27, 2007. Based on the report, the Bureau of Voting Systems Certification has determined that certain vulnerabilities outlined must be corrected by August 17, 2007, to continue this certification. Failure to do so will result in a denial of certification. Please see the attached document for the required corrections.

It is my understanding that Diebold is currently making corrections to the optical scan firmware that will address issues contained in the SAIT Lab report. When an amended firmware version for the Accuvote OS has been submitted, we will move forward to resume the testing and certification process. As it pertains to the touchscreen, we will not certify the system with this application. However, we will work with you to resolve the issues with the TSx prior to your next application in October. This certification schedule will provide time for Diebold counties to upgrade the firmware for currently certified optical scan and touchscreen machines prior to the Presidential Preference Primary.

Although there are numerous issues listed in the report, many are administration in nature or pose no security risk. Upon certification, the Division of Elections will be issuing a technical advisory to the Supervisors of Elections who use the Diebold voting system. The advisory will outline suggested additional election and security procedures to mitigate the administrative issues outlined in the report. We will forward a copy of that advisory to your office for your information.

Division of Elections

R. A. Gray Building, Room 316 • 500 South Bronough Street • Tallahassee, Florida 32399-0250
Telephone: (850) 245-6200 • Facsimile: (850) 245-6125
election.dos.state.fl.us

Mr. David Byrd
July 31, 2007
Page 2

Please do not hesitate to contact the Director of the Division of Elections, Amy K. Tuck, if you have further questions or concerns regarding this correspondence or the SAIT Lab report. The Division will be contacting your office regarding the implementation of the modifications to these issues.

Sincerely,

A handwritten signature in black ink, appearing to read "Kurt S. Browning". The signature is fluid and cursive, with a large initial "K" and a long, sweeping tail.

Kurt S. Browning
Florida Secretary of State

Attachment

Division of Elections

R. A. Gray Building, Room 316 • 500 South Bronough Street • Tallahassee, Florida 32399-0250
Telephone: (850) 245-6200 • Facsimile: (850) 245-6125
election.dos.state.fl.us

Attachment A

The following numbering system corresponds to the final report as provided by Security and Assurance in Information Technology Laboratory.

Required changes:

3.5 The Signature Flaw

The vendor's RSA signature verification is insecure (RSA is an algorithm for public-key cryptography). Signature comparisons generated with this method can be forged. The comparison employs what is called a SHA1 hash. The SHA1 hash entails 160 bits, which means that when the signatures are verified, only the 160 bits are verified and the remaining 1888 bits are not examined. Leaving these bits outstanding and not verified allows for a vulnerability for forgery attacks. This must be fixed in the certification to employ a standardized, widely accepted mode for public key verification. This will also be addressed in administrative procedures at the local level.

3.8.1.4 Attacker Can Hide Preloaded Votes

The system must mitigate the original published attack regarding preloaded votes with the changes in the RSA signature correction (see 3.5). However, because the memory card is not encrypted or authenticated it is still possible to load votes on a memory card. Election officials need to continue to restrict access to removable media and secure audit logging techniques should be employed.

3.9.1 AccuBasic Scripts Can Be Misused

The system allows AccuBasic code to perform conditional operations based on comparisons of data for such things as time, candidate names and other data. This might allow an attacker to hide exploits by manipulating this conditional data. The issue lies with the signature verification, which must be corrected in the certification (see. 3.5).

3.9.5 Unchecked String Operation: Allows Overwrite of Stack Memory

The unchecked string operations still exist in the code, other corrections in the software have already mitigated this vulnerability. This issue must be addressed and changed in the certification.

Administrative Procedures:

3.6 Optical Scan Memory Card Is Not Integrity Protected (see 3.8.1.4)

The data on optical scan memory cards is not encrypted or authenticated (except for the insecure signature on the AccuBasic script). This vulnerability can lead to potential attacks. Administrative procedures must be employed at the local level to limit access and possible exploitation.

3.8.1.1 Leaks Memory Card Contents

An attacker can copy the memory card contents to a laptop by connecting the laptop to the optical scanner. The attacker would turn the machine on, enter diagnostic mode by simultaneously hitting the “yes” and “no” buttons and selecting a menu option to dump the memory card’s contents. The current method to copy memory card contents is to allow one to use the “yes” and “no” buttons. Elections officials must monitor access to the optical scan machine through local security procedures.

3.8.1.2 Supervisor PIN Not Cryptographically Protected

Diebold uses a method for shuffling the supervisor’s PIN using the memory card’s key. Thus, someone with access to the memory card and reader and knowledge of the shuffling algorithm can determine the PIN. Election officials must maintain security procedures over the voting terminals and the removable media.

3.8.1.5 Vote Counters Are Not Directly Checked for Overflow

Candidate ballot counters are protected from overflow by a total ballot counter. These individual candidate vote counters can hold as many votes as the total ballot counter, so there should be no overrunning of all vote counters. Consistency checks have been implemented so that possible exploitation of this flaw is prevented. Election officials must also strictly monitor access to both the optical scan machines and the memory cards.

3.10.1 AccuBasic Scripts Are Not Authenticated on the GEMS (Global Election Management System) Server

GEMS itself does no checks to the AccuBasic byte code because the system relies on the RSA signatures to verify the code. The corrections made to section 3.5 (above) will correct the signature verification issue. In addition, the elections officials must restrict access to the GEMS server.

3.10.2 Password Does Not Protect Access to GEMS or Audit Logs

The GEMS password authentication process can be defeated in what is a publicly known attack. In order to mitigate against this attack, election officials must protect access to

GEMS servers and must never connect GEMS servers to the Internet or an untrusted network.

No Security Threat:

3.8.1.3 No Authentication Between GEMS and the Terminal

The written code provides for mutual authentication between the GEMS (election management) server and the optical scan terminal. However, the concern on this validation is if devices were to connect via the Internet. In Florida, there is no interaction with the Internet.

3.9.1 Error Checking is Inadequate

The system does not provide descriptive display prompts as to encountered errors. The prompts merely notes that it “does” or “does not” work. The issue raised is that without these prompts, an attack might not be noticed. However, it has been determined that the error messages are capable of being printed out for use by trained, technical staff. The actual display only notices that it “does” or “does not” work to prompt poll workers, who would then contact elections officials staff.

3.9.2 Error Codes Returned by the AV-OS System are Ignored

The system returns a status code indicating the success or failure of script interpretation. The function that provides this return value is present in the code, but does not require further action. All errors are reported within the Abasic processing which is inside the system and can be accessed and reviewed.

3.9.4 Public Key Hard-Coded into the Source

Embedding the public key in the source code does not pose a direct security problem. However, having the public key hard-coded into the source code prevents the vendor from routinely changing the public/private key pair. This is a trade-off because the key cannot be changed by the election official, but also cannot be changed by anyone else.

From: blcroll
Sent: Wednesday, August 01, 2007 12:36 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

We voted for Ms. Bowen because we were concerned about the state of our most precious right. Now our worst fears have come to light, I urge Ms. Bowen to immediately de-certify all of the machines and instead look into alternative ways to count votes that are transparent and open to audit.

Remember, as Stalin said, "The people who cast the votes decide nothing. The people who count the votes decide everything."

Ms. Becky Croll

From: susanmanetas
Sent: Wednesday, August 01, 2007 12:37 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mrs. Susan Manetas

From: Adrienne Kligman
Sent: Wednesday, August 01, 2007 8:47 AM
To: Voting Systems
Subject: Thanks/decertify vote machines

Thank you for conducting the "Red-Team" review, and please rid of the vote machines that do not meet reasonable security standards.

Thank You,
Adrienne Kligman

From: kaye547
Sent: Wednesday, August 01, 2007 12:39 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Dear SOS Bowen: Thank you, thank you, thank you. This is one of the most important issues facing our democracy today. Stand strong. You are right. In fact, we need paper ballots and hand counting to be sure our votes actually count.

Thank you again!

Ms. Kaye Peters

California Secretary of State
1500 11th Street
Sacramento, California 95814

Greetings;

Well I see that you tested the electronic voting machines digital security and found it wanting. Some statements did try to reassure everyone that they will be secure when they are used. That reassures me not at all.

I would be willing to bet that even when used as designed within the security surrounding the voting system there are many ways the vote can be altered. In fact there are even ways that do not even require that the Black Hat touch the voting machine. Ways that exploit weaknesses inherent in any computer and that could be used to alter the vote. And there is also Mother Nature....

One: Power is the most obvious. Will each precinct have backup power capable of running the voting machines for the entire polling day? How about protection from nearby lightning strikes? I have my doubts. A paper ballot needs no power and does not conduct electricity.

Two: Water is the enemy of computers. A leaky roof in a precinct or the trucks transporting them can damage the voting machines. Even a once wet paper ballot might well be countable.

Three: Could a cell phone sized device be created that could create a sufficiently powerful electromagnetic pulse that would damage the voting machine? I suspect the answer is yes. Paper ballots are immune to electronic interference.

Four: You only tested the machines themselves, but not the security of the system wherein they are stored, configured, distributed, used, collected and tallied. Can you honestly say their security is perfect? Paper ballots are much harder to "hack".

Because of these issues and others I am sure that we can both think of, I do not intend to vote using an electronic voting machine. I will ask the County Registrar of Voters to remove me from the voter roles before that, and will let both of you know why in no uncertain terms. And I have voted in virtually every election since 1972.

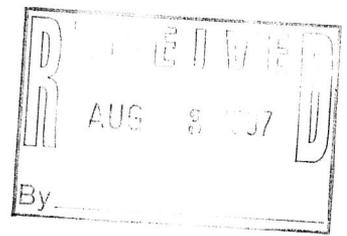
Quite Sincerely;



Keith B. Rosenberg

31 JULY 2007

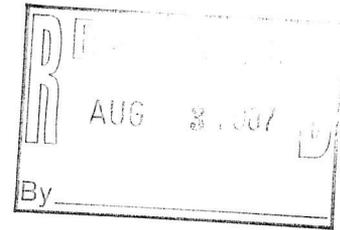
JULY 30, 2007



DEAR MS.BOWEN,
THANK YOU SO MUCH FOR INVESTIGATING THE CROOKED COMPUTER VOTING MACHINE COMPANIES. IT HAS BEEN SO OBVIOUS TO ME FROM THE BEGINNING THAT THESE MACHINES WERE EASILY COMPROMISED AND OUR VOTES JUST AS EASILY STOLEN. I AM LOSING ALL TRUST AND CONFIDANCE IN MY NATIONAL AND STATE GOVERNMENT'S ABILITY AND WILL TO PROTECT THE SANCTITY OF OUR VOTES. PLEASE DO NOT APPROVE THE DIEBOLD AND TWO OTHER COMPANIES' INSISTENCE ON USING THEIR CRIMINAL MACHINES IN ANY MORE ELECTIONS. I NOW VOTE ONLY WITH MAIL- IN BALLOTS AND I STILL HAVE LITTLE FAITH THAT THEY ARE COUNTED.
PLEASE RESTORE MY CONFIDANCE IN OUR ELECTION PROCESS. I WOULD PREFER A PAPER BALLOT.

SUSAN KAEFER, P.T.

The Honorable Debra Bowen
Secretary of State, California
1500 11th Street
Sacramento, CA 95814



The Honorable Secretary of State:

August 1, 2007

As someone who campaigned for you in the last election, I am pleased to write to you strongly supporting your efforts to require that ALL voting machines be tested, especially in light of recent evidence that such equipment is subject to tampering and manipulation. Election protection and the right to vote are FUNDAMENTAL to the democratic process. I am also aware that manufacturers of voting technology that do not have independent verification by means of a paper trail or review of the computer source codes have been used to benefit the Republican Party in closely contested elections. That observation is not a partisan statement but rather an affirmation of the need for an accurate vote tally, regardless of outcome.

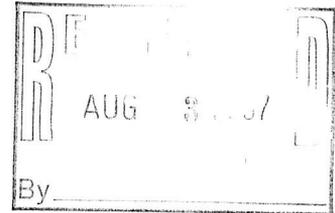
Please continue to stand firm on the issue of election protection in every way.


Gene Rothman

310-398-1414

07/31/07

Honorable Debra Bowen
California Secretary of State



Honorable Debra Bowen,

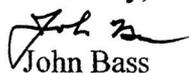
Thank you for your leadership in initiating the top to bottom review of California election systems. I was unable to attend the public hearing on Monday 07/30/07 due to work and family obligations. I have served as a precinct inspector for several elections in Alameda County and as a precinct coordinator. I have been serving on the Alameda County election advisory committee since its inception. In my opinion, it is well overdue to decertify all DRE (direct recording electronic) machines in the state of California.

Currently, the Registrar of Voters are dependent on the corporate vendors to run elections in California. They tend to trust the grossly inadequate system of federal testing and the vendors public relations. They tend to discount valid criticism through stating "it can't happen", "won't happen" or "didn't happen here" or conveniently forget when it did happen when it comes to problems with electronic voting. An example would be the re-call election of 2003. An article in the San Jose Mercury on Feb 1st 2004 stated in part "For an unknown reason, the computerized tally program had begun to award votes for Lt. Gov Cruz Bustamante to Burton, a socialist from Southern California. Similar mishaps have occurred across the country ever since election officials have embraced electronic voting in the wake of the Florida vote-counting debacle of 2000." That incident happened in Alameda County but, I have yet to hear the Registrar of Voters past or current acknowledge this incident in a public forum or give explanation on how it happened and how it has been rectified. There was a grand jury investigation in Alameda County in regard to the use of uncertified patches in the use in that election. The conclusion was to refer to the Secretary of State. Please do the will of the people and secure accuracy, transparency and accountability in all elections in the State of California. It is a terrible feeling as a voter to not know who really won and if your vote was counted as intended. It is even worse as a citizen to wonder if we truly live in a democracy.

I request the following four items as soon as possible:

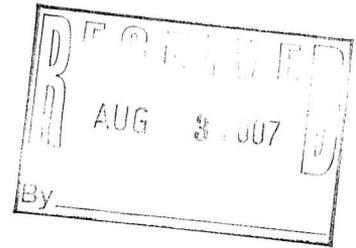
- 1) to outlaw the use of DREs in California elections with or without a paper trail immediately.
- 2) to conditionally certify ballot marking devices (BMD) for California use as soon as possible
- 3) to direct the Attorney General of the State of California to initiate new fraud cases on behalf of the voters of California in terms of breach of contract(s), the use of "uncertified patches" into election counting devices, failure to meet basic standards of a viable VVPAT, and failure to adequately keep voting records.
- 4) to initiate your office to work with the University of California and interested non profit organizations to develop and maintain an open source opti-scan vote counting system with a ballot marking device and precinct sorter that can be made available to the California counties and municipalities.

Sincerely,


John Bass

*Thank you!
This is a hand
copy of the letter
sent electronically
on 8/01/07.*

Deborah Bowen
California: Secretary of State
1500 11th Street
Sacramento, California
95814



REF: Voting Machine Certification

Greetings and Salutations,

Please accept my words in the spirit offered. I have always considered "The right to vote" as the "Holy Grail" of all republic and democratic forms of Government.

The notion of allowing private groups and corporations without 100% transparency, at every level, in every detail is liken to inviting a fox, carrying good intentions, into the chicken house. This idea which politicians seemed to have embraced is unsavory and offensive, to say the least.

O.K Enough, I got it. It is not my intent to rehash old mistakes and complaints. However, the fox is now inside the chicken house. So what do we do with him? I suggest that any and all vendors and voting machines that do not allow 100% transparency at every level of interrogation as suspect, and by obvious default, not engaged in the greater good of the people of the state of California.

Arguments against the surrender of proprietary source codes to appropriate state auditors, public inspection, and public verification, only holds water in the world of private enterprise. These same arguments against, are not acceptable credentials in an unfettered election process. By the rule of law, if there exists one, and if not, there should be one. The only secret that should be kept in an election is the identity of the voter.

Whatever portion that is suspect, of the whole process, that is proved to be unacceptable, should be enough to reject the overall use benefits of the entire system.

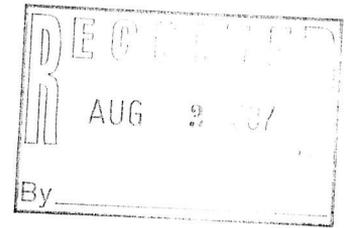
Plain and simple, VERITAS! No proof, no certification.

P.S. If you should require anything else of me beyond this letter, I happily await your ideas and requests.

TAX.
The Clark Family

Clark

July 30, 2007



Esteemed Secretary of State Bowen:

Thank you for your efforts to examine all the voting machines.

Now that we know that they can all be hacked and that there people willing and able to hack them, it is time to ban them! All elections should be decided by paper ballots that are counted, preferably by hand.

It is important to get the results right, even if it takes a little longer.

Again, thanks,

A handwritten signature in cursive script that reads "Steve Eklund".

Steve Eklund

From: Pandaeus, Rene
Sent: Wednesday, August 01, 2007 8:48 AM
To: Voting Systems
Subject: In support of SOS Debra Bowen's electronic voting machine audit

To Whom It May Concern:

Anything computerized can be hacked into. I believe when it comes to voting – all votes should be done the 'old-fashioned' way by punching a hole in the voting cards.

I sincerely believe that the 'punch card' way is the only accurate way for our votes to be properly accounted for.

RENE PANDAEUS

LPA

From: peselwyn
Sent: Wednesday, August 01, 2007 12:37 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Please ensure that only those voting machines that are absolutely secure are used in the next election!

Ms. Pamela Selwyn

From: Margaret Costello
Sent: Wednesday, August 01, 2007 8:50 AM
To: Voting Systems
Subject: Voting Systems

Thank you for your review of the electronic voting machines. I believe they are expensive and untrustworthy. It puts voting in the hands of private corporations that are not accountable to the voters. In Ohio they did not provide enough machines in poor neighborhoods during the 2004 presidential election. When fraud was suspected evidence was easily destroyed. I believe these machines are an institutional way to disenfranchise poor voters. Please make them go away. It is a tough decision you have to make. Please make the brave choice.

Thank you.
Margaret Costello

From: nancydqc@starstream.net [mailto:nancydqc@starstream.net]
Sent: Wednesday, August 01, 2007 12:41 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Thank you for keeping our elections honest and fair.

Ms. Nancy Droese

From: nancydqc
Sent: Wednesday, August 01, 2007 12:41 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Thank you for keeping our elections honest and fair.

Ms. Nancy Droese

From: Todd's Junk
Sent: Wednesday, August 01, 2007 8:51 AM
To: Voting Systems
Subject: Red Team review -- please decertify!

Dear Secretary of State Bowen --

Thank your for initiating the important "Red Team" review of California's voting machines. Your bold actions on this front have made California an example to the rest of the country in terms of how to deal with the voting crisis.

In light of the disappointing -- but predictable -- results of the review, your only viable course of action is to decertify these machines. I realize this may be an expensive proposition, but the threat of the public losing faith in the voting process is infinitely more expensive.

The solution is quite simple: despite an unsubstantiated conventional wisdom that they are prohibitive here in the United States, paper ballots seem to work quite well all over the world.

Alternatively, if electronic voting is absolutely necessary, a voter-verified paper backup is a must, and these backups must be counted subsequent to the certification, to verify the result. Again, quite simple.

I can travel to New York and use a machine to withdraw cash from a bank account in Los Angeles. The machine gives me a record of the transaction on paper, which I can then check against the bank's records when I receive a statement. If this sort of thing can take place millions of times a day without a hitch, then there is no

excuse for the cloud of doubt that currently hangs over our electoral system.

Sincerely,
Todd Slater

From: vjbn3@earthlink.net
Sent: Wednesday, August 01, 2007 12:43 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. VAROUJ JOHN JEBIAN

From: John Bass
Sent: Wednesday, August 01, 2007 8:52 AM
To: Voting Systems
Subject: public comment submission

07/31/07

Honorable Debra Bowen

California Secretary of State

Honorable Debra Bowen,

Thank you for your leadership in initiating the top to bottom review of California election systems. I was unable to attend the public hearing on Monday 07/30/07 due to work and family obligations. I have served as a precinct inspector for several elections in Alameda County and as a precinct coordinator. I have been serving on the Alameda County election advisory committee since its inception. In my opinion, it is well overdue to decertify all DRE (direct recording electronic) machines in the state of California.

Currently, the Registrar of Voters are dependent on the corporate vendors to run elections in California. They tend to trust the grossly inadequate system of federal testing and the vendors public relations. They tend to discount valid criticism through stating "it can't happen", "won't happen" or "didn't happen here" or conveniently forget when it did happen when it comes to problems with electronic voting. An example would be the re-call election of 2003. An article in the San Jose Mercury on Feb 1st 2004 stated in part "For an unknown reason, the computerized tally program had begun to award votes for Lt. Gov Cruz Bustamante to Burton, a socialist from Southern California. Similar mishaps have occurred across the country ever since election officials have embraced electronic voting in the wake of the Florida vote-counting debacle of 2000." That incident happened in Alameda County but, I have yet to hear the Registrar of Voters past or current acknowledge this incident in a public forum or give explanation on how it happened and how it has been rectified. There was a grand jury investigation in Alameda County in regard to the use of uncertified patches in the use in that election. The conclusion was to refer to the

Secretary of State. Please do the will of the people and secure accuracy, transparency and accountability in all elections in the State of California. It is a terrible feeling as a voter to not know who really won and if your vote was counted as intended . It is even worse as a citizen to wonder if we truly live in a democracy.

I request the following four items as soon as possible:

- 1) to outlaw the use of DREs in California elections with or without a paper trail immediately.
- 2) to conditionally certify ballot marking devices (BMD) for California use as soon as possible
- 3) to direct the Attorney General of the State of California to initiate new fraud cases on behalf of the voters of California in terms of breach of contract(s), the use of "uncertified patches" into election counting devices, failure to meet basic standards of a viable VVPAT, and failure to adequately keep voting records.
- 4) to initiate your office to work with the University of California and interested non profit organizations to develop and maintain an open source opti-scan vote counting system with a ballot marking device and precinct sorter that can be made available to the California counties and municipalities.

Sincerely,

John Bass

From: Jill Burrows
Sent: Wednesday, August 01, 2007 8:52 AM
To: Voting Systems
Subject: Thank you for protecting our vote

Dear Secretary of State Bowen. Thank you for reviewing the voting systems in California. Research shows that OpScan (which provides a paper ballot) is preferable to the touchscreen systems which have proprietary software and are easily hacked. The sanctity of our vote is paramount to our democracy and we need all of the Secretaries of State to perform their duties and put in place a voting system which is reliable, has a paper ballot, and is not in the hands of private corporations. Again, thank you for taking seriously this public trust. Sincerely, J.C. Burrows

From: Leilani
Sent: Wednesday, August 01, 2007 8:52 AM
To: Voting Systems
Subject: Red Team Review-Voting Machines

Dear Debra Bowen,

Thank you for conducting the "Red-Team" review of the major vote machines used in California. This is critically important to "We, the People". Without a real vote, we have only the illusion of a democracy.

Please do not allow these insecure, hackable vote machines to be used in your State. It is obvious to the Public that these machines with massive security flaws were created intentionally to manipulate the outcome of the election in favor of those in power, namely, Republicans, or those that stand with Corporate power and money. No wonder California has a Republican Governor! Hmmmmmm.

I live in Washington State, and very quickly the whole State was switched to Mail-in Ballot. California could do this for the 2008 Election. Please don't use these insecure machines that can corrupt the vote and our government. The Mail-In Ballot is simple, re-countable, secure.

Thank you for your good work!

Leilani Macmillan

From: Peggy
Sent: Wednesday, August 01, 2007 8:54 AM
To: Voting Systems
Subject: voting machines

Dear Debra,

Please hang tough. If we don't hold the voting machine manufacturers/suppliers accountable, the owners' of these companies and their political sponsors will be running roughshod over all of us from now on.

Regards.

Peggy Midling

From: Faith Voigt
Sent: Wednesday, August 01, 2007 8:55 AM
To: Voting Systems
Subject: Voting machines

Wonderful that somebody is at last taking steps to end this utterly corrupt system.

The rest of the world has difficulty comprehending how any American can presume to monitor voting in other lands when the electoral college system guarantees twisted results - and voting machines are installed to ensure that nobody shows up because their opinion won't be counted anyway.

Best of luck to you, stay strong and restore our faith in the American people.

Sincerely,
Faith Voigt (Brit resident in Germany)

From: Thomas Ryan
Sent: Wednesday, August 01, 2007 8:56 AM
To: Voting Systems
Subject: CA Voting System Analysis

First, I want to commend SoS Bowen for conducting the thorough review of CA election systems. This kind of analysis is long overdue. She has provided a critical national service.

Second, I want to encourage SoS Bowen to

- A) release **all** reports stemming from the study so that the public has a complete view of the hardware and software problems associated with these voting machines,
- B) decertify any machines that cannot be properly audited and pose a risk to upcoming election integrity,
- C) augment the state's auditing requirement to a point where reasonable assurances can be made that elections are accurate,

Tom Ryan, Ph.D.
Arizona Citizens for Fair Elections

From: GENE DERIG
Sent: Wednesday, August 01, 2007 8:58 AM
To: Voting Systems
Subject: Voting Machines

Dear Secretary of State Bowen:

We are not residents of California, but we are citizens of this nation who are very concerned about our voting system and the disarray it is in.

THANK YOU from all of us in this country for conducting the "Red Team" review. That was for the USA, not just California. What California does has huge impact on all of us. Here in Washington State we are correcting voting problems too.

"Vote privately, count publicly" is a motto we like. The machines are merely vote theft waiting to happen. To paraphrase Joe Stalin: "The votes aren't important. Who counts the votes is what is important". Chilling words, I believe.

Thanks again for having the review. Watching from up here we hope you dump the machines and get credibility back in the system.

Our best to you,

Gene and Marilyn Derig

From: Scott Bishop
Sent: Wednesday, August 01, 2007 9:04 AM
To: Voting Systems
Subject: Vote Integrity First

I don't have all the facts, but from what I have heard you have to take some difficult actions. Please do the right thing to protect the integrity of the most fundamental mechanism of our American democracy - the vote. I think you should be listening to the Apollo Alliance folks (<http://www.apolloalliance.org/>) not any part of corporate America. Profits are what corporations are for, not good government by/for/of the people.

I hope we can trust you... -Scott

From: Bureau of Public Secrets
Sent: Wednesday, August 01, 2007 9:04 AM
To: Voting Systems
Subject: Decertify

Please decertify all voting systems that have not passed rigorous inspections. Anything less is capitulating to possible, and in fact likely, fraud.

Ken Knabb

From: pamela cahill
Sent: Wednesday, August 01, 2007 9:05 AM
To: Voting Systems
Subject: voting

Debra Bowen,
Thank you for your courageous attempt to keep our voting system honest.
Please keep up the good work. You our fighting for the millions of
us
who can not and are not able to fight for ourselves.
Sincerely,
Pamela Cahill

From: Monica Mccabe
Sent: Wednesday, August 01, 2007 9:06 AM
To: Voting Systems
Subject: Voting systems

Thank you for reviewing our voting systems. We need a paper trail to keep everyone honest.

Monica McCabe

From: gangadevi
Sent: Wednesday, August 01, 2007 9:06 AM
To: Voting Systems
Subject: Preserve Our Vote

Thank you Debra Bowen.

With so many of our constitutional rights suspended, the only link we have with our democracy now is our vote. As already shown in elections back to 2000, the counting of them is highly suspect.

Please call for paper ballots or printed vote. If an ATM machine can readily spit out a receipt, a voting machine can do the same.

Demand our right to fair elections.

Cordially,
Allen Taylor

From: Robert Weeks
Sent: Wednesday, August 01, 2007 9:08 AM
To: Voting Systems
Subject: Voting Machine Review

Good Morning Secretary Bowen,

Your election to Secretary of State of California was the election result I was most pleased with when it occurred, because the integrity of our voting procedures is the single most important issue before us in California and in many other states. If the election process cannot be trusted then we cease to live in a democracy and it is only a matter of time before the American people have nothing but scorn and contempt for the electoral process.

Thank you so much for pushing for the recent review of the various voting machines. Thank you for being a champion of voting integrity. You will always have my vote. I hope that you can continue to fight for our voting rights.

Thanks again,

Robert Weeks

From: Justice Through Music
Sent: Wednesday, August 01, 2007 9:14 AM
To: Voting Systems
Subject: Please decertify these machines

I am so upset at the votemachine companies, lying to state officials to get these contracts, deceiving the public, harming democracy and doing this to make an extra buck. I want you to hit these companies as hard as possible. Decertify the machines and don't let them come back until they build a machine from the ground up that does the job on all fronts.

And thank you for ordering the review and calling them to task.

Brett Kimberlin

From: Kosta Gus Makreas
Sent: Wednesday, August 01, 2007 9:11 AM
To: Voting Systems
Subject: Let's Get Back to Paper ballots - 'NO' to flawed electronic voting systems

Hello Secretary of State Bowen,

THANK YOU for conducting the review of the major voting machine vendors!

I am an advocate of free and fair elections, so this review is important. I am not surprised that security flaws were uncovered.

Please do **not** certify any of these vendors, either conditionally or unconditionally.

Let's just get back to PAPER BALLOTS and forget the electronic methods. I am a software engineer with 30 years experience, so I know how flawed the vote-counting software is. My whole family and many friends are aware of paperless system problems (yeah, I've been informing them) and now also advocate for a return to the more verifiable, original paper ballots.

California will lead the way back to restoring our Democracy. You have a unique and powerful responsibility to help this by getting us back to Paper Ballots.

Thank you,

Gus Makreas

From: Mike VanLandingham
Sent: Wednesday, August 01, 2007 9:11 AM
To: Voting Systems
Subject: Thank you

Thank you for the Red Team review.

Please make sure that everyone's vote counts !

From: kbeckel@peoplepc.com
Sent: Wednesday, August 01, 2007 9:13 AM
To: Voting Systems
Subject: decertify

Please decertify all faulty voting machines and those with no paper trail.

From: Mickey Shell
Sent: Wednesday, August 01, 2007 9:14 AM
To: Voting Systems
Subject: Gratitude

Thanks for all the work you're doing on behalf of the electorate (and the remains of our democracy). You folks who take on this enormous task are amazing. Just wish the Democrats in Congress were as urgently aware and concerned, because what good is all the work they're doing if they lose their leverage in the next election?

Mickey Shell

From: Anne Barga [mailto:annebarga@charter.net]
Sent: Wednesday, August 01, 2007 9:14 AM
To: Voting Systems
Subject: voting machines

Dear Ms. Bowen,
Thank you for your work in reviewing voting machines.
Please help us to feel secure at our polling places that our votes are recorded accurately by correcting the massive security flaws that were found to exist currently. This is of utmost importance to our democracy and the future of our great Nation.
Thank you,
Anne Barga

From: Beverly
Sent: Wednesday, August 01, 2007 9:15 AM
To: Voting Systems
Subject: kudos

for standing up to the Diebolds ... these election machine companies have shown that they cannot be trusted!

From: Scott Mahood
Sent: Wednesday, August 01, 2007 9:16 AM
To: Voting Systems
Subject: voting machines

Say "NO!" to Diebold. Bring back the paper ballot.

From: dael4
Sent: Wednesday, August 01, 2007 9:16 AM
To: Voting Systems
Cc: evan davis; J30@yahoogroups.com
Subject: Finally to the bottom of the election debate

Thanks for uncovering the truth in the electronic voting systems and how fragile they really are. These machines are not what we need to build the foundation of our Democracy on.

In Ohio, we are faced with the threat that, many counties have destroyed ballots from the 2004 election though many had ballots stored from elections held many years prior.

This is serious business and just as serious is the prosecutorial action. Why do you think they wanted to change the federal attorneys?

I really believe that the time is now to act against any intentional election fraud or mismanagement of the voting process. These actions against democracy must not stand.

I have been close to those here in Ohio uncovering mounds of evidence in election malfeasance from precinct to precinct. I have worked tirelessly to promote the reality of our current system online, helping both Paul Lehto and Dr. Robert Fitrakis in my small way.

Please see:

www.fraudbusterbob.com

<http://neocon-panic-attacks.blogspot.com/> (please look at label list for election related articles)

Stephen Caruso

From: Angela Worden
Sent: Wednesday, August 01, 2007 9:17 AM
To: Voting Systems
Subject: Thank you for caring about the security of our voting system

Debra Bowen,

Thank you for caring about the security of our voting machines. Voting is one of the most important things we do as citizens of a democracy/ republic. You didn't ask me, but I think you should decertify the machines. The integrity of voting is dependant on the security of these machines. Perhaps we need to go back to paper ballots.

Angela Worden

From: snickels
Sent: Wednesday, August 01, 2007 9:19 AM
To: Voting Systems
Subject: Voting Integrity

Stephen Nickels
2880 Trigg Tower
Simpson Illinois 62985
snickels@shawneelink.net

What could be more important than knowing my vote will count, as I intended. Will California lead the Country in requiring all voting machines to be tamper proof? I hope so. Thank you for your time.
Peace & Impeachment,
Stephen

From: Dominick
Sent: Wednesday, August 01, 2007 9:17 AM
To: Voting Systems
Subject: voting machines

Dear Secretary of State Bowen,

I voted for you for many reasons and one of those reasons was that you were going to bring back integrity and honesty back to our voting system. Thank you for conducting the "Red-Team" review.

BUT, and don't you just love it when there is always a BUT?

Please GET RID of all computer generated voting machines. Even if they do leave a paper trail most of these machines can be compromised to change the tallies and Not ever be found out, even with a paper trail, especially with the sophisticated virus programs that are now out there.

Why take that chance to compromise our biggest right ever with the chance that our votes can be tampered with?

Thank you for taking the time to listen to me.

**Sincerely,
Dominick J. Di Noto**

From: Mark
Sent: Wednesday, August 01, 2007 9:17 AM
To: Voting Systems
Subject: Red Team review comment

Dear Deborah Bowen,

I wanted to thank you for conducting the red team review on the four types of voting machines in California. The results I understand indicate quite a few security flaws.

To my knowledge ATM machines are pretty secure but I heard they are 10-20 times more expensive than a single voting machine. Until we can put that much money into a single voting machine to make use it is secure we need go back to a paper ballot system of fill in the spaces or a punch system that leaves a definite verifiable trail.

I would urge you to decertify all of the current electronic voting machines.

Thank you,

Mark

From: Jill Levy
Sent: Wednesday, August 01, 2007 9:21 AM
To: Voting Systems
Subject: Voting machine review

To Debra Bowen,

Thank you so much for the "Red-Team" review! Given that all 4 voting machines were found to have massive security flaws, I feel strongly that they be decertified and another system be put in place. How about a return to the old pre computerized machines that seem to be straight forward and honest?

Sincerely,

Jill Levy

From: Lee Eisenberg
Sent: Wednesday, August 01, 2007 9:23 AM
To: Voting Systems
Subject: voting machines

While I am not a Californian, I consider it a good idea that you are asking for public comments about the topic. Public input is an essential part of democracy.

Lee Eisenberg
Portland, Oregon

From: leipham
Sent: Wednesday, August 01, 2007 9:22 AM
To: Voting Systems
Subject: Safeguard the election process

Please "de-certify" all of the electronic voting machines that are corruptible- including the optical scan machines. We need to have a voting system with a paper trail that is verifiable. I support you in protecting our voting rights.

Kathy Leipham

From: Linda [mailto:lindaseeley@charter.net]
Sent: Wednesday, August 01, 2007 9:25 AM
To: Voting Systems
Subject: Thank You

Thank you so much for watching out for our voting rights. We cannot use voting machines that are hackable! It is absurd. We need paper ballots with bipartisan monitored counting of the votes, just like we used to have.

Thanks again,
Linda Seeley

From: dnsbyrne
Sent: Monday, August 06, 2007 5:12 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. Dennis Byrne

From: maggie_evans
Sent: Monday, August 06, 2007 1:52 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

I hope this email is not too late and that my voice will count in the decision about using flawed voting machines. I can only ask that a decision be made that will protect the voting rights of citizens of California. Representative democracy is in peril at all levels. Please make a sound judgement that prevents deceit and lawlessness.

Ms. Maggie Evans

From: lonly
Sent: Monday, August 06, 2007 3:57 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

If the votes aren't accurately monitored and counted, we are no longer a democracy.

Ms. Lola Bice

From: b-lus-no
Sent: Monday, August 06, 2007 3:37 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. William Yeo

From: David Harris
Sent: Monday, August 06, 2007 11:28 AM
To: Voting Systems
Subject: Great Gratitude

Please Please Please See the Debra Bowen is thanked for being courageous and saving democracy. We are counting on her integrity.

David J. Harris Founder The Health Optimizing Institute

From: tim4business
Sent: Monday, August 06, 2007 3:07 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Diebold being friends with G.W. Bush should disqualify ANY such machine from use in California, but the track record of such devices is spotty at BEST. I believe the saying is, "If it ain't broke, don't fix it". Well, using electronic voting machines is an invitation to disaster. Just plain "no".

Mr. Tim Shullberg

From: anita
Sent: Monday, August 06, 2007 1:20 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

If our votes aren't safe, our democracy is over!

Mr. anita smiley

From: jweirj
Sent: Monday, August 06, 2007 1:11 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

if the votes don't register our votes accurately and safely we are no longer a democracy.

Mr. Warner Jepson

From: sanchez
Sent: Monday, August 06, 2007 12:38 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. Kimberly Hernandez

From: Neil Hudson
Sent: Monday, August 06, 2007 8:42 AM
To: Voting Systems
Subject: Keep up your clean elections campaign

Ms. Bowen,

I have been long supporter of decertifying electronic voting machines. Congratulations on your courage to stand up to the corporations who are trying to rob us of the only democratic input we have in our government.

I know you are under much political pressure from the ROVs, whose motivations are often questionable at best.

Please stay strong. California may still lead the way for the rest of the USA to have fair elections.

Neil Hudson

From: ruth19251
Sent: Sunday, August 05, 2007 6:38 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. Ruth Terry

From: toobie0535
Sent: Sunday, August 05, 2007 5:10 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. MICHAEL TOOBERT

From: sobelsolar
Sent: Sunday, August 05, 2007 4:41 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

if you can't find a hack proof machine go back to the old system

Mr. Gerald Sobel

From: lishevil
Sent: Sunday, August 05, 2007 3:46 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. Bowen,

I would like to thank you for decertifying the Diebold Voting machines. I will feel more confident that my vote will be counted and not tampered with. I realize this was not an easy decision and I appreciate your courage and integrity in insuring our right to vote. I only wish more leaders showed your integrity.

Mrs. Alicia Evilsizer

From: phyllisbrown
Sent: Sunday, August 05, 2007 2:20 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mrs. Phyllis Brown

From: kalitatodd
Sent: Sunday, August 05, 2007 1:47 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. Kalita Todd

From: louisealdrich
Sent: Sunday, August 05, 2007 1:44 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. Louise Aldrich

From: po
Sent: Sunday, August 05, 2007 12:47 PM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mrs. patrice o\neill

From: Linda Proctor
Sent: Sunday, August 05, 2007 8:27 PM
To: Voting Systems
Subject: to Debra

Dear Debra,

I know you are inundated with emails. Please take a most thoughtful approach to the voting machines being proposed. I am usually a big fan of progressive moves, but feel the risks WAY out way any positive potential. Our democracy is at stake.

Thank you for your attention,

Linda Proctor

From: lproctor1
Sent: Sunday, August 05, 2007 11:56 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. linda proctor

From: tonstin
Sent: Sunday, August 05, 2007 11:20 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. Tony Stinnett

From: lmjensen54
Sent: Sunday, August 05, 2007 9:24 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mrs. Lisa Jensen

From: jonyoung
Sent: Sunday, August 05, 2007 9:15 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. Jonathan Young

From: Global Wisdom
Sent: Sunday, August 05, 2007 5:24 PM
To: Voting Systems
Subject: Time to Sue Dieboldt!

Thank you for thoroughly testing our voting machines. It's time to take action as follows:

- 1) Decertify all machines that didn't pass muster.
- 2) Sue the manufacturers of these machines for their dishonest and irresponsible business practices. These vendors will continue to provide substandard machines for voters around the country until they feel it in the pocket book. Time to sue.
- 3) Do not accommodate these liars and cheats. These are the people that engineered the theft of the 2004 presidential election. That is a crime against the entire population of the United States. It is a crime against the Constitution. It is a crime against democracy. **NO NEGOTIATION WITH CRIMINALS OF THIS HORRIFIC LEVEL. SUE THEM FOR LYING.**

Cougar Brenneman

From: kayschuyler
Sent: Sunday, August 05, 2007 8:42 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

It is imperative that we protect our precious right to have our votes counted using secure tamperproof voting procedures.

Ms. Kay Schuyler

From: colette2thous7
Sent: Sunday, August 05, 2007 6:50 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. colette walczak

From: 2court
Sent: Sunday, August 05, 2007 6:44 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. John Foster

From: alimcnally
Sent: Sunday, August 05, 2007 6:02 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Our votes are precious and vital to our republic. Our votes cannot be privatized and able to be tampered with. All machines must be standardized and government property. All votes must have a paper trail, and voter friendly. Only then can we know our votes is accurate and has been counted.

Ms. alice mcally

From: smf39
Sent: Sunday, August 05, 2007 4:55 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

I'm so glad that you are reviewing and will find the difficulties and lack of "trail" that these machines leave. Perhaps you will find that returning to the paper ballot of the past is called for at this time!
Sue Forbes

Mr. Sue Forbes

From: lelovitz
Sent: Sunday, August 05, 2007 3:50 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Debra Brown ran on a campaign promise to make our State's voting system accurate and reliable, not beholden to corporations pushing their problem machines. She should therefore decertify those machines and uphold her promise.

Mr. Leo Elovitz

From: gkehoe
Sent: Sunday, August 05, 2007 3:23 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. Gary Kehoe

From: Ann Schafer and Lm Rockwell
Sent: Sunday, August 05, 2007 11:26 AM
To: Voting Systems
Subject: "If you have questions ..."

I use the "webtv.net" system, operated by the MicroSoft corporation,
for
my connection to the Internet.

Webtv.net subscribers, like me, can receive information by html code,
but not by pdf code used in your description of your actions taken for
decertification of the electronic vote-casting machine vendors.

1. Could you please supply the information in html code?
2. The Secretary's decision covers electronic vote-casting machines.
Does the decision also cover electronic vote-counting and
vote-tabulation machines, which are also a part of a complete
electronic Voting System?

Leroy M. Rockwell

From: s_thibodo
Sent: Sunday, August 05, 2007 2:57 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Get rid of the machines...Paper ballots only...It's the tried and true
method for ensuring that our votes are counted ...and recounted.

Mr. Scott Thibodo

From: Andrew Lukes
Sent: Sunday, August 05, 2007 10:39 AM
To: Voting Systems
Subject: Thanks!

Thank you!

I work in the network security field and know that security is a never ending race between the
good and bad guys.

Voting is too important to trust to electronic machines until the vendors prove that their systems
are secure by passing rigorous testing.

Thanks for have the insight and courage to make sure our votes count.

From: susan91344
Sent: Sunday, August 05, 2007 2:28 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Why hold elections if the results are not accurate and representative of EVERY vote? Voting must be exempt from sham and scam_ Hold the voting machine companies accountable for hacking potential testing and repair...have an independent agency verify results_better yet get rid of any potentially hackable machine...difficult to hack or rarely hackable is not good enough,,,young American men have died in Iraq because of a inept voting system
ENOUGH is ENOUGH_

Mr. Susan Pierce

From: agentrosyshades
Sent: Sunday, August 05, 2007 2:04 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Dear Debra:

I would like to thank you in your recent research in to the Voting Machines. I also would like to express my concern for the machines as well. I have read in the paper that some machines have arrived at polling places with a number of votes already in their system. How can we as Americans allow this to happen. We need to stop this. If it is the choice to move towards the voting machines more strict regulations need to be in order. Or we as constituents have option at out polling place to choice whether or not we would like a paper ballot or electronic ballot. In this day and age, and with the history of the last two elections I do not wish to use a voting machine. I will tell my friends and family to write to stop corrupt individuals from tampering with our rights to vote.

Thank you very much.

Rosa Tran

Miss Rosa Tran

From: phyllisr1
Sent: Sunday, August 05, 2007 1:11 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

I volunteered on behalf of voters last election and the potential for voter fraud or at minimum voter neglect was unbelievable. If the voters knew just how many blocks are put up to prevent their vote from counting there would be a widespread mayhem.

Ms. Phyllis Riley

From: connectj@sonic.net
Sent: Sunday, August 05, 2007 12:45 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Ms. Jan Brewer

From: Emily Monroe
Sent: Wednesday, August 01, 2007 9:26 AM
To: Voting Systems
Subject: Red Team Investigation on Voting Machines

Dear Ms. Bowen:

Although we are not voters in California, we think your efforts to correct major problems with voting machines [i.e. the sanctity and bedrock of our electoral process] are important as precedent-setting for other states.

This wouldn't be the first time California as led the way for the rest of the USA. Please continue the press toward a trouble-free election process which other states may proudly emulate.

Thank you.

Richard, Beth & Emily Monroe

From: Richard Meyer
Sent: Wednesday, August 01, 2007 9:27 AM
To: Voting Systems
Subject: Voting Machines

Dear Madam Secretary of State:

A team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES&S.

Please do not certify them.

Thank you for your attention.

RM

From: James dougherty
Sent: Wednesday, August 01, 2007 9:27 AM
To: Voting Systems
Subject: Red Team Review

You are commended for your efforts relating to the "Red Team" review of major voting machines in California. These machines, as currently developed, are a major threat to American democracy, having been intimately associated with significant voting fraud in several regions of the nation.

A paper trail MUST be instituted in California, as well as throughout the country, if voting reform is to work. Until voting machines can be certified as reliable, which is very questionable, paper ballots or a paper trail in association with voting machines MUST be implemented.

As a result of the significant security flaws uncovered by computer professionals in machines tested from Diebold, Sequoia, Hart and ES&S, your are urged to make a decision that supports democracy, even if it means to decertify these voting machines.

Again, thank you for your efforts.

James P. Dougherty

From: Ken Ellis
Sent: Wednesday, August 01, 2007 9:25 AM
To: Voting Systems
Subject: Red Team review

Dear Ms. Bowen,

Thanks for the careful review of electronic voting machines. I hope that the flawed machines are never used in elections. Please continue to do what you can to put a stop to election fraud.

Sincerely,

Ken Ellis

From: Elaine Booth
Sent: Wednesday, August 01, 2007 9:28 AM
To: Voting Systems
Subject: De-certify DREs

Dear Secretary of State Debra Bowen,

You are certainly between a rock and a hard place. With the CA Primary moved forward to February 5, and with rules calling for a comprehensive review of voting machines due six months prior, I commend your Herculean effort.

The investigation has determined that the machines are not secure, and the investigators concur that with more time for testing they would have found even more problems. The fact that all the investigators are all in firm agreement is very telling.

Additionally, paper trails are not ballots. Citizens cannot trust that their votes are counted as they are cast. Look at Ohio. What a mess. So much of the evidence linking the 2004 electoral practices to fraud has been "accidentally" destroyed, and evidence of voters' intentions was never retrievable in the first place, due to the invisible nature of vote counting on voting machines.

We need a system that cannot be hacked. It should be secure from vote tampering and "breaking and entering" by election officials, poll workers, Party officials, candidates, and the merchants who sell the system. We need software that is open, not proprietary. We need ballots that are counted visibly, and can be recounted. DREs do not do this.

I do not believe it is an exaggeration to say we are losing our democracy. I don't know all the options in front of you, and you have a very difficult decision to make. For my part, I think we cannot use these machines and have a democracy. We have to choose. It is evident that these machines can be demonstrably and easily hacked. I would choose to de-certify the machines and retain our democracy.

Sincerely,
Elaine Booth

From: Cori
Sent: Wednesday, August 01, 2007 9:29 AM
To: Voting Systems
Subject: Thank You

Thank you for conducting the Red-Team review. I feel hopeful again that you are one of the true civil servants unswayed by corporate donations and special interests.

I am so thankful that Californian's have a true leader in the fight against unreliable voting machines. It's the most important dilemma American citizens face in regards to democracy. I'm proud that a fellow female has the "moxie" to take a stand and challenge the "Unreliable Vote Machine's" supporters who allow the corporations to run our government.

Thank you!!!

Cori Lahners
Loanleaders of America, Inc

From: hal
Sent: Wednesday, August 01, 2007 9:30 AM
To: Voting Systems
Subject: Electronic Voting Machines

I am the owner/operator of KRXA 540 AM in Monterey, CA. We and our listeners strongly urge the Secretary of State to reject all electronic touch-screen voting machines due to their inherent lack of reliability and transparency and the concomitantly high potential for election fraud.

Hal Ginsberg

From: John W.Olver
Sent: Wednesday, August 01, 2007 9:28 AM
To: Voting Systems
Subject: against electronic computerized voting systems

These machines are an invitation to corrupt our electoral system. Once someone is inside of the software anything can happen. I worked with computers for 35 years and they are good tools but whoever is writing the code makes them dance to their tune.

John W. Olver

From: Tracy Valteau
Sent: Wednesday, August 01, 2007 9:31 AM
To: Voting Systems
Subject: NO on electronic voting systems!!!

I am strongly opposed to the use of electronic voting systems. As a computer programmer, I'm aware of their lack of transparency, and the ease with which the results can be manipulated. I find the very - thought- of using them unconstitutional, and dangerous to our government and way of life.

One does not hand a teenaged boy a gun, and say "It's OK... it's not loaded."

That's exactly what using electronic voting machines are: an unloaded gun... with only a select few holding the bullets.

Again: I'm strongly opposed to their use, and urge you to refuse to use them in California.

Regards

Tracy Valteau

From: Carol Martinak
Sent: Wednesday, August 01, 2007 9:33 AM
To: Voting Systems
Subject: Great Job!

Dear Debra Bowen,

Thank you for your hard work.

I believe we can do so much better regarding the computerized voting machines. If we can do it for banking, and casinos – we should certainly be able to do it for voting.

Best regards,

Carol Martinak
Manager, I.T.
Access Communications, LLC

From: kmacken210
Sent: Wednesday, August 01, 2007 9:33 AM
To: Voting Systems
Subject: Electronic Voting Systems Findings

California voters are indeed fortunate that you were elected in November because you took seriously the concerns of Californians to investigate the electronic voting systems that we use to exercise our most important role and right as citizens.

Your findings, that all the electronic systems that we use are hackable, beg action. I am writing to urge you to take action, in spite of the responses and excuses that we are hearing from the status quo, such as average voters would never be able to hack into the system. Of course not. I am not worried about the average voter.

The citizens of this country and this state have been living with governmental and corporate corruption, waste, lack of accountability and lack of transparency for many years now, and that needs to stop. We are counting on you to take the next necessary steps to restore California voters' faith in the elections process by keeping this process transparent and accessible to the public.

Thank you,
Kathleen MacKenzie

From: Belisle, Joseph A HS
Sent: Wednesday, August 01, 2007 9:35 AM
To: Voting Systems
Subject: "Red Team" Results Comment

I am not a resident of California though I do greatly admire much of your great state. The good people at Velvet Revolution sent me an e-mail today in regard to 'Red Team' review of the computer voting machines used in your state. They asked that those who receive their e-mailings to send in comment to your office about computer voting machines.

I've read a great many articles on the performance of computer voting machines. And my understanding and position on them is that they cannot be trusted. Even the best security systems can be bested. And these voting machines are pathetic when it comes to hacking. Test after test has proven that not only can they be hacked but they can be done relatively easily and leave no trace of the hack. I do not hold much faith in democracy in America. But if our votes can be so easily invalidated then democracy can't exist in America. Though I must have some faith and hope if I'm stilling willing to send a comment to California's SOS.

At least in this basic facet of democracy, please hold voting systems accountable to the strictest controls and not allow voting machines. I am a resident of Massachusetts, about as far away from California as you can get in our nation, but each state affects the others. I look to your state as well as my own as a leader in rights of the people. Please deny the use of computerized voting machines.

Thank you for listening,

Joseph A. Belisle

From: Alby Baker
Sent: Wednesday, August 01, 2007 9:35 AM
To: Voting Systems
Subject: those pesky voting machines and those who create them

Debra Bowen, please and thank you for stepping up to daylight the problems with the new voting machines. Our nation and democracy are being destroyed piece by piece by those who wish to have maximum influence and control. It's a moment right out of science fiction..."it could never happen here". Well , the creeps and criminals are well on they're way.

Thanks for your involvement. I fervently hope they don't get to you; and that they begin to be brought to justice. That they have gotten this far without being brought to trials and prisons says everything about our nation and time. Good luck!

Alby Baker

From: CNolan
Sent: Wednesday, August 01, 2007 9:14 AM
To: Voting Systems
Subject: VOTING MACHINE REVIEW

Secretary of State Debra Bowen,
Thank you very much for your efforts to make sure that voting machines are reliable. I understand that computer scientists and professionals found major security flaws in all machines your department tested. That news is a **very big concern** to me. Voters need to be able to trust that when they cast a vote it is recorded for the person or issue they voted for.

I trust you to decertify these machines or make sure problems are fixed.

Sincerely,
Carolyn E. Nolan

From: Erin Frost
Sent: Wednesday, August 01, 2007 9:39 AM
To: Voting Systems
Subject: Vote Machines

SOS Bowen:

Thank you for conducting the "Red-Team" review of vote machines which found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES&S.

Given such security flaws, the only option that will protect voters and keep our elections honest is to decertify them these machines.

Please take voters into account as you make this decision of what to do with the vote machines that do not meet reasonable security standards.

Sincerely,
Erin Frost

From: Helissa Penwell
Sent: Wednesday, August 01, 2007 9:41 AM
To: Voting Systems
Subject: throw out the electronic voting machines

It would be better to go to an all write-in system, where we mail in our paper ballots, than to use the electronic systems of today. Please do not certify the machines, even conditionally. Our democracy is at stake.

Helissa Penwell

From: Todd Lockwood
Sent: Wednesday, August 01, 2007 9:41 AM
To: Voting Systems
Subject: Thank you!

Thank you for researching flawed voting systems!

Your efforts are appreciated.

Now please decertify these dangerous machines until their flaws are fixed. Your actions, given the size of California, could have a positive impact on the entire nation.

Thank you,

Todd Lockwood

From: Regina
Sent: Wednesday, August 01, 2007 9:42 AM
To: Voting Systems
Subject: voting machines

It is obvious even to a non computer mavin, like me, that computer machines for voting is a dumb idea. Especially when produced and managed by private companies that can be bought off , if the occasion should arise. I know enough about computers to know that they are vulnerable to tampering and that it is not always possible to validate one's vote. I realize that voting is never fool proof, no matter how it is processed, but the machines are too untrustworthy. I want paper ballots and hand counting. I will volunteer in my area if you need more volunteers.

Regina M. Moritz - California voter

From: bankersg
Sent: Wednesday, August 01, 2007 9:43 AM
To: Voting Systems
Subject: Electronic voting systems

Every time I have seen you, my associates and I have warned that electronic voting machines cannot be successfully monitored. There are too many ways to infiltrate them. Your investigations have proven us correct. It is time that we go back to paper ballots marked with a pen by the voter and counted publicly with witnesses. Anything less will not guarantee accurate elections.

Dorothy Reik
President
Progressive Democrats/Santa Monica Mountains

P.S. Your staff never responded to our invitation to the PDA/PDLA./PDA annual fundraiser. I think after all the work we did to get you elected we at least deserve a response.

From: Helen Rose
Sent: Wednesday, August 01, 2007 9:44 AM
To: Voting Systems
Subject: Voting Machines

Dear Gentlepeople:

That voting machines are readily hackable has now been well established by a wide variety of computer-literate citizens and academics.

If the citizenry doesn't have confidence in fair elections, our democracy is doomed.

I urge you to consider paper ballots, hand-counted.

Very truly yours,

Helen Rose

From: Julie Dahl
Sent: Wednesday, August 01, 2007 9:45 AM
To: Voting Systems
Subject: Thank You

Thank you for arranging the test hacking of the voting machines. You said you'd do it and you did. This is vital for the safety of our votes. Will you be taking the next step of banning the use of these defrauding, vote-stealing machines in any and all future elections in our state? I hope so, though I know will take a bit of time. In the meantime, can you educate voters about the safest way to get each individual vote actually counted accurately?

Thank you again for proving your ability to follow through and for serving the state's voters.
Julia Dahl

From: Beaton, Alisa
Sent: Wednesday, August 01, 2007 9:45 AM
To: Voting Systems
Subject: Electronic voting machines

Dear Secretary of State Bowen,

I feel confident that, with the objective of securing the votes of all California voters, you will decertify any or all electronic voting machines, no matter how much their initial cost to the state, if they are found unreliable.

Thank you, Secretary of State Bowen. It was a happy day for many of us Californians when we had the pleasure of casting our votes for you.

Alisa Beaton

From: Lynn Meadows
Sent: Saturday, July 14, 2007 9:51 AM
To: Voting Systems
Subject: Red Team concerns.

Thank you for being concerned about the voting system and the machines being used.

I helped with the Ohio recount in 04. I am also a regular election inspector. I have had many concerns about our voting system. I believe that we must offer the voters the most safe and reliable system possible. They must feel confident that their vote counts!

One of the most sensible ways to assure this is to have random audits. That is common to monitor accounting systems, why not our voting system.

Thank you for your courage to stand up for the voters. If the companies making the machines have nothing to hide, they should welcome the opportunity to verify the reliability of their machines.

Lynn Meadows
Chelsea, Michigan

From: Ed Haggard
Sent: Wednesday, August 01, 2007 9:50 AM
To: Voting Systems
Subject: voting machines

Greetings Debra Brown,

I heard about the review of voting machines in California. Thanks for doing that. Please reject the vote machines that do not meet reasonable security standards. This is so critical for our country.

Ed Haggard

From: Mary M.Freedlund
Sent: Wednesday, August 01, 2007 9:51 AM
To: Voting Systems
Subject: Fwd: Mail delivery failed: returning message to sender

Dear Secretary:

Please, please either throw out the voting machines that have tested positive with access to hackers or adjust them in some verifiable way so that the public can be guaranteed correct election results by the next election. Thank you very much. Yours,

Mary Murphy Freedlund

From: Florence Vincent
Sent: Wednesday, August 01, 2007 9:51 AM
To: Voting Systems
Subject: Please get rid of the machines

Our vote is the most precious thing we have. Please don't give it over to public companies. It belongs in the public domain.

Many thanks
Florence

Florence Vincent

From: Sandy Rounds
Sent: Wednesday, August 01, 2007 9:52 AM
To: Voting Systems
Subject: Voting Machines

I think you would be supporting Democracy and the right of the people to free and fair elections if you De-Certify the voting machines. Thank You,

Sandy G. Rounds

From: Mary Baker
Sent: Wednesday, August 01, 2007 9:53 AM
To: Voting Systems
Subject: voting machines

Thank you for organizing the "Red Team" reviewing security for voting machines. I have worked in the IT field and also been a precinct captain for elections. Voting machine security could be a major problem if the issue is not addressed.
Mary Baker

From: Jane Engelsiepen
Sent: Wednesday, August 01, 2007 9:54 AM
To: Voting Systems
Subject: THANK YOU

Dear Secretary of State Bowen,

THANK YOU for addressing and exposing the nightmare of electronic voting. Your top to bottom review may send shock waves through this complacent nation and be the tipping point to regain the veracity of our nations elections.

Imagine having a president who was really elected by the votes of the people? Fascinating concept.

THANK YOU!

Most Sincerely,

Jane Engelsiepen

From: lamura@finestplanet.com
Sent: Wednesday, August 01, 2007 9:55 AM
To: Voting Systems
Subject: Vote

Why vote if we can't be assured our vote will not be counted correctly? We need a paper trail and to recycle machines that do not meet security standards. Thank you Debra Bowen for making the right decisions and backing those decisions.

From: Barbara Kennedy [mailto:bkenn202@sbcglobal.net]
Sent: Wednesday, August 01, 2007 9:57 AM
To: Voting Systems
Subject: Decertify Hacked Electronic Voting Systems

Congratulations to Secretary of State Bowen for exposing the weaknesses of the current batch of electronic voting systems. Software should be open-source so that defects can be easily detected - there should be no proprietary software in certified voting systems. Please decertify all currently hacked systems.

Barbara Kennedy

From: Doris Parker
Sent: Wednesday, August 01, 2007 9:58 AM
To: Voting Systems
Subject: e-voting

I am not from California, but I am from Florida, whose questionable voting machines sure took a toll on the country in 2000. Why, after nearly eight years, do we still have unresolved problems with e-machines? There is just no valid excuse for any state not to have taken care of this issue. At least in Florida Governor Crist has outlawed touch-screen e-voting, and I feel better about casting my vote. Do the right thing! Do the right thing! Do the right thing!
Doris Parker, United States citizen voter.

From: Diane
Sent: Wednesday, August 01, 2007 9:55 AM
To: Voting Systems
Subject: please decertify electronic voting machines!

Dear Ms. Bowen,

I am writing to encourage you to take the bold step of decertifying all the electronic voting systems in the state. These machines can't be trusted, and as a voter, I urge you to fight for fair and accountable voting machines.

Thank you very much,

Diane Bloch

From: jlsklar
Sent: Wednesday, August 01, 2007 10:01 AM
To: Voting Systems
Subject: voting machines

Please decertify the voting machines which you have found not to be secure. Your panel tested all the models and found major security flaws. This would not be good to let people vote on these machines.

I urge you to do the right thing.

Thanks,

Jill Leight-Sklar

From: Steve Osborn
Sent: Wednesday, August 01, 2007 10:02 AM
To: Voting Systems
Subject: No on electronic, hackable, voting systems.

Dear Ms Bowen,

Please, the only way to have a fair, accountable, election is by using a system that provides a voter verified paper trail. You could save millions by going back to the paper system, with counts at the precincts verified by poll watchers. The count, and the LOCKED ballot boxes are then passed up to the county. The results would be quicker and the security would be much better.

In case of a dispute, the LOCKED ballot boxes are taken from the SECURE storage area and the ORIGINAL ballots are recounted.

These hackable, non-verifiable, electronic systems are an expensive nightmare leading to yet more corruption in government.

Steve Osborn

From: Steven M. Jacobs
Sent: Wednesday, August 01, 2007 10:02 AM
To: Voting Systems
Subject: Support for secure voting machines

Debra Brown, Secretary of State, California

I support your past stand for secure voting machines and urge you to hold a firm stand. Thank you.

Steven Jacobs
From: Al Baars
Sent: Wednesday, August 01, 2007 10:03 AM
To: Voting Systems
Subject: "Red-Team" review

Thank you for helping to ensure that the people still have a vote. Unfortunately with such a short time before the elections it may not be a good idea to keep the machines in place. Paper ballots might be the best solution at this point, but what if we called on Apple computer to create voting machines? They seem to be able to produce secure systems better than anyone.

Thank you for your time,
Al Baars

From: Mary L. Johnson
Sent: Wednesday, August 01, 2007 10:04 AM
To: Voting Systems
Subject: California voting machines

Dear Ms. Bowen,

Thank you for your analysis of computerized voting. Please do not allow voting to continue in California using computerized voting and vote-counting machines. A vote is not worth the effort it takes if it is not counted, or miscounted, and both can happen all too easily with these machines.

Thank you for your consideration.

--

Mary L. Johnson, Ph.D.

From: James dougherty
Sent: Wednesday, August 01, 2007 9:27 AM
To: Voting Systems
Subject: Red Team Review

You are commended for your efforts relating to the "Red Team" review of major voting machines in California. These machines, as currently developed, are a major threat to American democracy, having been intimately associated with significant voting fraud in several regions of the nation.

A paper trail MUST be instituted in California, as well as throughout the country, if voting reform is to work. Until voting machines can be certified as reliable, which is very questionable, paper ballots or a paper trail in association with voting machines MUST be implemented.

As a result of the significant security flaws uncovered by computer professionals in machines tested from Diebold, Sequoia, Hart and ES&S, your are urged to make a decision that supports democracy, even if it means to decertify these voting machines.

Again, thank you for your efforts.

James P. Dougherty

From: Mary L. Johnson
Sent: Wednesday, August 01, 2007 10:04 AM
To: Voting Systems
Subject: California voting machines

Dear Ms. Bowen,

Thank you for your analysis of computerized voting. Please do not allow voting to continue in California using computerized voting and vote-counting machines. A vote is not worth the effort it takes if it is not counted, or miscounted, and both can happen all too easily with these machines.

Thank you for your consideration.

--

Mary L. Johnson, Ph.D.

From: Tim Callahan
Sent: Wednesday, August 01, 2007 10:09 AM
To: Voting Systems
Subject: Thank you for the Top to Bottom Review of Voting Machines

Secretary of State Bowen,

Thank you for your investigation, and please decertify all voting systems that can be tampered with or that do not have a clear paper trail.

Tim Callahan

From: Ruth Hoke
Sent: Wednesday, August 01, 2007 10:09 AM
To: Voting Systems
Subject: Comment on Top to Bottom Review

Dear Secretary Bowen:

Thank you for conducting the Review. We believe the best solution to our election problem is hand-counted paper ballots. We believe enough volunteers can be found to perform these counts. For those who feel we need instant results, we recommend statewide exit polls. There is no place in a democracy for privately-owned vote count systems; the system must be owned by and accountable to the citizens only!

Sincerely,

Kathryn Ruth Hoke
George L. Hurlburt

From: Ouapiti Robintree
Sent: Friday, August 03, 2007 7:27 AM
To: Voting Systems
Subject: VOTING MACHINE FRAUD -- Please nip this problem in the bud!

To: Secretary of State Debra Bowen
re: validity and function of electronic voting
machines

Dear Secretary Bowen,

I am writing to share my concern about the use of electronic voting machines in recent US elections. It has been shown repeatedly that these machines are easily manipulated for fraudulent purposes, and American citizens have very serious concerns about the validity of our recent election outcomes. If there is a HINT of illegality about these machines, it is your duty to decertify them and, if at all possible, return the American populace to the use of paper-and-pencil ballots which we've used to record our votes, until such time (which I doubt) as these machines can be programmed against ANY tampering. It is imperative that you hold these companies accountable for lying and deceiving state officials. The refusal to step up and do the right thing NOW may lead to inaccurate reporting of the American people's will for government, and THAT IS A TRAITOROUS OFFENCE! How can we be a nation of informed voters, if our rights to vote are taken away by corrupted computer-voting programs?

Our founders held that voting was a citizen's right and duty; please don't let this country go down in history as crumbling under the corruption of this administration. Regardless of your party membership, surely you must see that "Those who cast the votes don't matter; those who count the votes do."
(paraphrasing Josef Stalin)

History will record your actions for posterity, and it would be a sad day if this nation crumbled because of the iniquity and vice of corrupt politicians and voting machine companies. Please do the right thing and stand up for American virtue and TRUE freedom: the right to express ourselves by voting for the men and women we trust to lead this country back into virtue and respect from the rest of the world.

Yours sincerely, one more concerned citizen,
Ms. Robin O. Robintree

From: Jackie Maruhashi
Sent: Friday, August 03, 2007 10:20 AM
To: Voting Systems
Subject: Top-To-Bottom Review of Voting Machines

August 2, 2007

The Honorable Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, CA 95814 /Sent via e-mail to: _votingsystems@sos.ca.gov
<<mailto:votingsystems@sos.ca.gov>>_/

/___/*RE: Top-To-Bottom Review of Voting Machines*

**Dear Secretary Bowen:

We support the August 1, 2007 letter sent to you by the Asian Pacific American Legal Center and other civil rights and civic engagement organizations. The Asian Law Alliance is a non-profit community law office that has significant experience working with new voters and those who are limited English proficient.

We oppose any decertification of the voting systems as a means of addressing the report's findings that question the security and accessibility of the voting systems. We support recommendations calling for corrective action to mitigate or eliminate the security vulnerabilities identified in the report. In addition, we believe that accessibility issues addressed in the report can be remedied without forcing counties to switch to other voting systems.

Currently, Santa Clara County voters may vote in Chinese, Spanish, Tagalog, and Vietnamese in addition to English on the Sequoia AVC Edge electronic voting machines. These machines offer increased access to the polls when compared to the paper-based voting systems. As a result, voter registration and turnout have increased tremendously in Santa Clara County.

With so little time left before the February 2008 election, we urge you to fix the problems identified in your July 27, 2007 report, but not decertify our voting system.

Sincerely,

Richard Konda,
Executive Director

From: Joe Harty]
Sent: Friday, August 03, 2007 12:10 PM
To: Voting Systems
Subject: Absolutely no computer voting machines....

Secretary of State,

The mere fact that these machines are still being considered for the primary's use means that money is flooding the talking heads departments in these nefarious organizations still. Diebolt alone stands as the shining example of a new kind of criminal, a vote distorter on the pay of the gop with a track record with the GOP going back to the secretary of state/GOP hack Kathleen Harris of Florida back in 1999 and the deliberate, proven action to disenfranchise 40,000 people and tinker with the poll numbers so that for the first time the polling numbers did not match their votes.

The absentee ballots should be the only alternative to paper ballots at the polls like in Oregon, as their is no trust in any of the computer voting machines, even with paper trails because the people who are involved and own these companies are less then democratic . They are disloyal to our secular democracy. As a matter of fact I consider this a fundamentalists problem . I refer to the cult of the american Taliban, the southern christians, who just like the Taliban radicals in Afghanistan hold everyone who thinks different from them in contempt worthy of being attacked, those kind of people maybe alright to rule their cults, but have no place in our democracy.

Please shut this down, when you do it will have a instant effect in other states, also in the process of bankrupting a field unworthy instrumentations set-up to give ultimate power to corporation types over us all. This in direct opposition to the single most dynamic democracy on the earth at any time in history. Stop the machines involvement with the vote, crush their grip on the system here, if California leads other states will follow. I believe this maybe the last chance to stop this. Please shut them down now! Last, feel free to send whatever information that shows your research's findings.

Joseph F.P. Harty

From: danielle guion
Sent: Wednesday, August 01, 2007 10:09 AM
To: Voting Systems
Subject: ...in Hawaii...

WE were subjected to Hart Inter Civic!! 'They' were (during vote counting, I was an 'observer',)
MEN in RED shirts enclosed in a little room where we had no access!!

At training for observers, we weren't given straight answers...no answers!!! They avoided
questions like, "How do I know the vote was counted?" And, "Where's the receipt?" "How does
this 'cyber' vote get counted?"

No answers...I could see how rigged this was....our Elections 'Person' (a DEMOCRAT!!) was so
enticed by something.....he bought into this even though there was ample warning this was not
kosher!!!

Thanks and good luck....come to Hawaii next!

Danielle Guion-Swenson

From: Jack Kaplan
Sent: Wednesday, August 01, 2007 10:11 AM
To: Voting Systems
Subject: Thank you, and consider these points.

Thank you for the vision to keep our voting system open to all of the public, and to be recorded
accurately for all of the public. If we are to survive as a people, and as a democracy, your work at
this juncture is critical. Do not underestimate your importance at this time, and do not be easily
discouraged. We are all paying attention. We do not want the vote privatized or controlled by
private corporations with incompetent equipment owned and operated by partisan corporations.

Also we do not want our voting rolls thinned out in any way by cumbersome registration tactics,
and "caging lists," and other partisan tactics to suppress the voters participation in the electoral
process.

Finally, as Secretary of State, you may be able to influence the legislation to get us free airtime
for candidates and issues, on the public forum of people's media airwaves now squatted upon by
private media corporations.. Private corporations should not be the gatekeepers to our media
public squares. That's the only way we will have a diverse range of candidates. Public financing
of campaigns is okay, but media triples its rates at campaign time and cuts coverage, as well, to
force the purchase of inflated priced 30 second soundbites.

Also consider ranked voting or instant runoff voting as a way to include more candidates and
widen discussion on the important issues effecting our survival at this time.

Jack Kaplan

From: Monique
Sent: Wednesday, August 01, 2007 10:12 AM
To: Voting Systems
Subject: Electronic Voting Machines

Dear DebraBowen!

THANK YOU for your courage and an excellent job in hunting down those who wish to give us more of the BUSH whackers..... we certainly do NOT need more of THAT crazy destroyer (and HE thinks he is the decider!) We will keep our hopes alive with someone as brave as YOU are!

From: Michael C Travali
Sent: Wednesday, August 01, 2007 10:13 AM
To: Voting Systems
Subject: Voting Machines

Thanks for the Red Team review. If machines have security flaws they should be decertified and returned.

Michael C. Travali

From: Colleen Spining
Sent: Wednesday, August 01, 2007 10:13 AM
To: Voting Systems
Subject: Debra Bowen, we have your back . . .

Decertify these machines; they are too iffy. The public needs to know their votes can not be tampered with.

Respectfully,

Colleen Spining

From: Jane Engelsiepen
Sent: Wednesday, August 01, 2007 10:14 AM
To: Voting Systems
Subject: DECERTIFY THEM

Dear Secretary of State Bowen,

You must DECERTIFY the voting machines which were discovered to be hackable. There is no other viable alternative.

Please lead the way to rid our country of electronic voting machines.

Most Sincerely,

Jane Engelsiepen

From: Mail4CarolR@aol.com
Sent: Wednesday, August 01, 2007 10:15 AM
To: Voting Systems
Subject: Protecting my vote

I want to be able to verify that my vote is correctly cast on any machine that is used for voting. Period. I want to be able to see that this vote is delivered to those who are counting the votes. And this process needs to be easily verifiable. If such conditions are not available, I will demand a paper ballot and urge all voters to do the same.

From: Mark Reback
Sent: Wednesday, August 01, 2007 10:20 AM
To: Voting Systems
Subject: I support decertification of all electronic voting machines in California

Dear Secretary of State Bowen-

Thank you for your efforts to illuminate the security flaws within all electronic voting machines in use in California. I urge you to hold the voting machine companies accountable and decertify all electronic voting machines in California in time for the February 2008 election.

As you know, last week, the results came in from California's top-to-bottom ³Red Team² review of the four major vote machines used in that state, where a crack team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES.

Obviously, the machine vendors are extremely opposed to the review results and any action by the Secretary of State's office, and they are trying hard to lobby against any action.

Secretary Bowen, you now have to make a crucial decision. You know what you have to do. Decertify all electronic voting machines and require a paper voting trail for all elections in California.

The people of California thank you and your office for conducting the ³Red-Team² review, and please follow through and decertify all electronic voting machines in California because they do not have reasonable security standards.

Sincerely,

Mark Reback

From: blcroll
Sent: Wednesday, August 01, 2007 12:36 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

We voted for Ms. Bowen because we were concerned about the state of our most precious right. Now our worst fears have come to light, I urge Ms. Bowen to immediately de-certify all of the machines and instead look into alternative ways to count votes that are transparent and open to audit.

Remember, as Stalin said, "The people who cast the votes decide nothing. The people who count the votes decide everything."

Ms. Becky Croll

From: susanmanetas
Sent: Wednesday, August 01, 2007 12:37 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mrs. Susan Manetas

From: Adrienne Kligman
Sent: Wednesday, August 01, 2007 8:47 AM
To: Voting Systems
Subject: Thanks/decertify vote machines

Thank you for conducting the "Red-Team" review, and please rid of the vote machines that do not meet reasonable security standards.

Thank You,
Adrienne Kligman

From: kaye547
Sent: Wednesday, August 01, 2007 12:39 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Dear SOS Bowen: Thank you, thank you, thank you. This is one of the most important issues facing our democracy today. Stand strong. You are right. In fact, we need paper ballots and hand counting to be sure our votes actually count.

Thank you again!

Ms. Kaye Peters

California Secretary of State
1500 11th Street
Sacramento, California 95814

Greetings;

Well I see that you tested the electronic voting machines digital security and found it wanting. Some statements did try to reassure everyone that they will be secure when they are used. That reassures me not at all.

I would be willing to bet that even when used as designed within the security surrounding the voting system there are many ways the vote can be altered. In fact there are even ways that do not even require that the Black Hat touch the voting machine. Ways that exploit weaknesses inherent in any computer and that could be used to alter the vote. And there is also Mother Nature....

One: Power is the most obvious. Will each precinct have backup power capable of running the voting machines for the entire polling day? How about protection from nearby lightning strikes? I have my doubts. A paper ballot needs no power and does not conduct electricity.

Two: Water is the enemy of computers. A leaky roof in a precinct or the trucks transporting them can damage the voting machines. Even a once wet paper ballot might well be countable.

Three: Could a cell phone sized device be created that could create a sufficiently powerful electromagnetic pulse that would damage the voting machine? I suspect the answer is yes. Paper ballots are immune to electronic interference.

Four: You only tested the machines themselves, but not the security of the system wherein they are stored, configured, distributed, used, collected and tallied. Can you honestly say their security is perfect? Paper ballots are much harder to "hack".

Because of these issues and others I am sure that we can both think of, I do not intend to vote using an electronic voting machine. I will ask the County Registrar of Voters to remove me from the voter roles before that, and will let both of you know why in no uncertain terms. And I have voted in virtually every election since 1972.

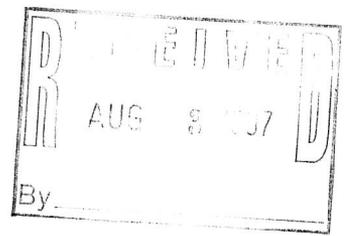
Quite Sincerely;



Keith B. Rosenberg

31 JULY 2007

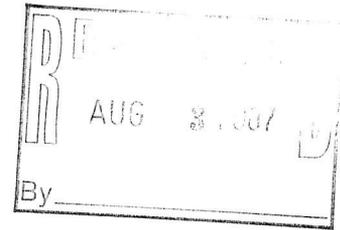
JULY 30, 2007



DEAR MS.BOWEN,
THANK YOU SO MUCH FOR INVESTIGATING THE CROOKED COMPUTER VOTING MACHINE COMPANIES. IT HAS BEEN SO OBVIOUS TO ME FROM THE BEGINNING THAT THESE MACHINES WERE EASILY COMPROMISED AND OUR VOTES JUST AS EASILY STOLEN. I AM LOSING ALL TRUST AND CONFIDANCE IN MY NATIONAL AND STATE GOVERNMENT'S ABILITY AND WILL TO PROTECT THE SANCTITY OF OUR VOTES. PLEASE DO NOT APPROVE THE DIEBOLD AND TWO OTHER COMPANIES' INSISTENCE ON USING THEIR CRIMINAL MACHINES IN ANY MORE ELECTIONS. I NOW VOTE ONLY WITH MAIL- IN BALLOTS AND I STILL HAVE LITTLE FAITH THAT THEY ARE COUNTED.
PLEASE RESTORE MY CONFIDANCE IN OUR ELECTION PROCESS. I WOULD PREFER A PAPER BALLOT.

SUSAN KAEFER, P.T.

The Honorable Debra Bowen
Secretary of State, California
1500 11th Street
Sacramento, CA 95814



The Honorable Secretary of State:

August 1, 2007

As someone who campaigned for you in the last election, I am pleased to write to you strongly supporting your efforts to require that ALL voting machines be tested, especially in light of recent evidence that such equipment is subject to tampering and manipulation. Election protection and the right to vote are FUNDAMENTAL to the democratic process. I am also aware that manufacturers of voting technology that do not have independent verification by means of a paper trail or review of the computer source codes have been used to benefit the Republican Party in closely contested elections. That observation is not a partisan statement but rather an affirmation of the need for an accurate vote tally, regardless of outcome.

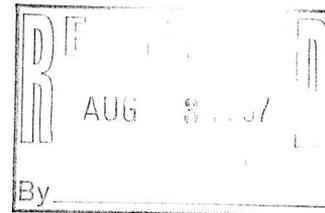
Please continue to stand firm on the issue of election protection in every way.

Gene Rothman
Gene Rothman

310-398-1414

07/31/07

Honorable Debra Bowen
California Secretary of State



Honorable Debra Bowen,

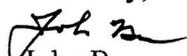
Thank you for your leadership in initiating the top to bottom review of California election systems. I was unable to attend the public hearing on Monday 07/30/07 due to work and family obligations. I have served as a precinct inspector for several elections in Alameda County and as a precinct coordinator. I have been serving on the Alameda County election advisory committee since its inception. In my opinion, it is well overdue to decertify all DRE (direct recording electronic) machines in the state of California.

Currently, the Registrar of Voters are dependent on the corporate vendors to run elections in California. They tend to trust the grossly inadequate system of federal testing and the vendors public relations. They tend to discount valid criticism through stating "it can't happen", "won't happen" or "didn't happen here" or conveniently forget when it did happen when it comes to problems with electronic voting. An example would be the re-call election of 2003. An article in the San Jose Mercury on Feb 1st 2004 stated in part "For an unknown reason, the computerized tally program had begun to award votes for Lt. Gov Cruz Bustamante to Burton, a socialist from Southern California. Similar mishaps have occurred across the country ever since election officials have embraced electronic voting in the wake of the Florida vote-counting debacle of 2000." That incident happened in Alameda County but, I have yet to hear the Registrar of Voters past or current acknowledge this incident in a public forum or give explanation on how it happened and how it has been rectified. There was a grand jury investigation in Alameda County in regard to the use of uncertified patches in the use in that election. The conclusion was to refer to the Secretary of State. Please do the will of the people and secure accuracy, transparency and accountability in all elections in the State of California. It is a terrible feeling as a voter to not know who really won and if your vote was counted as intended. It is even worse as a citizen to wonder if we truly live in a democracy.

I request the following four items as soon as possible:

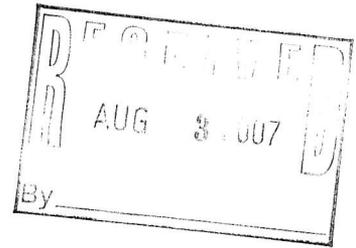
- 1) to outlaw the use of DREs in California elections with or without a paper trail immediately.
- 2) to conditionally certify ballot marking devices (BMD) for California use as soon as possible
- 3) to direct the Attorney General of the State of California to initiate new fraud cases on behalf of the voters of California in terms of breach of contract(s), the use of "uncertified patches" into election counting devices, failure to meet basic standards of a viable VVPAT, and failure to adequately keep voting records.
- 4) to initiate your office to work with the University of California and interested non profit organizations to develop and maintain an open source opti-scan vote counting system with a ballot marking device and precinct sorter that can be made available to the California counties and municipalities.

Sincerely,


John Bass

*Thank you!
This is a hand
copy of the letter
sent electronically
on 8/01/07.*

Deborah Bowen
California: Secretary of State
1500 11th Street
Sacramento, California
95814



REF: Voting Machine Certification

Greetings and Salutations,

Please accept my words in the spirit offered. I have always considered “The right to vote” as the “Holy Grail” of all republic and democratic forms of Government.

The notion of allowing private groups and corporations without 100% transparency, at every level, in every detail is liken to inviting a fox, carrying good intentions, into the chicken house. This idea which politicians seemed to have embraced is unsavory and offensive, to say the least.

O.K Enough, I got it. It is not my intent to rehash old mistakes and complaints. However, the fox is now inside the chicken house. So what do we do with him? I suggest that any and all vendors and voting machines that do not allow 100% transparency at every level of interrogation as suspect, and by obvious default, not engaged in the greater good of the people of the state of California.

Arguments against the surrender of proprietary source codes to appropriate state auditors, public inspection, and public verification, only holds water in the world of private enterprise. These same arguments against, are not acceptable credentials in an unfettered election process. By the rule of law, if there exists one, and if not, there should be one. The only secret that should be kept in an election is the identity of the voter.

Whatever portion that is suspect, of the whole process, that is proved to be unacceptable, should be enough to reject the overall use benefits of the entire system.

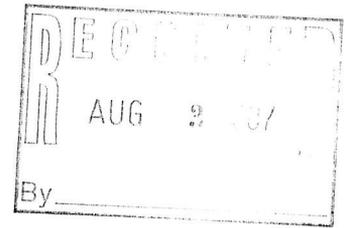
Plain and simple, VERITAS! No proof, no certification.

P.S. If you should require anything else of me beyond this letter, I happily await your ideas and requests.

TAX.
The Clark Family

Clark

July 30, 2007



Esteemed Secretary of State Bowen:

Thank you for your efforts to examine all the voting machines.

Now that we know that they can all be hacked and that there people willing and able to hack them, it is time to ban them! All elections should be decided by paper ballots that are counted, preferably by hand.

It is important to get the results right, even if it takes a little longer.

Again, thanks,

A handwritten signature in cursive script that reads "Steve Eklund".

Steve Eklund

From: Pandaeus, Rene
Sent: Wednesday, August 01, 2007 8:48 AM
To: Voting Systems
Subject: In support of SOS Debra Bowen's electronic voting machine audit

To Whom It May Concern:

Anything computerized can be hacked into. I believe when it comes to voting – all votes should be done the 'old-fashioned' way by punching a hole in the voting cards.

I sincerely believe that the 'punch card' way is the only accurate way for our votes to be properly accounted for.

RENE PANDAEUS

LPA

From: peselwyn
Sent: Wednesday, August 01, 2007 12:37 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Please ensure that only those voting machines that are absolutely secure are used in the next election!

Ms. Pamela Selwyn

From: Margaret Costello
Sent: Wednesday, August 01, 2007 8:50 AM
To: Voting Systems
Subject: Voting Systems

Thank you for your review of the electronic voting machines. I believe they are expensive and untrustworthy. It puts voting in the hands of private corporations that are not accountable to the voters. In Ohio they did not provide enough machines in poor neighborhoods during the 2004 presidential election. When fraud was suspected evidence was easily destroyed. I believe these machines are an institutional way to disenfranchise poor voters. Please make them go away. It is a tough decision you have to make. Please make the brave choice.

Thank you.
Margaret Costello

From: nancydqc@starstream.net [mailto:nancydqc@starstream.net]
Sent: Wednesday, August 01, 2007 12:41 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Thank you for keeping our elections honest and fair.

Ms. Nancy Droese

From: nancydqc
Sent: Wednesday, August 01, 2007 12:41 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Thank you for keeping our elections honest and fair.

Ms. Nancy Droese

From: Todd's Junk
Sent: Wednesday, August 01, 2007 8:51 AM
To: Voting Systems
Subject: Red Team review -- please decertify!

Dear Secretary of State Bowen --

Thank your for initiating the important "Red Team" review of California's voting machines. Your bold actions on this front have made California an example to the rest of the country in terms of how to deal with the voting crisis.

In light of the disappointing -- but predictable -- results of the review, your only viable course of action is to decertify these machines. I realize this may be an expensive proposition, but the threat of the public losing faith in the voting process is infinitely more expensive.

The solution is quite simple: despite an unsubstantiated conventional wisdom that they are prohibitive here in the United States, paper ballots seem to work quite well all over the world.

Alternatively, if electronic voting is absolutely necessary, a voter-verified paper backup is a must, and these backups must be counted subsequent to the certification, to verify the result. Again, quite simple.

I can travel to New York and use a machine to withdraw cash from a bank account in Los Angeles. The machine gives me a record of the transaction on paper, which I can then check against the bank's records when I receive a statement. If this sort of thing can take place millions of times a day without a hitch, then there is no

excuse for the cloud of doubt that currently hangs over our electoral system.

Sincerely,
Todd Slater

From: vjbn3@earthlink.net
Sent: Wednesday, August 01, 2007 12:43 AM
To: Voting Systems
Subject: Decertify the Hackable Voting Machines

Mr. VAROUJ JOHN JEBIAN

From: John Bass
Sent: Wednesday, August 01, 2007 8:52 AM
To: Voting Systems
Subject: public comment submission

07/31/07

Honorable Debra Bowen

California Secretary of State

Honorable Debra Bowen,

Thank you for your leadership in initiating the top to bottom review of California election systems. I was unable to attend the public hearing on Monday 07/30/07 due to work and family obligations. I have served as a precinct inspector for several elections in Alameda County and as a precinct coordinator. I have been serving on the Alameda County election advisory committee since its inception. In my opinion, it is well overdue to decertify all DRE (direct recording electronic) machines in the state of California.

Currently, the Registrar of Voters are dependent on the corporate vendors to run elections in California. They tend to trust the grossly inadequate system of federal testing and the vendors public relations. They tend to discount valid criticism through stating "it can't happen", "won't happen" or "didn't happen here" or conveniently forget when it did happen when it comes to problems with electronic voting. An example would be the re-call election of 2003. An article in the San Jose Mercury on Feb 1st 2004 stated in part "For an unknown reason, the computerized tally program had begun to award votes for Lt. Gov Cruz Bustamante to Burton, a socialist from Southern California. Similar mishaps have occurred across the country ever since election officials have embraced electronic voting in the wake of the Florida vote-counting debacle of 2000." That incident happened in Alameda County but, I have yet to hear the Registrar of Voters past or current acknowledge this incident in a public forum or give explanation on how it happened and how it has been rectified. There was a grand jury investigation in Alameda County in regard to the use of uncertified patches in the use in that election. The conclusion was to refer to the

Secretary of State. Please do the will of the people and secure accuracy, transparency and accountability in all elections in the State of California. It is a terrible feeling as a voter to not know who really won and if your vote was counted as intended . It is even worse as a citizen to wonder if we truly live in a democracy.

I request the following four items as soon as possible:

- 1) to outlaw the use of DREs in California elections with or without a paper trail immediately.
- 2) to conditionally certify ballot marking devices (BMD) for California use as soon as possible
- 3) to direct the Attorney General of the State of California to initiate new fraud cases on behalf of the voters of California in terms of breach of contract(s), the use of "uncertified patches" into election counting devices, failure to meet basic standards of a viable VVPAT, and failure to adequately keep voting records.
- 4) to initiate your office to work with the University of California and interested non profit organizations to develop and maintain an open source opti-scan vote counting system with a ballot marking device and precinct sorter that can be made available to the California counties and municipalities.

Sincerely,

John Bass

From: Jill Burrows
Sent: Wednesday, August 01, 2007 8:52 AM
To: Voting Systems
Subject: Thank you for protecting our vote

Dear Secretary of State Bowen. Thank you for reviewing the voting systems in California. Research shows that OpScan (which provides a paper ballot) is preferable to the touchscreen systems which have proprietary software and are easily hacked. The sanctity of our vote is paramount to our democracy and we need all of the Secretaries of State to perform their duties and put in place a voting system which is reliable, has a paper ballot, and is not in the hands of private corporations. Again, thank you for taking seriously this public trust. Sincerely, J.C. Burrows

From: Leilani
Sent: Wednesday, August 01, 2007 8:52 AM
To: Voting Systems
Subject: Red Team Review-Voting Machines

Dear Debra Bowen,

Thank you for conducting the "Red-Team" review of the major vote machines used in California. This is critically important to "We, the People". Without a real vote, we have only the illusion of a democracy.

Please do not allow these insecure, hackable vote machines to be used in your State. It is obvious to the Public that these machines with massive security flaws were created intentionally to manipulate the outcome of the election in favor of those in power, namely, Republicans, or those that stand with Corporate power and money. No wonder California has a Republican Governor! Hmmmmmm.

I live in Washington State, and very quickly the whole State was switched to Mail-in Ballot. California could do this for the 2008 Election. Please don't use these insecure machines that can corrupt the vote and our government. The Mail-In Ballot is simple, re-countable, secure.

Thank you for your good work!

Leilani Macmillan

From: Peggy
Sent: Wednesday, August 01, 2007 8:54 AM
To: Voting Systems
Subject: voting machines

Dear Debra,

Please hang tough. If we don't hold the voting machine manufacturers/suppliers accountable, the owners' of these companies and their political sponsors will be running roughshod over all of us from now on.

Regards.

Peggy Midling

From: Faith Voigt
Sent: Wednesday, August 01, 2007 8:55 AM
To: Voting Systems
Subject: Voting machines

Wonderful that somebody is at last taking steps to end this utterly corrupt system.

The rest of the world has difficulty comprehending how any American can presume to monitor voting in other lands when the electoral college system guarantees twisted results - and voting machines are installed to ensure that nobody shows up because their opinion won't be counted anyway.

Best of luck to you, stay strong and restore our faith in the American people.

Sincerely,
Faith Voigt (Brit resident in Germany)

From: Thomas Ryan
Sent: Wednesday, August 01, 2007 8:56 AM
To: Voting Systems
Subject: CA Voting System Analysis

First, I want to commend SoS Bowen for conducting the thorough review of CA election systems. This kind of analysis is long overdue. She has provided a critical national service.

Second, I want to encourage SoS Bowen to

- A) release **all** reports stemming from the study so that the public has a complete view of the hardware and software problems associated with these voting machines,
- B) decertify any machines that cannot be properly audited and pose a risk to upcoming election integrity,
- C) augment the state's auditing requirement to a point where reasonable assurances can be made that elections are accurate,

Tom Ryan, Ph.D.
Arizona Citizens for Fair Elections

From: GENE DERIG
Sent: Wednesday, August 01, 2007 8:58 AM
To: Voting Systems
Subject: Voting Machines

Dear Secretary of State Bowen:

We are not residents of California, but we are citizens of this nation who are very concerned about our voting system and the disarray it is in.

THANK YOU from all of us in this country for conducting the "Red Team" review. That was for the USA, not just California. What California does has huge impact on all of us. Here in Washington State we are correcting voting problems too.

"Vote privately, count publicly" is a motto we like. The machines are merely vote theft waiting to happen. To paraphrase Joe Stalin: "The votes aren't important. Who counts the votes is what is important". Chilling words, I believe.

Thanks again for having the review. Watching from up here we hope you dump the machines and get credibility back in the system.

Our best to you,

Gene and Marilyn Derig

From: Scott Bishop
Sent: Wednesday, August 01, 2007 9:04 AM
To: Voting Systems
Subject: Vote Integrity First

I don't have all the facts, but from what I have heard you have to take some difficult actions. Please do the right thing to protect the integrity of the most fundamental mechanism of our American democracy - the vote. I think you should be listening to the Apollo Alliance folks (<http://www.apolloalliance.org/>) not any part of corporate America. Profits are what corporations are for, not good government by/for/of the people.

I hope we can trust you... -Scott

From: Bureau of Public Secrets
Sent: Wednesday, August 01, 2007 9:04 AM
To: Voting Systems
Subject: Decertify

Please decertify all voting systems that have not passed rigorous inspections. Anything less is capitulating to possible, and in fact likely, fraud.

Ken Knabb

From: pamela cahill
Sent: Wednesday, August 01, 2007 9:05 AM
To: Voting Systems
Subject: voting

Debra Bowen,
Thank you for your courageous attempt to keep our voting system honest.
Please keep up the good work. You our fighting for the millions of
us
who can not and are not able to fight for ourselves.
Sincerely,
Pamela Cahill

From: Monica Mccabe
Sent: Wednesday, August 01, 2007 9:06 AM
To: Voting Systems
Subject: Voting systems

Thank you for reviewing our voting systems. We need a paper trail to keep everyone honest.

Monica McCabe

From: gangadevi
Sent: Wednesday, August 01, 2007 9:06 AM
To: Voting Systems
Subject: Preserve Our Vote

Thank you Debra Bowen.

With so many of our constitutional rights suspended, the only link we have with our democracy now is our vote. As already shown in elections back to 2000, the counting of them is highly suspect.

Please call for paper ballots or printed vote. If an ATM machine can readily spit out a receipt, a voting machine can do the same.

Demand our right to fair elections.

Cordially,
Allen Taylor

From: Robert Weeks
Sent: Wednesday, August 01, 2007 9:08 AM
To: Voting Systems
Subject: Voting Machine Review

Good Morning Secretary Bowen,

Your election to Secretary of State of California was the election result I was most pleased with when it occurred, because the integrity of our voting procedures is the single most important issue before us in California and in many other states. If the election process cannot be trusted then we cease to live in a democracy and it is only a matter of time before the American people have nothing but scorn and contempt for the electoral process.

Thank you so much for pushing for the recent review of the various voting machines. Thank you for being a champion of voting integrity. You will always have my vote. I hope that you can continue to fight for our voting rights.

Thanks again,

Robert Weeks

From: Justice Through Music
Sent: Wednesday, August 01, 2007 9:14 AM
To: Voting Systems
Subject: Please decertify these machines

I am so upset at the votemachine companies, lying to state officials to get these contracts, deceiving the public, harming democracy and doing this to make an extra buck. I want you to hit these companies as hard as possible. Decertify the machines and don't let them come back until they build a machine from the ground up that does the job on all fronts.

And thank you for ordering the review and calling them to task.

Brett Kimberlin

From: Kosta Gus Makreas
Sent: Wednesday, August 01, 2007 9:11 AM
To: Voting Systems
Subject: Let's Get Back to Paper ballots - 'NO' to flawed electronic voting systems

Hello Secretary of State Bowen,

THANK YOU for conducting the review of the major voting machine vendors!

I am an advocate of free and fair elections, so this review is important. I am not surprised that security flaws were uncovered.

Please do **not** certify any of these vendors, either conditionally or unconditionally.

Let's just get back to PAPER BALLOTS and forget the electronic methods. I am a software engineer with 30 years experience, so I know how flawed the vote-counting software is. My whole family and many friends are aware of paperless system problems (yeah, I've been informing them) and now also advocate for a return to the more verifiable, original paper ballots.

California will lead the way back to restoring our Democracy. You have a unique and powerful responsibility to help this by getting us back to Paper Ballots.

Thank you,

Gus Makreas

From: Mike VanLandingham
Sent: Wednesday, August 01, 2007 9:11 AM
To: Voting Systems
Subject: Thank you

Thank you for the Red Team review.

Please make sure that everyone's vote counts !

From: kbeckel@peoplepc.com
Sent: Wednesday, August 01, 2007 9:13 AM
To: Voting Systems
Subject: decertify

Please decertify all faulty voting machines and those with no paper trail.

From: Mickey Shell
Sent: Wednesday, August 01, 2007 9:14 AM
To: Voting Systems
Subject: Gratitude

Thanks for all the work you're doing on behalf of the electorate (and the remains of our democracy). You folks who take on this enormous task are amazing. Just wish the Democrats in Congress were as urgently aware and concerned, because what good is all the work they're doing if they lose their leverage in the next election?

Mickey Shell

From: Anne Barga [mailto:annebarga@charter.net]
Sent: Wednesday, August 01, 2007 9:14 AM
To: Voting Systems
Subject: voting machines

Dear Ms. Bowen,
Thank you for your work in reviewing voting machines.
Please help us to feel secure at our polling places that our votes are recorded accurately by correcting the massive security flaws that were found to exist currently. This is of utmost importance to our democracy and the future of our great Nation.
Thank you,
Anne Barga

From: Beverly
Sent: Wednesday, August 01, 2007 9:15 AM
To: Voting Systems
Subject: kudos

for standing up to the Diebolds ... these election machine companies have shown that they cannot be trusted!

From: Scott Mahood
Sent: Wednesday, August 01, 2007 9:16 AM
To: Voting Systems
Subject: voting machines

Say "NO!" to Diebold. Bring back the paper ballot.

From: dael4
Sent: Wednesday, August 01, 2007 9:16 AM
To: Voting Systems
Cc: evan davis; J30@yahoogroups.com
Subject: Finally to the bottom of the election debate

Thanks for uncovering the truth in the electronic voting systems and how fragile they really are. These machines are not what we need to build the foundation of our Democracy on.

In Ohio, we are faced with the threat that, many counties have destroyed ballots from the 2004 election though many had ballots stored from elections held many years prior.

This is serious business and just as serious is the prosecutorial action. Why do you think they wanted to change the federal attorneys?

I really believe that the time is now to act against any intentional election fraud or mismanagement of the voting process. These actions against democracy must not stand.

I have been close to those here in Ohio uncovering mounds of evidence in election malfeasance from precinct to precinct. I have worked tirelessly to promote the reality of our current system online, helping both Paul Lehto and Dr. Robert Fittrakis in my small way.

Please see:

www.fraudbusterbob.com

<http://neocon-panic-attacks.blogspot.com/> (please look at label list for election related articles)

Stephen Caruso

From: Angela Worden
Sent: Wednesday, August 01, 2007 9:17 AM
To: Voting Systems
Subject: Thank you for caring about the security of our voting system

Debra Bowen,

Thank you for caring about the security of our voting machines. Voting is one of the most important things we do as citizens of a democracy/ republic. You didn't ask me, but I think you should decertify the machines. The integrity of voting is dependant on the security of these machines. Perhaps we need to go back to paper ballots.

Angela Worden

From: snickels
Sent: Wednesday, August 01, 2007 9:19 AM
To: Voting Systems
Subject: Voting Integrity

Stephen Nickels
2880 Trigg Tower
Simpson Illinois 62985
snickels@shawneelink.net

What could be more important than knowing my vote will count, as I intended. Will California lead the Country in requiring all voting machines to be tamper proof? I hope so. Thank you for your time.
Peace & Impeachment,
Stephen

From: Dominick
Sent: Wednesday, August 01, 2007 9:17 AM
To: Voting Systems
Subject: voting machines

Dear Secretary of State Bowen,

I voted for you for many reasons and one of those reasons was that you were going to bring back integrity and honesty back to our voting system. Thank you for conducting the "Red-Team" review.

BUT, and don't you just love it when there is always a BUT?

Please GET RID of all computer generated voting machines. Even if they do leave a paper trail most of these machines can be compromised to change the tallies and Not ever be found out, even with a paper trail, especially with the sophisticated virus programs that are now out there.

Why take that chance to compromise our biggest right ever with the chance that our votes can be tampered with?

Thank you for taking the time to listen to me.

**Sincerely,
Dominick J. Di Noto**

From: Mark
Sent: Wednesday, August 01, 2007 9:17 AM
To: Voting Systems
Subject: Red Team review comment

Dear Deborah Bowen,

I wanted to thank you for conducting the red team review on the four types of voting machines in California. The results I understand indicate quite a few security flaws.

To my knowledge ATM machines are pretty secure but I heard they are 10-20 times more expensive than a single voting machine. Until we can put that much money into a single voting machine to make use it is secure we need go back to a paper ballot system of fill in the spaces or a punch system that leaves a definite verifiable trail.

I would urge you to decertify all of the current electronic voting machines.

Thank you,

Mark

From: Jill Levy
Sent: Wednesday, August 01, 2007 9:21 AM
To: Voting Systems
Subject: Voting machine review

To Debra Bowen,

Thank you so much for the "Red-Team" review! Given that all 4 voting machines were found to have massive security flaws, I feel strongly that they be decertified and another system be put in place. How about a return to the old pre computerized machines that seem to be straight forward and honest?

Sincerely,

Jill Levy

From: Lee Eisenberg
Sent: Wednesday, August 01, 2007 9:23 AM
To: Voting Systems
Subject: voting machines

While I am not a Californian, I consider it a good idea that you are asking for public comments about the topic. Public input is an essential part of democracy.

Lee Eisenberg
Portland, Oregon

From: leipham
Sent: Wednesday, August 01, 2007 9:22 AM
To: Voting Systems
Subject: Safeguard the election process

Please "de-certify" all of the electronic voting machines that are corruptible- including the optical scan machines. We need to have a voting system with a paper trail that is verifiable. I support you in protecting our voting rights.

Kathy Leipham

From: Linda [mailto:lindaseeley@charter.net]
Sent: Wednesday, August 01, 2007 9:25 AM
To: Voting Systems
Subject: Thank You

Thank you so much for watching out for our voting rights. We cannot use voting machines that are hackable! It is absurd. We need paper ballots with bipartisan monitored counting of the votes, just like we used to have.

Thanks again,
Linda Seeley

Jeff Syrop
3389 Mallard Ct
Hayward CA 94542
Home: (510) 581-3973
Mobile: (510) 909-0150
Work: (510) 264-5180

8/5/07

Secretary of State Debra Bowen
California Secretary of State
1500 11th Street
Sacramento CA 95814

Dear Secretary of State Bowen,

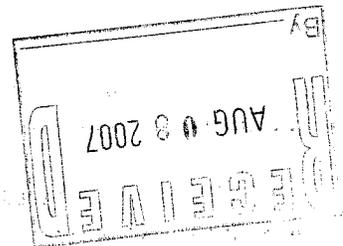
Thank you from the bottom of my heart for having the courage and patriotism to stand up and decertify suspect voting machines. Butte County Registrar Candace Grubbs says, "Election officials in the state of California have worked long and hard to ensure elections come off well, and this is how we are treated?" Is she crazy? Does she value smoothness over accuracy? Our nation is basically being destroyed by President Bush, who LOST the 2000 election to Al Gore, which Ms. Grubbs would know if she would take the time to read the first 75 pages of Greg Palast's "The Best Democracy Money Can Buy." What you are doing is job one if we are to remain a democracy.

I laud your efforts and I pray you maintain the strength to stand up to the people who no longer respect the laws in our Constitution. I urge you to give a copy of *Profiles in Courage* to anybody who hassles you. You truly *are* a profile in courage, and I'm proud that I voted for you.

Sincerely,



Jeff Syrop
Technical Writer
3389 Mallard Ct
Hayward CA 94542
(510) 909-0150



Virginia R. Harris
7777 Bodega Avenue #F-10
Sebastopol, CA 95472

(707) 829-5822
vrharris@sonic.net

August 4, 2007

Debra Bowen, Secretary of State
1500 Eleventh Street
Sacramento, CA 95814

Dear Secretary Bowen,

Thank you for challenging the use of electronic voting machines. I am not in favor of leaving a right as precious as a citizen's vote to vagaries of computers and those who build and program them. As has been proven over and over these machines are not reliable, can easily be "hacked", and cannot be trusted to give an accurate vote count. If there is a question, the machine will only give what it already gave with no way to double check.

I constantly wonder why there is not a standardized paper ballot statewide. With the amount of paper that is thrown away and recycled every year, why not use some of it to make ballots?

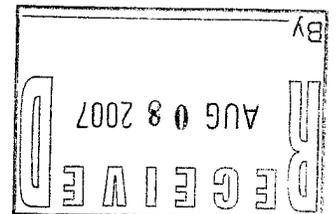
I know as a nation we think that if the technology is available we have to use it. If an optical scanner breaks down, at least there is a piece of paper that can be counted. With the electronic machines, even with a paper receipt, the vote may not be accurate in the machine.

I urge you to outlaw the electronic machines and to consider instituting a standardized paper ballot statewide. Thank you for your attention and consideration.

Sincerely,



Virginia R. Harris



Sheldon Kadish
14320 Addison Street
Apartment 213
Sherman Oaks, CA 91423-1841
Phone/Fax 818-501-5357

August 8, 2007

Secretary of State Debra Bowen
via Fax 916-653-1458

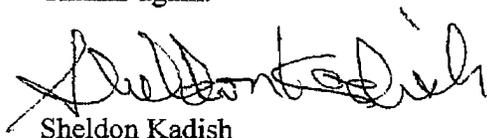
Madam Secretary:
(It still feels so good to say that.)

I want to send you a quick note to say "Thank You" for your stand on election protection. I saw the editorial in the Sacramento Bee saying that decertifying some of the electronic voting systems was going to cause chaos in the February primary. The editorial writer, was wrong. You did the right thing, and I'm proud of you.

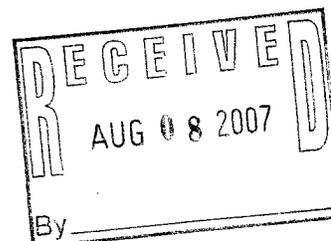
Don't let the mini-minds get to you. If they want their equipment to be certified, they must fix the deficiencies in their machines and furnish your office with open source codes. I'm especially disturbed that the manufacturers of the Inka-Vote Plus system didn't submit their machines and software for certification. If Conny McCormack had put any pressure on them, their submissions would have been made on time.

If LA County has to use paper ballots in the next election, it will not be the fault of your office. The Registrar/Recorder has only herself to blame.

Thanks again.



Sheldon Kadish
(Valley Grassroots For Democracy)



Secretary Of State, Debra Bowen,

8-6-0

I just want to thank you for your tiring efforts to bring back our democracy back to vote with paper ballots and restricted use of the machines.. I had read the article yesterday in the San Diego Union Tribune. I am pleased at your decision and hope you will continue to be strong with our voting rights and no deceptions. I believe in the last 2 presidential elections that it was fixed and many ballots were thrown out. I want our votes to count and have a paper trail. The Diebold machines and others have proven to me to be unethical and corrupt to use. I voted for you as I am a concerned citizen on many matters. But voting is where it all starts! Who we elect and how it is done needs to be protected as we vote.

Thank you,



Joie Ankney

1425 Northrim Ct. #235

San Diego, CA. 92111

858-569-0930 home number

Joie_was_here@yahoo.com



||| AUG 8 2007
By _____

8/6/07

SECRETARY OF STATE BOWEN,

I JUST WANTED TO THANK
YOU FOR PUTTING CALIFORNIA
ON TRACK FOR FAIR AND HONEST
ELECTIONS! ELECTION RESULTS
SHOULD NOT BE IN QUESTION.
AND WHEN THEY ARE WE THE
PEOPLE SHOULD BE SERVED,

Mary E. Fenstermacher
1527 Idaho Avenue
Santa Monica, CA 90403
310-395-3199/310-493-3331(c)
maryfens@earthlink.net

August 5, 2007

Ms. Debra Bowen
California Secretary of State
1500 11th Street
Sacramento, California 95814

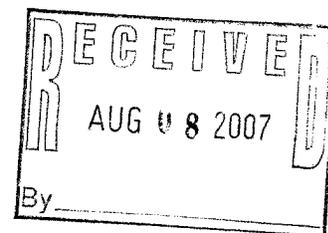
Dear Ms. Bowen,

I am 60 years old and a 23 year resident of California. I prize my right to vote, and exercise it consistently. I am writing to say **thank you** for protecting the right of all Californians to have their votes counted as they are cast.

Your leadership is exemplary. I hope that leaders in other states pay attention and follow suit.

Sincerely yours,

Mary Fenstermacher



Jim Foster

1108 Rosario Drive, Topanga, CA 90290

Tel: 310 4553453 Fax: Home Fax Phone jfoster1@earthlink.net

Sunday, August 5, 2007

Dear Debra Bowen,

Bless you, Debra Bowen. You are protecting democracy.

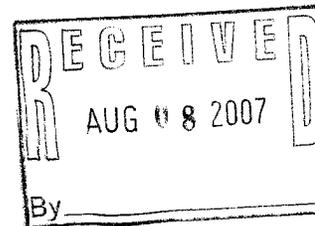
If anything remains sacred in these troubled times, If there's anything all Americans can agree on, it's the rule of democracy.

I voted for you last time and will next time too

Sincerely yours,

A handwritten signature in cursive script that reads "Jim Foster". The signature is written in black ink and includes a horizontal line extending to the right from the end of the name.

Jim Foster

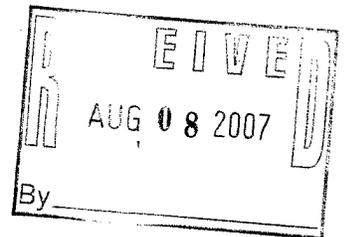


voter machines: 8/6/07

Dear Sect. State Bowen,

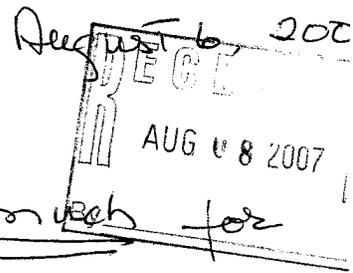
Thankyou for testing all
the voting machines!!!

😊 Sincerely - Will Melchre



Dear Debra Bowen,

Thank you very much for
getting the voting machine
mess straightened out!
Man if we can just scotch that



August 5, 2007

Honorable Debra Bowen
Secretary of State
State Capitol
1500 - 11th St. - 6th floor
Sacramento, CA 95814

Dear Secretary of State Bowen,

As a former election administrator of many years, I want you to know how happy I am with your actions against the corrupt computerized voting machines which have so damaged our democracy.

With your guidelines in place, it will become extremely difficult for the makers of these machines to continue to steal our elections as they have for the past 8 years. How different our country and the world would be today if Al Gore were our president (who would have been elected except for the fraudulent voting machines) instead of George Bush (who has now stolen two elections.)

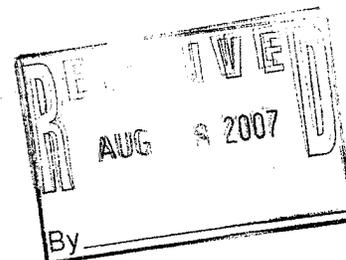
May the rest of our country follow your lead!

Respectfully submitted,

Evelyn Roberson

Evelyn Roberson
113 Larkspur Drive
Santa Rosa, CA 95409

PS Enjoy the roses, hope they arrived OK.



From: Mark Reback
Sent: Wednesday, August 01, 2007 10:20 AM
To: Voting Systems
Subject: I support decertification of all electronic voting machines in California

Dear Secretary of State Bowen-

Thank you for your efforts to illuminate the security flaws within all electronic voting machines in use in California. I urge you to hold the voting machine companies accountable and decertify all electronic voting machines in California in time for the February 2008 election.

As you know, last week, the results came in from California's top-to-bottom³Red Team² review of the four major vote machines used in that state, where a crack team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES.

Obviously, the machine vendors are extremely opposed to the review results and any action by the Secretary of State's office, and they are trying hard to lobby against any action.

Secretary Bowen, you now have to make a crucial decision. You know what you have to do. Decertify all electronic voting machines and require a paper voting trail for all elections in California.

The people of California thank you and your office for conducting the³Red-Team² review, and please follow through and decertify all electronic voting machines in California because they do not have reasonable security standards.

Sincerely,

Mark Reback

From: Caryl Green
Sent: Wednesday, August 01, 2007 10:18 AM
To: Voting Systems
Subject: Please decertify

Thank you for considering to decertify the voting machines. It is the only right and moral thing to do. Thank you for reading this.

Caryl Green

From: juliehoy On Behalf Of Julie Hoy
Sent: Wednesday, August 01, 2007 10:20 AM
To: Voting Systems
Subject: Please decertify electronic voting machines in CA

Dear Secretary of State Bowen,

Thank you for conducting the "Red-Team" review. I'm appalled at how insecure electronic voting machines are. They are a threat to democracy, because the voters don't decide the elections, the vote counters decide the election. Please take a stand against electronic voting machine companies and do allow their faulty machines to be used in the state of California.

Sincerely,
Concerned Citizen
Julie Hoy

From: Francis Scalzi
Sent: Wednesday, August 01, 2007 10:25 AM
To: Voting Systems
Subject: Touch Screen Voting Machines

Secretary Bowen:

Although I am not a resident of California, but Arizona, I wish to offer my gratitude to you for your pursuit of the problem with California touch screen voting machines which have recently been shown to be so easily corrupted by computer researchers. Since our voting franchise is so fundamental to our democracy, there can be no more urgent national problem, and not one restricted to any single state. I hope that you will continue your attention to restoring the integrity the voting process in California and set an example for other states to follow suit. In my own opinion, the touch screen voting machines have long been demonstrated to be a total failure all across the nation, and should be banned and removed entirely from the voting process. If our nation is able to spend many \$ billions per month in a failing "adventure" in Iraq, we certainly should surely be able to unsure that we have honest and reliable voting procedures.

Again, thank you for your efforts.

Francis V. Scalzi

From: Bill Sanchery
Sent: Wednesday, August 01, 2007 10:25 AM
To: Voting Systems
Subject: Decertify the machines, PLEASE!!!

Dear Madam Secretary:

Thank you for stepping up and having the electronic voting machines tested, confirming what we all knew, they can be manipulated. I understand that you only have a few days to decide whether to decertify the flawed machines. I am sure there is great pressure on you from high places to do nothing. Please, do not give in to that pressure. Please continue to be a champion of the people, and decertify all of them. It is outrageous that the vendors foisted these crooked machines on us in the first place. Please decertify them and secure verifiable paper ballots for California for the 2008 presidential elections, and set an example for the nation.

Thank you for your courageous campaign for accurate elections, the cornerstone of a democracy. And thank you for being one of a very few politicians that we can count on to do the right thing.

Sincerely,
Bill Sanchery

From: Carol Fisher
Sent: Wednesday, August 01, 2007 10:30 AM
To: Voting Systems
Subject: Red Team

Ms. Bowen,

I salute you for standing up to the abuses inherent in these election machines. We felt the devastating impact of their hack-ability during Ohio's 2004 elections. Thank you for using your position to redress to this dire threat to our voting rights.

With heartfelt appreciation--
Carol Fisher

From: Stu Anderson
Sent: Wednesday, August 01, 2007 10:27 AM
To: Voting Systems
Subject: Please de-certify electronic voting machines

Dear Madam Secretary,

Thank you for having the electronic voting machines tested and proving that they can be tampered with. Please continue on your courageous path and decertify all of these machines.

I am a graduate of MIT and I design embedded control systems - the class of machinery that includes voting machines. It is very hard to create software that is flawless. It is harder to create software systems that can't be tampered with. And darn near impossible to verify - especially if the manufacturers are reluctant to open their systems to public scrutiny and testing.

California needs verifiable paper ballots, not "magic boxes" from private vendors!

Thank you for standing up for the common good.

Stu Anderson

From: audreyafranklin
Sent: Wednesday, August 01, 2007 10:31 AM
To: Voting Systems
Subject: Voting machines negate a citizens right to vote and expect it to count....

The so-called "Red Team" has reviewed the four major vote machines used in California and found them seriously lacking in credibility. In short, a crack team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES&S. I think they should be disallowed and written off as bad investments in infrastructure and paper ballots should be re-instituted. At least, they can be re-counted through scanners and show true results.
Audrey A. Franklin

From: Astrida R. Blukis Onat
Sent: Wednesday, August 01, 2007 10:32 AM
To: Voting Systems
Subject: Voting Rights

Thanks to Debra Bowen for all her work in support of voting rights.
Keep up the good work.

Astrida Onat

From: Janie Sheppard
Sent: Wednesday, August 01, 2007 10:34 AM
To: Voting Systems
Subject: Please decertify machines

Having contributed to your election on the premise that you would decertify any machines that could be hacked I was very disappointed to hear that you were not going to do that.

Please reconsider your decision and cause the vendors and the reluctant county elections officials to jump through the hoops required to get hack-proof machines in place for the primary election. Or require hand counting.

I have worked in elections in Mendocino County every election but one since 1998 and I am appalled to think that our democracy is being undone by "machines." It's horrifying to me.

Thank you very much,

Janie Sheppard

From: Steve Phillips
Sent: Wednesday, August 01, 2007 10:34 AM
To: Voting Systems
Subject: Decertify machines from Diebold, Sequoia, Hart, and ES&S

Dear Debra Bowen,

Thank you for conducting the "Red-Team" review of voting machines.

Now that the team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES&S, it seems obvious to me that the design flaw is intentional so that they may manipulate elections. Decertification of these flawed machines and using paper ballots that can be counted is the only way that true voter intent will be realized.

Thank you, Steve Phillips

From: Mary Evans
Sent: Wednesday, August 01, 2007 10:36 AM
To: Voting Systems
Subject: California is so important!

Dear Secretary Bowen,

Thank you for investigating the voting machines. If they are not up to par, perhaps California could be the first state to have hand counts of paper ballots at the precinct level. In public view, this is an old fashioned, yet fool-proof way to have honest elections.

Thank you for your fine work that affects the entire nation.

Sincerely,

Mary E. Evans

From: Jeff Galvin
Sent: Wednesday, August 01, 2007 10:37 AM
To: Voting Systems
Subject: Please DO NOT certify flawed machines

Dear Ms. Bowen

If they have security flaws, or if they do not give a paper trail for audit purposes. PLEASE DO NOT certify those electronic voting machines.

- Jeff

Jeff Galvin - CEO
1Mart Corporation

From: Barbara Whipperman
Sent: Wednesday, August 01, 2007 10:38 AM
To: Voting Systems
Subject: voting machines

Debra Bowen -

Thank you so much for running the hacking test of voting machines! I know the results present logistical problems for our next elections, but we need verifiable vote counting. Please do not certify machines which allow fraudulent vote counting as a possibility. Back to hand counted paper ballots if necessary!

Barbara Whipperman

From: heather gray
Sent: Wednesday, August 01, 2007 10:38 AM
To: Voting Systems
Subject: thank you for the opportunity for review and comment

Dear Ms. Bowen,

At no time in recent history has the security of and confidence in our voting system been more important. As a former California resident and current resident of the notorious Broward County in Florida, where our votes were challenged, stolen, shredded, stashed in giant black garbage bags and dumped into neighboring districts' dumpsters, and thousands upon thousands of absentee ballots held at a regional post office for weeks and not delivered until it was too late to vote, for lack of a penny in postage, I am extremely sensitive to voting security and ethics issues.

Please take very seriously the ends to which this administration and its operatives have attempted to suppress, cage, disenfranchise, harass, and otherwise nullify the efforts of millions of Americans to participate in this eroding democracy.

And if you are of that party, and happy with their agenda, remember, that once in play, these tactics can be used by ANY party in power for their own ends, independent of the will of the people.

Sincere, respectful regards and appreciation,
Heather Gray

From: Patricia Morgan
Sent: Wednesday, August 01, 2007 10:37 AM
To: Voting Systems
Subject: Voting Machines

Thank you for conducting the "Red Team" study.

Please do your utmost to be sure that California voters can trust that the ballots they cast will be counted.

Patricia Morgan

From: psbandrox@aol.com
Sent: Wednesday, August 01, 2007 10:40 AM
To: Voting Systems
Subject: hackable voting machines

Hackable voting machines are unacceptable. They are in large part responsible for the terrorist reign of the bush crime family as the whole world knows that Al Gore was elected president. You are, then, largely responsible for the Iraq debacle and the deaths and maiming of many hundreds of thousands of people on this planet. The blood of all those killed and wounded in Iraq is on your hands!

From: Michael J. McGillivray
Sent: Wednesday, August 01, 2007 10:41 AM
To: Voting Systems
Subject: Public comment, Voting credibility

California's actions in assessing the integrity of electronic voting are being watched all over the country. I believe this amounts to a crisis in our democracy. Thank you for undertaking a serious review. The vendors of flawed equipment, by demonstrating their incompetence, have made the case for those of us who do not want corporations running our elections. Please understand that, regardless of the aggressive lobbying you're likely to run up against, a thankful nation will support your forthright actions.

Michael J. McGillivray

From: Eric Ranvig
Sent: Wednesday, August 01, 2007 10:45 AM
To: Voting Systems
Subject: Wanted:honest and true results

Dear Secretary Bowen,

Thank you for seeking our input regarding voting systems in California.

Our society is so obsessed with efficiency in terms of time, but currently voting technology cannot deliver efficient results without compromising accuracy or being susceptible to tampering and fraud. Is it so terrible to have a voting system that takes a few more hours to tabulate, but is accurate and tamper free? The corporate media must have the results within an hour in order that a winner can be declared and regular programming can resume. However, for everyone else there is no rush. We simply want the results to be honest and true.

The manufacturers of electronic voting machines knew in advance that they might get caught producing unreliable machines and they produced them anyway. Now they have been caught. They should eat the expense of their poor calculation.

This may sound extreme, but I would rather go back to simple paper ballots and let it take a few days to count the votes, before I would accept unreliable electronic voting machines.

Please, keep your priorities straight: honest and true results over quick but unreliable results.

Thank you for your concern for this important issue.

Sincerely,

Eric Ranvig

From: Bolsero@aol.com
Sent: Wednesday, August 01, 2007 10:46 AM
To: Voting Systems
Subject: Voting Machines

We saw what happened in 2000 and 2004 when Bush was ILLEGALLY selected.NO MORE MACHINES. I want PAPER BALLOTS!Thank you,Debra.

From: Bruce Berkowitz
Sent: Wednesday, August 01, 2007 10:48 AM
To: Voting Systems
Subject: voting machines

After the results of the Red Team review of the voting machines it would seem the only prudent thing to do would be to decertify those machines that failed until they could be fixed to the point of passing the review.
thank you
Bruce Berkowitz

From: Byron C. Bellamy
Sent: Wednesday, August 01, 2007 10:44 AM
To: Voting Systems
Subject: Election Integrity

Dear Deborah Bowen:

I support your actions wholeheartedly. I trust you as a public servant, think you're smart, and know you're a good American. If you can't fix this, no one can.

I'd like to see a return to hand-counted paper ballots. I don't trust a single electronic voting machine vendor -- I think they've all engaged in treasonous skullduggery, and a return to absolute election integrity is the solution. However -- you're the dragonslayer, and whatever it is possible for you to do, do it. I helped elect you, and I trust you to do the right thing. Make your decision -- I'll support you whatever it is.

I still think your election was the single most important election in modern American history. I think your role in the rebirth and revitalization of the United States cannot be overstated. You are at the center of the cyclone, and I know you can do this -- I have such faith in you as a person.

Thank you for being such a straight arrow. I know you'll protect everybody's votes, be they Democratic, Republican, Independent, Green, or Silly Party.

Sincerely,

Byron C. Bellamy

From: Guruneil
Sent: Wednesday, August 01, 2007 10:49 AM
To: Voting Systems
Subject: election theft by bushit

We don't want the bush-cheney crime gang stealing any more of our elections. Make sure it never happens again!

From: Jeralene Corley
Sent: Wednesday, August 01, 2007 10:57 AM
To: Voting Systems
Subject: Re: voting machines

Debra Bowen
CA Secretary of State
1500 11th Street
Sacramento, CA 95814
July 30, 2007

Ms. Bowen:

We are looking to you to ensure that people with disabilities have the opportunity to vote independently and privately. People with disabilities want both an accessible and secure vote. California still has to meet the HAVA requirements for an independent and confidential vote. Federal legislators realized last week that there was insufficient time to decertify and develop entirely new voting systems in time for the 2008 elections.

Currently certified voting systems provide greater access to voting than any other in the past. There was a suggestion that the current machines remain available only to persons with disabilities. People with disabilities want their votes to be cast in a secure system and be counted just like everyone else. To say that these machines are only good enough for this particular population is unacceptable and discriminatory.

We support the State in including accessibility testing as part of the State certification process. Our hope is that State accessibility testing will help increase the accessibility of voting systems for the cross-disability community, including persons with cognitive disabilities. We recognize that there is a need for continued research and development of voting systems to increase their accessibility, vote verification capabilities and security.

While currently certified voting systems are not perfect, they should be used until new more accessible machines are available. We cannot deprive the disabled community from practicing their right to vote.

We have been a resource to you and would like to continue to work with you to ensure accessible and secure voting in California.

Respectfully,

Jeralene (Jeri) Corley

From: Michael-David Sasson
Sent: Wednesday, August 01, 2007 10:50 AM
To: Voting Systems
Subject: Please decertify insecure voting machines

Thank you for conducting the "Red-Team" review. Please take the next logical step and decertify the machines that do not meet reasonable security standards and hold companies accountable for lying and deceiving the state officials.

Sincerely,

Michael David Sasson

From: James Hosley
Sent: Wednesday, August 01, 2007 10:51 AM
To: Voting Systems
Subject: Voting Machine Accountability

Secretary Bowen, thank you for conducting the electronic voting machine testing. I'm sorry that the results were so disappointing.

At this point, I hope that you will decide to allow nothing less than secure and totally accountable (paper trail) voting machines to be used in California.

This is a tough decision, but please act on what you told the voters before you were elected.

Voting is such an act of faith and trust in a system run by our government.

Voters need to be assured that their vote is recorded accurately and is counted correctly.

Thank you.

James K. Hosley

From: Susan Arth
Sent: Wednesday, August 01, 2007 10:51 AM
To: Voting Systems
Subject: bring back paper ballots

Dear Secretary Bowen,

I am writing to express my stong feelings AGAINST touchscreen voting.

It is

clear from your recent study and report that the machines currently in use

are far too susceptible to manipulation and fraud for we voters to feel

confidant that our votes will be fairly counted.

Please return California to a system of paper ballots with optical scanners.

In the event of suspected shenanigans or technological failure, the paper

ballots can be used to double-check the talleys. This is the system used by

nearly every other civilized country in the world. It would be worth waiting

a day or so for election results (if necessary) to ensure that the votes

have been accurately counted.

Thank you for making our voting rights your main priority. I surely appreciate your efforts, and I know I have plenty of company.

Susan Arth

Sue Arth

CEO

Sea of Change

From: Kathy Kearney
Sent: Sunday, August 05, 2007 8:36 AM
To: Voting Systems
Subject: THANK YOU!!!!

Thank you for decertifying the Diebold and Sequoia machines. This is a HUGE step toward restoring election integrity in the United States.

I'm

sure there will be fierce political reaction, but there are lots and lots of us out here behind you. Great job!

Kathleen Kearney

From: Richard M. Wolfe
Sent: Wednesday, August 01, 2007 10:53 AM
To: Voting Systems
Subject: Test Results!

Debra:

Super thanks for getting at the truth! Please protect our voting system from the dictators!

If electronics can't be foolproof, then let's go back to paper... :-)

Richard M. Wolfe

From: Sarah Rah
Sent: Wednesday, August 01, 2007 10:53 AM
To: Voting Systems
Subject: voting machines

Debra Bowen
Thanks for the Red Team Project. Please be sure our voting rights are protected, and insist on voting machines with paper trails.
Sarah Rah

From: Mike Suddarth
Sent: Wednesday, August 01, 2007 10:55 AM
To: Voting Systems
Subject: De-Certify

Hello

I gave to your campaign. I encouraged my friends. I voted for you. California once was THE most progressive state in our union. Let us lead once again. Lead the nation back to paper ballots. Please, take voting machines away. Stop the privatization of our democracy.

Fred M. Suddarth

From: Suzanne Lowe [mailto:suzelowe@sbcglobal.net]
Sent: Wednesday, August 01, 2007 10:56 AM
To: Voting Systems
Subject: Thank you for analyzing voting machines+++

Secretary Bowen. It seems like this effort is one of the most important activities that the government can do to protect our democracy. The voting machines have been proven to be hackable and should not be approved. Paper ballots or backup are fine.

Keep up the good work.

Sincerely,

Suzanne Lowe – Teacher

From: Jackie Riskin [mailto:jackieriskin@yahoo.com]
Sent: Wednesday, August 01, 2007 10:56 AM
To: Voting Systems
Subject: Debra Bowen's top to bottom review of voting systems

I just want to thank you so much for your wonderful work. I know the "wolves" will attack you, and I hope and assume that you will continue to do the right thing for the voters of California.

I am attaching 3 of the signs that we created for the press conference on July 30th. I think you'll appreciate them. They did appear on T.V. and in print the following day.

Jacqueline Riskin

Thank You

DEBRA BOWEN

Secretary of State

Protecting Our Votes

... As Promised!

**TOUCHSCREEN
VOTING MACHINE:**

\$5,000.

PAPER BALLOT: 10¢

FAIR & ACCURATE ELECTIONS:

PRICELESS!!

**Debra Bowen -
Cleaning Up the
Voting
Machines!**



From: Mike Gruener [mailto:mgruener@bellsouth.net]
Sent: Wednesday, August 01, 2007 10:59 AM
To: Voting Systems
Subject: Thank you Debra

Dear Secretary of State Bowen,

Thank you for your leadership in voting rights reform. I wish we had it so good in Florida.

Sincerely,

Mike Gruener

From: Harley Gorrell
Sent: Wednesday, August 01, 2007 11:02 AM
To: Voting Systems
Cc: ejschuller@yahoo.com
Subject: Comment on the voting machines...

I have been programming for over 20 years and it is my opinion that the voting machines should be decertified.

They should be decertified not only because of the current round of flaws, but also for the suspicion and distrust that they introduce to the voting process. Not everyone will have the skills to understand what happens inside a computer, but all citizens would be able to inspect paper ballots.

Paper based systems have their problems, but forging or tapering with physical ballots requires more effort and could leave a trail of physical evidence as to what really took place.

My preference would be to have a a voting system which allowed for manually marked ballots and electronic systems which produce a paper ballot for the voter. After visually inspecting the ballot for correctness the voter then places in in the box. (To aid in the counting process the votes might also be encoded as machine readable text. In the event of a mismatch, the human readable text is the binding value.)

harley.

From: Carol Kline
Sent: Wednesday, August 01, 2007 11:02 AM
To: Voting Systems
Subject: Thank you and please decertify machines

Dear Debra Bowen,

Thank you for conducting the "Red-Team" review. Please decertify the machines that do not meet reasonable security standards and hold the companies accountable for lying and deceiving the state.

Thank you again,

Carol Kline

From: Jack McCurdy
Sent: Wednesday, August 01, 2007 11:02 AM
To: Voting Systems
Subject: Voting machines review

Dear Ms. Bowen:

I strongly support you taking action to implement the recommendations of the Top-to-Bottom Review of voting machines certified for use in California and applaud your diligence and courage in attacking this crucially-important matter as our new Secretary of State. I am urging the Humboldt County Democratic Central Committee to adopt a resolution supporting your efforts and lauding your initiative in this regard.

Please keep us all informed with up-to-date postings on your web site about developments in instituting protections for the integrity of our voting process in California.

Thank you,

Jack McCurdy

From: old age
Sent: Wednesday, August 01, 2007 11:03 AM
To: Voting Systems
Subject: Electronic Voting Machines

Dear Secretary of State Bowen,

Please do not certify the electronic voting machines that you have before you. There are just too many problems and uncertainties to put these machines into use. Even with a paper trail.

Than you,

Miles & Erica Anderson

From: Ahcros
Sent: Wednesday, August 01, 2007 11:04 AM
To: Voting Systems
Subject: Make our voting machines safe!

Dear Ms. Bowen,
You ran on a platform of cleaning up our voting procedures. As a result, I both contributed to your campaign and voted for you.

Now the time has come to act. We must have accountable, reliable voting machines that produce verifiable paper results before the next election!

Please take whatever actions are necessary to ensure our voting safety, just like you promised when you campaigned.

Thank you,
Ann Crosby

From: Ainger. Joel
Sent: Wednesday, August 01, 2007 11:05 AM
To: Voting Systems
Subject: Voting Machines

Get rid of all electronic voting machines. Paper ballots, hand counted is the only way. Otherwise, we just get buggered by fascists. This is the common knowledge of the day, and to disregard it is an act of war against the dignity and decency of the people.

From: WWMarkB@aol.com
Sent: Wednesday, August 01, 2007 11:05 AM
To: Voting Systems
Subject: Decertify the voting machines

Dear Ms. Bowen,

Thank you for conducting the "Red-Team" review. I urge you to decertify the voting machines because they do not meet reasonable security standards. I also urge you to hold the companies accountable for lying and deceiving the state officials.

Sincerely,

Mark Rosin

From: Roy Tuckman
Sent: Wednesday, August 01, 2007 11:06 AM
To: Voting Systems
Subject: Voting Machines

Dear Ms. Bowen,

Thank God we have some good guys in office - thank you for having the voting machines tested. We may yet avoid seeing President Giuliani in 2008.

The machines should be junked - returned for refund if possible and set a tone for the nation. If they MUST be used, then they should all be programmed for liberal candidates.

As for our voting technology... When I was a boy, I would go to the polls with my mother and see her vote (for FDR). There IS a paper trail
- it is called BALLOTS and like other advanced industrialized nations, there should be no machine between the voter and the vote; no political machine and no computerized machine.

No one in their right mind will care if it takes more hours to get a CORRECT vote count.

Sincerely

Roy Tuckman

From: Candice Basham
Sent: Wednesday, August 01, 2007 11:07 AM
To: Voting Systems
Subject: Please return to paper ballots...

We can count them! We can recount them! The paper can be created from recycled paper and recycled again.

Remember how the country was going for Kerry in a landslide on the day of the last presidential election. Even though every possible Democratic voter who could be tricked out of a legitimate vote had been taken care of, Kerry was winning. But then the vote count started flipping. Karl Rove said he never had any doubt as to the outcome because "he who counts the votes wins." Black box voting is for single-party dictatorships.

I vote only by paper ballot.

American democracy is so compromised by lobbyists and Congresspeople who have to spend their time making money for the next campaign so they can buy TV ads on the public airwaves. If we can return to paper balloting, count and recount and have faith in our elections, maybe we can learn something from England and provide free, substantial ads

on TV for legitimate candidates. The corporate-consolidate media isn't providing much of a real function to a democracy.

With real democratic elections, we might even be able to enable citizens to see a doctor when they need to...wouldn't that be advanced?

Sincerely,

Candice Basham

From: Sam Durant
Sent: Wednesday, August 01, 2007 11:09 AM
To: Voting Systems
Subject: decertify electronic voting systems

Dear Secretary Bowen,

Thank you for conducting the Red Team review of what we now know are fatally flawed voting machines. As a voting, taxpaying Californian I urge you to unconditionally decertify all electronic voting machines. Nothing less than our Democracy is at stake.

Sincerely,
Sam Durant

From: Marian Katz
Sent: Wednesday, August 01, 2007 10:57 AM
To: Voting Systems
Subject: decertify flawed voting machines

Dear Secretary of State Bowen:

I have been following this issue of voting machines for a long time. After two presidential elections in which there was evidence of manipulation of votes, which may have (and I believe did), influence the election outcomes and deny the majority preference, enough is enough.

Thank you for conducting your "Red-Team" review of the four major vote machines used in our state. I am aware that this review found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES&S. That should be enough to ensure that you decertify them, at least until the problems are fixed. It is not enough to fix the machines, it is also imperative that there be a paper trail for EVERY California vote, and you must hold the companies accountable for lying and deceiving state officials.

As Secretary of State you must continue to stand up to the machine vendors and protect Californians' voting rights.

Thank you for your service and integrity.

Yours,
Marian Katz

From: Fisher, Jean E.
Sent: Wednesday, August 08, 2007 7:29 AM
To: Voting Systems
Subject: Thank you, Debra Bowen!!!

Dear Secretary of State Debra Bowen,

Thank you so much for taking a strong stand for democracy and standing up against corruption in our election system. The right to vote and know that our vote counted correctly is the basis of democracy and once tampering with our votes begins, democracy crumbles. Unfortunately, this is already happening in our country and it must be stopped! You have taken the courageous step forward to stop corruption in our voting system!!

There is a naivety that exists in the supporters of technology, in that just because it's "technical", it makes for a better product. The "tech" industry does not have the vision to foresee problems, thereby lacking the intelligence to prevent future problems. Then you add the factor of corruption and you set a path for disaster.

My dad had a stroke resulting in dementia. For three months, he was in and out of hospitals, rehab centers and nursing homes. They kept pumping him with different drugs in attempts to stabilize his blood pressure. What I discovered was that they were alternating with digital and manual blood pressure taking. Each "machine" gave different readings. At one appointment, the digital reading was high and the nurse said she would retake it with the manual "machine". I asked which method was more accurate - she said manual! I asked why then do you use digital - she said because it was "faster"!!! I demanded the doctors/nurses use manual only for taking my dad's blood pressure and within about 2 weeks his blood pressure was stabilized with the correct medication!

My point with this story is that the "high-tech" method is NOT always the best method for accuracy. For accuracy in voting, I would much rather wait a week or two to know the REAL winners in elections. No computerized voting!!! Just because they're faster does not mean they are accurate. The speed of high-tech voting also makes it easier to corrupt and then hide the corruptions.

PLEASE continue to do your good work and never, never cave in to the corrupt corporate lies and cover-ups of the "Diebolds"!! Tell the "Diebolds" to take a hike!!

I will continue to support your diligence to stand up to the corporatizing our voting system!!

THANK YOU!!

Jean Fisher

From: Kathleen Wynne
Sent: Sunday, August 05, 2007 5:45 PM
To: Voting Systems
Subject: THANK YOU

Dear Secretary Bowen:

I wanted to give my heartfelt thanks to you and your staff for your bold and courageous actions on behalf of all citizens of this country. Decertifying these machines was the right thing to do. Now is the time to take election reform a step further.

There is a growing coalition of citizens who support hand counted paper ballots at the precinct on election night. Democracy for New Hampshire and Paul Lehto conducted a Zogby Poll and found that 92% of the American people would like to "see" their votes counted. This cannot be done with any voting machine. In fact, since the advent of these machines, citizens no longer feel they are part of the elections process, merely bystanders because the machines are inherently secret, require expert oversight and control and will never be citizen friendly.

The machine advocates have always claimed that hand counts are more prone to fraud. However, they've never been required to prove that their assessments against hand counts were correct. I propose that, while you wait for the vendors to respond to your demands in order to be recertified, let's have an open, public debate comparing the merits of hand counts vs. machine counts. Let's get the evidence out in the open for the public to see and let the truth be the judge of which method is the best in protecting the integrity of our elections. The people deserve to know the facts on both sides of this issue.

I urge you to please have someone from your office contact me to discuss the details of conducting such a debate. I am certain once I have had the opportunity to explain the who, where and how this could be done, I believe you will see that such a debate will make the difference in reestablishing confidence in our election process to the American people that will transcend the recertification of these voting systems.

Sincerely,

Kathleen Wynne
Former Associate Director Black Box Voting.org
Founder HCPBnow.org
Member VoteRescue.org

From: Stuart Kirkham
Sent: Sunday, August 05, 2007 1:48 PM
To: Voting Systems
Subject: Thank you

I would like to thank you for addressing this serious crisis that threatens our nation's democracy. I strongly urge you to ensure that our elections are fair, that everyone has access, and that there is accountability in the results.

Personally, I would encourage moving to a statewide (if not nationwide) standard whereby the official vote count is tallied from paper ballots (collected and tabulated under strict supervision) with electronic scanning used to provide an unofficial but quick tally of results (as well as providing a check on the official tally). Do not be bullied by people who claim that quick results are necessary to prevent a crisis. This argument is false, and people who use this argument are creating a contrived crisis. Remember in the 2000 presidential election, that even though the Bush camp was crying "crisis!" that 75% of Americans favored letting the vote count take as long as it needed.

Please continue to stand up for democracy and against detractors for improving our electoral system. Voting in elections is the cornerstone of our democracy, and people must have faith in the voting systems if they are to participate. It boggles the mind to think that anyone in our country would oppose such reform. Indeed, when I hear people defending these unaccountable voting machines, I immediately become suspect of their motives.

Also, the criticism that testing was carried out under unrealistic conditions is disingenuous. I am sure that I do not need to remind you that in the Florida election of 2000, that evidence suggested that Diebold's leadership was conspiring with Republican personnel on delivering the election for the Republicans.

Please, do whatever it takes to make these elections fair and accountable. I am partial to the idea of paper ballots. And do not let county officials dither and delay to prevent the implementation of reforms, as they will undoubtedly blame the "failure" upon you.

I wish you the best of good fortune in this most important struggle for our democracy.

~~~~~  
William Stuart Kirkham  
Ph.D., Geography

From: Kelsey Ramage  
Sent: Saturday, August 04, 2007 10:37 AM  
To: Voting Systems  
Subject: THANK YOU FOR DE-CERTIFYING

Dear Sec of State Bowen and staff

Thank you so much for your splendid courage, and your admirable determination to stand up for election integrity!!! Your decision to de-certify the main voting machines inspires my grateful respect, and helps restore voter confidence.

Facing tremendous pressures from all sides during this crucial time, you stepped up to demand honest elections, that most vital underpinning for our state, and our nation. These slimy voting systems have finally met the light of day. By providing the leadership we expect from California, your decision and clarity help guide the rest of our nation toward restored honesty and strict accountability in our elections. Hooray!

Thank you very much for your integrity, your bravery, and your heroism.

May peace and blessings flow to you,

sincerely,

Kelsey Ramage

**From:** Phyllis Huster  
**Sent:** Saturday, August 04, 2007 9:22 AM  
**To:** Voting Systems  
**Subject:** Status of Georgia Lawsuit against State of Georgia and Diebold by citizens

Dear Ms. Bowen:

I want to applaud you for your very brave, courageous recent decertification of electronic voting machines in California. I am writing to update you on our lawsuit in Georgia, a lawsuit Bev Harris calls one of the 2 most important election integrity lawsuits in the nation. We have multiple documented counts of why Diebold machines in Georgia both Optiscan and DRE are NOT CAPABLE of providing secure, auditable elections and we are using this lawsuit to demand the complete decertification and remove of Diebold as a vendor to the state. While now the suit has no damages associated, let me assure you the discovery we have already received puts us in a nice situation to begin criminal proceedings against elections officials who by state constitution and election law are bound to both manage honest elections and secure an integrity based voting system for their citizens. We have already won 2 counts of our suit and the press release of this success is attached below. We feel with the discovery gotten to date, we can prove all counts of our lawsuit.

This may not be apparent to you now, but your only choice in California to have a secure election is to go back to Hand counted paper ballots. But I can advocate a way to go from

voting machines back to paper in a smoother stepwise fashion that does not compromise quality. I am a 20 year telecomm veteran. I recently launched 10 releases of software for AT&T and Tmobile respectively with software that serves 20Million customers. Both companies were only able to achieve 91.6% and 95.5% software quality, which is industry standard for telecomms, the enterprise software quality standards are MUCH MUCH MUCH lower. Diebold I'm sure does not have such HIGH pass rates on their software quality and have never published any testing standards to this nature. This means, if translated to Diebold, which they cannot say they are that high quality, but let's assume they achieved telecomm quality rates of 95% in their software, because ALL SOFTWARE RELEASED has flaws, flaws you cannot predict till that routine is executed, you are then telling 5 out of 100 voters their votes will not be counted(or more voters if the bug involved entire machines losing their memory which I have attached below evidence from over \$30,000 I spent buying the election data from the 2004 election.

There is no similar quality tradeoff in the hand counted paper ballots world, for each ballot a citizen fills out, assuming UNBROKEN CHAIN OF CUSTODY to the ballot box and same night citizen counting of the votes, there is 100% accuracy and 100% accountability for every ballot. As a 20 year telecomms software veteran, I say to you THERE IS NO TECHNOLOGY WAY TO RUN HONEST INTEGRITY BASED ELECTIONS. Paper once marked cannot be unmarked except by perceivable means, software once marked, can be remarked 1,000 or a million times without notice to anyone because of the nature of software. Software, Dear Ms. Bowen, software will never produce secure elections. So that leaves you 2 choices.

1. Hand counted paper ballots

2. Software based elections with a Single Race, per precinct randomized race audit. The argument against this is the cost of audits, the problem with timing, the problem with what happens when the machines don't add up to the audit, triggering a statewide full recount which adds weeks to the after the fact election. TRUE PURIST election freaks like me say the counting has to happen on election night, in full view of citizens with video cameras as the ONLY WAY to ensure an honest election. so i'm only advocating #1 above. But you could feasibly use the precinct level, randomized race audit (for each precinct the Elections director puts all races in a hat, picks a race out randomly for all thousands of precincts in your state, guaranteeing the randomized, quality of the audit. I will also say that for all the audits and recounts that were paid for and conducted in Ohio (by the green/libertarian party) by the Busby/Bilbray folks , in New Mexico, in Georgia, in other parts of country after 2004 and 2006 elections, NONE OF THE AUDITS or RECOUNTS were ever fully allowed to continue, as Republicans flew in GOP Staffers from DC to destroy the ballots (in OH the ballots are gone) and in San Diego, the similar tactic was used as in 2004 when Bush and his GOP "Brooks Brothers" flew into Miami where the count was going solidly to Gore, they flew in \$1M worth of staffers to disrupt the counting, to prevent the citizens from counting the ballots. You stand on shakey legislative and legal ground to think there is legal precedent for HONEST AUDITS and the lack of those laws makes it easy for vigilante justice, the thug wins and the thug will always be a dishonest politician whether republican or in Georgia "Dixiecrat" democrat like Cathy Cox.

I write you as a former citizen of Georgia, Ground Zero for election fraud in the United States. We have had these bastard Diebold Touchscreen and Optiscam machines since 2002 and went from 132 years of Democratic leadership for Governor, for House for Senate and for President to by 2006, a fully republican replacement for all such offices. Georgia was RIGGED in the worst way. This kind of overnight change in voting patterns is not only unlikely, it was facilitated by the famous Rob Georgia patch which I hope you read the Alameda lawsuit brought by Blackbox voting to understand the impact of such a security breach.

I want to update you on several areas that should make my case simply, and legally. Because as a citizen, Madame Secretary, you should know that I OWN THE ELECTIONS, in my former state of Georgia I owned the elections for which I voted and now in my new home of Seattle, I own the elections there. However, Georgia thinks that Diebold and the SOS office owns elections because when I asked by way of Open Records for the ballots in Georgia, they sent me a letter (see below) saying that I was basically a terrorist for asking for such records and that because the ballots are all software now, the state has to protect it's PROPRIETARY Software agreements with Diebold instead of produce software that the citizen can see an possibly use to manipulate elections. HUH? I can't get ballots.

<http://www.countpaperballots.com/cox-terrorist-response.htm>

COMMENTARY:

When a citizen asked for the 2004 Georgia Election data which can only be characterized by getting full access to the Diebold source data files, their response was:

WOULD COMPROMISE SECURITY AGAINST SABOTAGE OR CRIMINAL OR TERRORIST ACTS

this very letter I am told is cause for me to sue the state for 3 times the cost of the machines, adding up to \$150M dollars. Imagine the loss to the state of that kind of suit. Would you want citizens in California to have a similar lawsuit against your state? Don't think we're not ready to take those actions. Because I have lost years of my life fighting this battle and I'm pretty sick of the folks who think we NEED ELECTRONIC MACHINES to run our elections. we don't and we can't.

You stand at the peak of the BIGGEST decision in history. to let the #1 state for electoral votes, make the right decision to go back to paper ballots, which 95% of the other countries use hand counted paper ballots and Ireland walked away

from a \$40M EUro investment in machines to go back to paper ballots, you Ms. Bowen, are sitting in the most powerful position in the free world. to restore democracy to the most influential country in the world. If you could go back in a time machine and show that election fraud is what installed bush in the first place and definitely in the 2nd election and erase all those fraudulent elections and put Gore in office and do the right thing, please consider the billions of dollars back in US treasury, the 3,000 mothers who would have their soldiers back in their arms. The impact of your decision is HUGE and it is NOT TIME FOR COMPROMISE. I am a reasonably hard working person, and I have lost relationships, money and time to this battle and I have one thing to do this Saturday morning is to convince you that getting a 'better machine' is the wrong angle. It's time to start lawsuits against all the vendors for 3 times the money you spent Citing of all things the simplest of documents , the earliest FEC document published April 30th of 2002, saying that the machines must produce ballot images of the voter's intent, none of the machines produce such ballot images and this is what our case hinges on.

If I own the elections as a citizen I also can at any time after the election get copies of all ballots because of the anonymous nature of the ballots that is the only way citizens can count and validate honest elections, that's why citizen counting of ballots election night is so TERRIBLY IMPORTANT. I can compare the hand printed signatures (not electronic but hand signed) signatures of the pollbooks to validate who ACTUALLY SHOWED UP TO VOTE and the ballot total must match the pollbook total and that way you know that every vote counted. The use of machines to handle voter registration and the automated pollbook in Georgia, resulted in 75,000 cards the citizens used to sign in with being left in a dumpster, compromising the social security #, the ID and address of each of those voters. This is not only a lawsuit waiting to happen also in California, it shows that electronic pollbooks are also a HUGE VIOLATION OF THE CITIZEN privacy and no system, if it's electronic can manage to provide honest/anonymous/secure voter registration and pollbook sign-in on election day.

By using any of your existing electronic machine vendors, you are telling me, the citizen, I Can't have the ballot to count because these machines do not have a paper ballot. Even in the case of an optiscan form, which many point to as the ballot, the election code is modified to NOT COUNT THIS AS THE BALLOT OF RECORD. Another problem with the optiscan is they are not put in SECURE BALLOT BOXES, but often travel in rubber banded groups from here to there to there, from precinct, to county office to precinct, in a most insecure and prone to human error way. That is why ballot boxes and I would maintain LOCKED Ballot boxes are not only critical to an honest elections they

are a gaiting factor to an honest election so absentee voting via optiscan is a compromise at best for folks that are not present to vote.

These optiscan ballots get lost and have a seriously broken chain of custody with one and 2 week voting periods meaning that the only other way to vote is to do it on ONE DAY and not spread out over a time period. In WA we have a terrible situation, voting by mail. THis is ridiculous. Voting by mail represents 4 or 5 opportunities to BREAK THE CHAIN OF CUSTODY. This is also a huge problem. The US mail has an average loss rate of

I will also point out the Voter GA lawsuit has won 2 significant counts, corroborated by the Republican Secretary of State, Karen Handel who is doing not only a miraculous job managing to sort out what to do in her state, but struggles with the very same issues you struggle with in as nonpartisan a manner as we have seen. I will remind you it was a democrat Secretary of State Cathy Cox that stole the elections for Georgians and let privatized elections erode any sense of democracy in our state. She is famous for posing for the inside cover of a Diebold folder as seen below demonstrating not only the blatant lack of understanding of the nature of elections, but lack of need for companies, who's motive is merely profit, that these corporations the minute you sign the legal agreement to have that technology, you rob the citizens of honest elections.

**ress Release**

**August 1, 2007**

## **SOS Audit Trail Report Strengthens VoterGa Lawsuit**

ATLANTA, GA Plaintiffs from VoterGA explained today how conclusions in an audit trail report recently released by Sec. of State Karen Handels office corroborate the premises of two legal counts in their pending lawsuit suit against Georgias current method of voting. The report was based on findings made public at audit trail pilot hearings conducted last year by the State Election Board at the request of board member, Randy Evans. The plaintiffs cited two key conclusions:

The sequential printing of the VVPAT paper ballots does not guarantee voter anonymity as required by Georgia law.

The manual audits, while successful in verifying the accuracy of the electronic vote count, proved very costly, time-consuming, and prone to human error.

Voter GA founder Garland Favorito explained: Our lawsuit specifically states that the chosen Diebold pilot technology jeopardizes the ballot secrecy requirement of the Georgia Constitution and makes it impractical to insure the accuracy of each vote cast at the time of use on Election Day. We explained these issues to SB500 conference committee members prior to the audit trail bill being passed. We recommended using any technology that produces separate paper ballots. These would allow a precinct to manually audit a race in about 30 minutes.

Plaintiff Mark Sawyer added: The Elections Division chose the most error-prone, time-consuming tallying approach conceivable. The main advocate of this ill-fated pilot was former Elections Director, Kathy Rogers, who, over our objections at the legislature, insisted on using only Diebold for the pilot. Should we be surprised that she now works for Diebold? Under the circumstances, I think not.

Black Box Voting author, Bev Harris who starred in HBOs Hacking Democracy and founded the Black Box Voting web site, stressed that: This is one of the two most important law suits in America. The plaintiffs must have their day in court.

VoterGA stands for Voters Organized for Trusted Election Results in Georgia. Its lawsuit contends that the Georgias current method of electronic voting is both illegal and unconstitutional under state laws. More information can be found at the organizations web site, [www.voterga.org](http://www.voterga.org).

**Media Contacts:** Garland Favorito

I could continue but Ms. Bowen, I want to make myself available as well as Garland anytime to update you on the lawsuit and that that means to all Diebold users nationwide if the lawsuit proves successful. It will remain a legal justification to support not only decertification, but removing the electronic voting apparatus in any state immediately before any of the next elections. You truly want to watch this suit and not have California try hard to get it right, but then have a legal suit make all your work seem ill advised, and worst case, setting your state up for similar citizen lawsuits. I know the activists in CA, and know that they are capable of enormous progress.

I think you are close to doing the right thing, but going to a wet noodle bad Diebold approach versus a full on removal of vendors known to have problems is critical. Now is a time for action and you have the citizens voice behind your every action.

I can be reached anytime by email or phone 678.314.3227. I can also ask for time on your calendar to outline the 7 counts of our lawsuit and the impact that will have on the nation if the suit is won.

Thanks,  
Phyllis

**From:** Sheila Parks  
**Sent:** Monday, August 06, 2007 8:19 AM  
**To:** Secretary of State Bowen; Goldberg, Evan; Finley, Lowell; Voting Systems; Elections - El Dorado County  
**Subject:** THANK YOU + More  
**Importance:** High

Dear Secretary Bowen, Evan Goldberg, and Lowell Finley,

Thank you for your courageous, heroic and Amazonian stand for democracy in the USA and against so much of the electronic voting machine industry.

You have done brilliant work and I applaud you; however, there remains much to be done.

Op scans have been hacked and will continue to be hacked. You are well aware of this.

Audits need to be random and who will ensure that?

And audits come too late in the process.

The vote needs to be counted right the first time.

Please, consider going to hand-counted paper ballots (HCPB) the only way our voting rights will be fully protected.

\*\*\*\*\* I am including links here to two articles I have had published about HCPB and am also including (below my phone number) a copied and pasted version here for your convenience, of the first link, **which includes a HCPB protocol used in Acton, ME, which I highly recommend to you for use in CA This protocol counted 944 ballots in 4 hours, using six teams of two counters each. THEY COUNTED THE BALLOTS TWO TIMES IN THE FOUR HOURS. There were seven races and two initiatives.**\*\*\*\*\*

[http://www.opednews.com/articles/opedne\\_sheila\\_p\\_070718\\_on\\_site\\_observations.htm](http://www.opednews.com/articles/opedne_sheila_p_070718_on_site_observations.htm)

<http://www.tikkun.org/magazine/specials/article.2006-04-10.1693298872> An updated version can be found at <http://electionfraudnews.com/News/HCPBNow.htm>,

Thanks and for all you do,

Sheila Parks, Ed.D.

July 18, 2007

## **ON-SITE OBSERVATIONS OF THE HAND-COUNTING OF PAPER BALLOTS AND RECOMMENDATIONS FOR THE GENERAL ELECTION OF 2008**

*By Sheila Parks*

### **ON-SITE OBSERVATIONS OF THE HAND-COUNTING OF PAPER BALLOTS AND RECOMMENDATIONS FOR THE GENERAL ELECTION OF 2008**

Copyright © 2007 by Sheila Parks, Ed.D.

#### **INTRODUCTION**

Between May 2, 2006 and November 7, 2006, I observed the hand-counting of paper ballots in three elections in two New England states. The purpose of these observations was to gather first-hand data concerning the feasibility, effectiveness and accuracy of the use of HCPB. These elections were as follows:

- (1) Rockport, Massachusetts (MA), on May 2, 2006, Town Election
- (2) Hudson, MA, on May 8, 2006, Town Election
- (3) Acton, Maine (ME), on November 7, 2006, General Election

All three hand-countings of paper ballots were conducted smoothly and were finished in a timely manner. This paper describes the various protocols used and presents recommendations for the use of hand-counted paper ballots (HCPB) in the upcoming elections of 2008. Absentee ballots, provisional ballots and chain of custody of the ballots are not dealt with in this paper, although they are also crucial elements of an HCPB system.[1]

Much has been written about the fraud and error associated with the use of electronic voting machines - both Direct Recording Electronic (DRE'S/touchscreens) and Optical Scan (op scans/opti scans).[2] Because of this fraud and error, HCPB have been put forth as an alternative to electronic voting machines.[3] The use of an HCPB system will ensure that each vote is counted as intended and as cast by the voter. Although HCPB do not address the egregious suppression of the vote (mostly of people of color, elders and low income people), partnering a solution to the elimination of this suppression with the use of HCPB is the only way to have honest and transparent elections.

The jurisdictions that I observed were not selected randomly. They were places that I could drive to comfortably from my home in Boston, MA. Moreover, I was interested in

observing an election in Acton, ME because the Town Clerk had told me that after the first hand-counting, the ballots would be hand-counted a second time.[4] I received permission to observe the elections from each Secretary of State, or their assistants, and from each Town Clerk. For full transparency, I introduced myself as an advocate of HCPB, who wanted to observe an HCPB election. I was very well received and felt comfortable in all places. All three Town Clerks were very generous with their time and expertise.

In each of the three elections observed, number two pencils were used by the voters to hand mark their paper ballots. In each of the elections, the counters worked in teams of two. In addition, the counters were told that it was the intent of the voter that was to be counted, and when in doubt, the counters called over the Town Clerk or Warden[5] to ask questions about specific ballots and how to count them. Finally, in each of the elections, the counters were able to hand-count the paper ballots in a short time (see specifics below).

### **ACTON, ME, NOVEMBER 7, 2006, GENERAL ELECTION**

I will first describe the HCPB election in Acton, ME on November 7, 2006 because this protocol used a procedure that would produce the most accurate count of the votes - namely, a second hand-count was done immediately after the first hand-count.

The ballot box was a plain, wooden box with a slot into which voters put their ballots. There were six teams, of two counters each, doing the hand-counting. The counters came in specifically to count; they had not worked at the polls earlier in the day. Each team consisted of a Republican and a Democrat. The teams first counted the ballots into batches of 50, and then these batches of 50 were counted again.

The teams then hand-counted the votes cast in each contest for each batch of 50 ballots in the following manner: One member of the team would read out loud the name marked off for each contest; the other member of the team marked the vote on a tally sheet that corresponded to the ballot. A voter's entire ballot was tallied for all of the contests before the counters went on to tally the next voter's ballot. The talliers counted each vote by making a hash mark (small, straight vertical line).[6] After four vertical lines were made, a fifth line was made diagonally through the first four marks. For each person running for office (and for each initiative), the tally sheet was marked off into five columns vertically and two rows horizontally, providing 10 rectangular spaces in each of which five hash marks could be written - a total of 50 hash marks - i.e., votes - per contest or initiative. A dark horizontal line separated the names in each contest. At the end of the counting of all of the races in a batch of 50 ballots, the counters totaled the hash marks for each race on the tally sheet and entered that number on the tally sheet in the "TOTAL VOTE" column. There was a special sheet for write-ins.

Immediately after the first hand-count of a batch of 50 ballots, a second hand-count, on a

new tally sheet, was done of this same batch of 50 ballots by these same counters. Again, the entire ballot of each voter was tallied before the counters proceeded to the next voter's ballot. This time, the person who had read the names out loud marked each vote on the tally sheet, and the person who had tallied read out loud the ballot choices. After the votes on all 50 ballots in a batch were marked on the tally sheet, the totals for each contest were obtained and written on the tally sheet. If the totals for the candidates in any contest or for any initiative were not exactly the same on the first and second tally sheets (i.e. on the first and second countings), these contests or initiatives were counted a third time. I observed such a situation two times.

The HCPB election in Acton, ME demonstrates that paper ballots can be hand-counted immediately a second time, at the precinct on election night, before the results are posted at the precinct, in order to ensure an honest and transparent count in a timely manner. The election in Acton, ME also indicates that paper ballots can be hand-counted in a very short time. With seven races and two initiatives, the six teams of two people each were able to hand-count twice 944 ballots in four hours.

### **ROCKPORT, MA, MAY 2, 2006, TOWN ELECTION HUDSON, MA, May 8, 2006, TOWN ELECTION**

The elections in Rockport and Hudson will be discussed together because they were similar in various respects. Both counted the votes cast only once,[7] and both used the same kind of tally sheets provided by the MA Secretary of State. In both jurisdictions the ballots were counted into batches of 50. The tally sheet was a large piece of paper that was marked off into a grid with horizontal and vertical lines forming small rectangular boxes (similar to the squares of graph paper). The vertical columns were marked with a heavy line at each multiple of five columns. There were 50 rectangular boxes across each horizontal line. At the top of the tally sheet, each vertical column was numbered from 1-50. On both the left hand and right hand sides of the tally sheet were the names of the people running in that particular race. One tally, as a hash mark, was put into one box, beside the name of the person voted for. A voter's entire ballot was tallied for all of the contests before the counters went on to tally the next voter's ballot. After the 50 ballots were tallied, the totals for each contest were entered into the "Totals" column at the end of the 50th box. Blanks and write-ins were also marked on this sheet. Four or five teams of two poll workers did the hand-count. One read from the ballot, and the other person placed the hash mark in the appropriate box on the tally sheet.

Rockport, MA used an old wooden ballot box.[8] A poll worker turned the brass handle on the box as each voter put her/his ballot into the box. Numbers on the front of the box automatically changed as ballots were placed in it, counting the cumulative number of ballots placed in the box. The machine marked each ballot with the precinct number down the center of the ballot as it went through the machine. The preceding characteristics of the ballot box provided a measure of security for the ballots, minimizing the danger of stuffing the ballot box, a criticism often leveled at the HCPB process. As noted earlier, this paper does not examine in detail issues of security such as

chain of custody, but rather deals with protocols for HCPB.

There were two crews of poll workers, morning and afternoon. One crew came in at 6:30AM and worked until 12:30PM. The second crew came in at 12:30PM and worked until 6:30PM. At 6:30PM, the second crew went home for dinner until 8PM, when they came back to hand-count the paper ballots. The morning shift came back at 6:30PM to work at the polls and then to hand-count the paper ballots. The polls closed at 8PM. The paper ballots were hand-counted by five teams of two workers each.

In Hudson, the ballot box was an old box made of gray wood. The ballot box rang when the voter put in her/his ballot, and the poll worker turned the crank of the box, moving the ballot from the slot of the box into the box. When the poll worker cranked the ballot into the ballot box, each ballot was inked with "Town of Hudson, precinct 6." [9] This ballot box also provided a degree of security for the ballots.

The Clerk could hire eight people per precinct, not including the Warden and Clerk, who were also present for the hand-counting. There were two shifts of poll workers, 7AM-5PM and 5PM-8PM, which was when the polls closed. The second shift did the counting. Poll workers had to be registered voters in the town of Hudson. Although it was preferred that the counters lived in the precinct where they worked, it was not necessary.

The elections in Rockport and Hudson again demonstrate that paper ballots can be hand-counted in a reasonable time. In Rockport, it took about one hour to hand-count 522 ballots; there were six races and no initiatives. In Hudson it took about one hour to hand-count 59 ballots; there were 14 races and no initiatives. As noted, both communities used ballot boxes that provided a degree of security for the ballots.

## **RECOMMENDATIONS TO BEGIN WITH THE 2008 GENERAL ELECTION (WHICH INCLUDES THE PRESIDENTIAL ELECTION)**

### **Recommendations Based on My Observations**

(1) Based on my observations in Acton, ME, this paper recommends the hand-counting of paper ballots followed immediately by a complete second hand-counting and a reconciliation of the two counts, if necessary, by additional counting. [10] A second hand-counting is crucial to check the accuracy of the first hand-count. If a discrepancy is found between the two countings, counting should continue until the counts are reconciled. This paper also recommends the procedure used in Acton of counting the ballots into batches of 50, counting a batch of 50 and then immediately counting that batch of 50 again. Some critics of electronic voting machines have pointed out the need to obtain a second count, called an audit, after the first original tabulation of votes;

however, there is no consensus as to how such an audit should or could be done. The second counting of ballots recommended in this paper goes beyond the concept of an audit to a comprehensive process encompassing a second counting of every vote and a reconciliation of the two counts.

(2) From my observations of these three hand countings, I prefer the tally sheets used in Acton, ME over the graph-like grid used in both Rockport, MA and Hudson, MA. During my observations, it appeared that the Acton tally sheet was easier for the counters to use. With the grid-like tally sheets, care had to be taken by the counters not to lose their place.

(3) Because HCPB require careful attention to and scrutiny of the ballots, it is recommended that people who have not worked at the polls all day come in to do the counting, as in Acton, ME.

(4) As noted, this paper does not deal in detail with the issue of security of the ballots. However, it is recommended that research be done concerning the cost of manufacturing ballot boxes with the characteristics described for Hudson, MA and Rockport, MA.

-

### **Additional Recommendations**

The present author has been involved with voting rights for the last five years. Based on her previous work,[11] she also further expands the use of HCPB to include the following recommendations:

(1) In addition to the four recommendations presented above, it is recommended that an HCPB protocol also have the following characteristics: (a) Ballots would be counted at the precinct by registered voters in that precinct. (b) The counting would be done in full view of the public. (c) The counting would be videotaped. (d) The results would be posted at the precinct immediately after the count. (e) To be manageable, precincts would be no larger than 1000 registered voters. (Because the concept of HCPB operates at the precinct level, even large communities can adopt such a system.) (f) In each precinct there would be at least 10 teams of two counters each (a Democrat and a Republican).[12] These teams would count the ballots, one counter reading the name and the other counter making the mark on the tally sheet. For the second counting, the counters on each team would switch roles. (g) Whether or not there would be observers as part of the team of counters, and if so, how many, needs more research and is beyond the scope of this paper.

(2) This paper recommends that poll workers who participate in the process of HCPB be

paid at a rate that will be respected by the community. This will be possible because a large amount of money will be saved with the elimination of electronic voting machines. The Help America Vote Act (HAVA) paid states hundreds of millions of dollars to buy electronic voting machines, both DRE'S and/or op scans.[13] One machine can cost anywhere from \$3,000 - \$5,000[14] and that amount does not include storing, maintenance, and upgrade. In contrast, for an HCPB election, the cost for the counting could be \$2400.00 per precinct for each election, with ten teams of two workers each, as described above, and paying each worker \$20/hour for six hours (\$120). HCPB by registered voters from the precinct would also keep the money in the community. As is true for op scan electronic voting machines, money would also have to be spent for the cost of printing the ballots.[15] If hundreds of millions of dollars had not been spent for the purchase, storage and upgrade of electronic voting machines, imagine the money our communities could have used for health care and education.

## **EPILOGUE**

On January 4, 2006, I had the good fortune to watch on TV the voting in Congress for Speaker of the House. One at a time, each representative called out orally her/his choice for Speaker, and that vote was tallied by hand. This hand counting of oral votes was done by two Republicans and two Democrats, all of whom had been appointed by the Clerk of the House. The Electronic Board that usually counts the votes of the Representatives was not used for this count; the official vote was tallied by hand. I could not help but wonder how the Representatives would have felt had their votes not been recorded accurately, or not at all, as voters throughout the USA experienced in recent elections. For voters in each precinct in the USA, hand-counting of paper ballots would assure that each of our votes is counted as intended and as cast, as the oral votes of our Representatives, were hand-counted, as intended and as cast, in the House of Representatives.

## **ENDNOTES**

[1] For a beginning discussion of chain of custody, see the present author's paper *Hand-Counted Paper Ballots Now*. A version of this article first appeared in the April 2006 issue of *Tikkun*, <http://www.tikkun.org/magazine/specials/article.2006-04-10.1693298872>, retrieved from the Web February 28, 2007. An updated version can be found at <http://electionfraudnews.com/News/HCPBNow.htm>, retrieved from the Web February 28, 2007. "Ballot boxes must be clearly marked and visible in plain view. Ballot boxes will be sealed and locked whenever they contain ballots and are not being actively used. Ballot boxes are secured from the beginning of voting until the end of counting by a chain of custody procedure. Ballot boxes never leave the polling place until after the vote is counted, audited and certified. Each time ballot boxes move from the physical control of or visual contact from one person to another, a duplicate record signed by all counters and observers must be made relinquishing and gaining control. There will be a documentation process wherein each ballot box will have a record of its handling from the beginning of the day to the end of counting. On the web site of computer science expert Professor Douglas W. Jones, there is a very clear and detailed protocol for "Ballot and Ballot Box Transportation" and "Ballot Storage." The reader is referred specifically to these two sections (the last two on this link): <http://www.cs.uiowa.edu/~jones/voting/paper.html>

[2] Listed here are some of the outstanding articles about the fraud and error resulting from electronic voting machines; some are from the mainstream media, others from scholarly sources, and yet others from technical groups: (1) The public hacking of electronic voting machines by Harri Hursti, working with Black Box Voting, <http://www.bbvforums.org/forums/messages/2197/6847.html>, retrieved from the Web February 21, 2007. (2) The U.S. Government Accountability Office (GAO) in its nonpartisan September 2005 report on elections states in its conclusions: "Numerous recent studies and reports have highlighted problems with the security and reliability of electronic voting systems ... the concerns they raise have the potential to affect election outcomes ... Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, But Key Activities Need to be Completed.", <http://www.gao.gov/new.items/d05956.pdf>, retrieved from the Web March 7, 2007. (3) Article by Robert F. Kennedy, Jr. in Rolling Stone (Issue 1002, June 15, 2006), [http://www.rollingstone.com/politics/story/11717105/robert\\_f\\_kennedy\\_jr\\_will\\_the\\_next\\_election\\_be\\_hacked/print](http://www.rollingstone.com/politics/story/11717105/robert_f_kennedy_jr_will_the_next_election_be_hacked/print), retrieved from the Web February 21, 2007. (4) Report of the Brennan Center Task Force of NYU, on June 27, 2006, [http://www.brennancenter.org/press\\_detail.asp?key=100&subkey=36345](http://www.brennancenter.org/press_detail.asp?key=100&subkey=36345), retrieved from the Web February 21, 2007 and [http://brennancenter.org/dynamic/subpages/download\\_file\\_38150.pdf](http://brennancenter.org/dynamic/subpages/download_file_38150.pdf), retrieved from the Web February 22, 2007. (5) Papers by Ed Felton et al. from Princeton University in Sept. 2006, <http://dubiousprofundity.com/hackthevote.pdf>, retrieved from the Web February 21, 2007. (6) Problems that occurred with electronic voting machines in many states in the General Election on November 7, 2006, especially the 18,000 undervotes in Sarasota County, FL, [http://www.nytimes.com/cq/2006/12/20/cq\\_2056.html](http://www.nytimes.com/cq/2006/12/20/cq_2056.html), retrieved from the Web February 20, 2007. (7) NIST discussion draft, December 1, 2006, <http://vote.nist.gov/DraftWhitePaperOnSIIinVMSG2007-20061120.pdf>, retrieved from the Web February 22, 2007. (8) The annotated bibliography by Rady Ananda, <http://tinyurl.com/2gwlv>, retrieved from the Web May 11, 2007.

[3] On August 4, 2006, Nancy Tobi posted this article about HCPB in NH, [http://www.opednews.com/articles/genera\\_nancy\\_to\\_060804\\_the\\_granite\\_state\\_de.htm](http://www.opednews.com/articles/genera_nancy_to_060804_the_granite_state_de.htm), retrieved from the Web March 12, 2007. An editorial first carried in the Ketchikan Daily News, December 1, 2006, written by Editor Terry Miller, called for HCPB for the president and vice president, <http://www.ketchikandailynews.com/>, retrieved from the Web January 12, 2007. (Thanks to John Gideon of Daily Voting News for pointing out the Ketchikan editorial.) On December 7, 2006, the editorial was then picked up by the Juneau Empire, [http://juneauempire.com/smart\\_search/](http://juneauempire.com/smart_search/), retrieved from the Web January 12, 2007. Rady Ananda wrote an HCPB Implementation Strategy for 2007 on January 3, 2007, [http://www.opednews.com/articles/opedne\\_rady\\_ana\\_070102\\_evoting\\_exit\\_strateg.htm](http://www.opednews.com/articles/opedne_rady_ana_070102_evoting_exit_strateg.htm), retrieved from the Web March 13, 2005. In February 2007, in Missouri (MO), Show Me The Vote, led by Phil Lindsey, introduced an initiative to go on the ballot that, if passed, would mean that MO would not use electronic voting machines in their elections, but would use HCPB. This initiative must first get enough votes from the public to appear on the ballot, <http://www.scoop.co.nz/stories/HL0702/S00271.htm>, by Michael Collins, retrieved from the Web March 12, 2007. (To contact Show Me The Vote, email Phil at [galloglas@sbcglobal.net](mailto:galloglas@sbcglobal.net).) Another HCPB initiative, led by Kathleen Wynne, is in the form of a petition from the American People to Congress, urging Congress to reintroduce the Paper Ballot Bill of 2006, <http://hcpbnow.org/petition.html>, retrieved from the Web July 13, 2007. In June 2007, at The DFA (Democracy for America) Democracy Fest in New Hampshire, in a telephone call to the attendees, Representative Dennis Kucinich stated that he will introduce The Paper Ballot Bill of 2007, mandating HCPB for all federal offices. Kucinich has changed the bill from his 2006 version, H.R. 6200, which had mandated HCPB for the offices of president and vice-president only, [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109\\_cong\\_bills&docid=f:h6200ih.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6200ih.txt.pdf), retrieved from the Web, March 30, 2007.

[4] I observed one of the three HCPB methods authorized by the Maine Secretary of State, called "The Reading Method": "The team counts each lot together; 1 member reads and the other member tallies. The team members then switch roles, so that the tally is done a second time. If they agree, that count is completed. If there is a discrepancy, the team must recount the race or races where the count was off. ...." From Maine Revised Statutes Annotated (MRSA), CONDUCT OF ELECTIONS, Chapter 9, page 3, (Title 21-A §695).

[5] "Warden" is the name used in Massachusetts for the poll worker in charge of the election in that

precinct. Different names are used in different states. The person is not an elected official

[6] In April 2004, Teresa Hommel described some hand-counting methods used in Canada and New York City, <http://wheresthepaper.org/CountPaperBallots.htm> , retrieved from the Web January 13, 2007.

[7] Another method of hand-counting paper ballots is the sort and stack protocol, <http://www.sos.nh.gov/FINAL%20EPM%208-30-2006.pdf> (pp 144-146), retrieved from the Web May 11, 2007. In this method, used by the state of New Hampshire, the ballots are first sorted into stacks for each candidate, and then the stacks are counted. In email correspondence, December 2, 2006 and December 4, 2006, with Nancy Tobi from Democracy for New Hampshire, Tobi states that NH uses the sort and stack method for both election night counts and for recounts. She says that it is used primarily for "... single member races - where there is a yes/no choice..." and for straight ticket votes. Sort and stack is not usable in all situations. With this protocol, as with those used in Rockport and Hudson, votes are counted only once; the manual recommends a second count if there is a "close race." A "close race" is not defined. A mandatory second count for all ballots could be added to this protocol.

[8] The ballot box said "Town of Rockport, Precinct 2" and was dated 1922.

[9] The ballot box was made by S. Ralph Cross and Sons, Inc., 120 Mayfield Street, Worcester 2, MA, now out of business. The box was dated 1971.

[10] Joanne Karasak has recommended a first count followed by "an immediate second 'blind' count (blind count meaning that the second team of counters do not know the total on the first count)." Email posted June 26, 2007. Based on my observations in Maine, I think it would be too confusing to change counters.

[11] See Sheila Parks, *What Went Wrong in Ohio & Black Box Voting*, <http://www.tikkun.org/magazine/reviews/article.2006-01-06.7975946864>, retrieved from the Web March 18, 2007; Sheila Parks, *Hand-Counted Paper Ballots Now* (see endnote 1); Roy Lipscomb and Sheila Parks, *Hand-Counted Paper Ballots: Frequently Asked Questions*, <http://www.scoop.co.nz/stories/HL0705/S00261.htm> , retrieved from the Web May 20, 2007.

[12] If there additional parties on the ballot, representatives from these parties should also participate in the counting.

[13] Thanks to my good friend Lucius Chiaraviglio, HCPB activist, for his help with this endnote, [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_public\\_laws&docid=f:publ252.107](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ252.107) , retrieved from the Web March 13, 2007.

[14] Thanks to Paul Letho for sending me this information. See Appendix A, <http://www.votersunite.org/info/SequoiaContract.pdf>, retrieved from the Web March 18, 2007, for the contract between Snohomish County, Washington and Sequoia Voting Systems, Inc. for a detailed example of what electronic voting machines cost. This contract was for more than \$5 million dollars. Appendix A is contained in his lawsuit against Sequoia Voting Systems, Inc., [www.votersunite.org/info/lehtolawsuit.asp](http://www.votersunite.org/info/lehtolawsuit.asp) , retrieved from the Web March 18, 2007.

[15] Email correspondence, March 6, 2007, with Chief Legal Counsel, Election Division, Office of the Secretary of State, MA. In MA in 2006 there were 71 precincts using HCPB. For the MA State Primary election in 2006, the cost was \$444 per precinct (which included two parties) for ballot printing, which included absentee ballots, specimen ballots and instruction cards. For the General Election in 2006, the cost was \$391 per precinct.

Authors Bio: Sheila Parks, Ed.D., is an Organizing Consultant who lives in Boston, MA. She is a long time feminist and peace & justice activist/organizer on many issues and has been involved in the current wave of voting rights for five years.

**From:** Jeff Goodwin  
**Sent:** Saturday, August 04, 2007 11:38 PM  
**To:** Voting Systems  
**Subject:** THANK YOU

Secretary Bowen: YOU ROCK !!!!

STICK TO IT...YOU DID THE RIGHT THING AND IT'S THE VOTERS OF CALIFORNIA WHO ARE BEHIND YOU 1000%.

Any election official who gives you a hard time IS OUT OF LINE. At best, their role in this context is to dispassionately advise, if credible, rather than advocate, which is not their job, role, or domain.

MORE FUEL:

On Aug. 1, the Brennan Center at New York University Law School released a report with more than 60 examples of electronic voting machine failures in 26 states in 2004 and 2006. The California examples included Spanish-language ballots that were cast by voters but not counted in Sacramento in 2004, and votes for presidential and U.S. Senate candidates that were assigned to another candidate in San Diego in 2004.

Perhaps the most striking recent example was not cited in the Brennan Center report. In a 2006 judicial race in Columbus, Ohio, the defeated incumbent, Carol Squire, challenged the results in court. Magistrate Joel Sacco issued a ruling this July finding that 721 out of Franklin County's 835 precincts had vote totals that did not match the number of people who signed in to vote. In all, 86

percent of the precincts had inaccurate counts. Expert witnesses also cited the breakdown of the paper trail audit systems, which prevented an accurate recount.

"Evidence has come forward in a variety of courtrooms that shows this technology is deeply flawed and there already have been a series of problems," said John Bonifaz, legal director for VoterAction, a public interest law firm involved in voting machine litigation in a half-dozen states. "For them to deny that this doesn't happen in the real world is contrary to the facts in the real world."

**From:** Connie Pracht  
**Sent:** Saturday, August 04, 2007 7:24 PM  
**To:** Voting Systems  
**Subject:** [Fwd: VOTING decision will be made today]

**Dear Ms Bowen,  
Secretary of State, California**

**Thank you! Thank you!Thank you!Thank you!Thank you!Thank you!Thank you!  
Thank you!Thank you!Thank you!Thank you!Thank you!Thank you!Thank you!  
Thank you!!!!!!!**

**Your decision on our voting system is wonderful, thoughtful, --and an example for Secretaries of State across the nation--it is my prayer that they**

**show the same vision, respect for the public trust and courage that you have demonstrated for them.**

**Thank you,  
Constance Pracht**

**From:** Karen Bowling  
**Sent:** Saturday, August 04, 2007 2:51 PM  
**To:** Voting Systems  
**Subject:** Thank goodness!

I have followed this fiasco diligently since 2000 and am so elated at Bowen's gumption and brains to take on the powers-that-be regarding the safety of our elections. Why is it that everytime there was a snafu in machines across the country, it always benefitted a Republican? Any idiot could have seen that it wasn't an accident that everytime votes disappeared, exit polls reversed the votes counted, etc. it was always Democrats on the short end of the stick. The Republicans added election machine fraud, thanks to Bob Ney and his crony of Diebold Republican crooks, to their other arsenal of tricks to steal elections. Hopefully, we can fix the actual voting process by paper ballots and allowing regular, election workers to hand-count votes, and then we must attack election fraud itself. The suppressing of minority votes with various ID requirements, caging voters by sending phony letters to new voters, robo-phone calls, misinforming voters of when/where to vote, challenging voters by intimidating them with being arrested, etc. etc. has to stop and all Americans need to not only have the right to vote, but should be encouraged to participate in our democracy. Do we have U.S. Attorneys here in California that will uphold the voting rights and laws of all our citizens. The woman who replaced Lam here in San Diego is a member of the Federalist Society and may be one of those who is only trying to gain favor with Bush and Rove regarding the right to vote. Debra, you have done a wonderful thing for California and I'm so happy to have supported and worked for your election. You have really done something very spectacular not only for California, but also for the United States. Congratulations for all your hard work.

Karen Bowling

**From:** Linda Sutton  
**Sent:** Thursday, August 09, 2007 11:36 AM  
**To:** Voting Systems  
**Subject:** Re: Thank you for your email message.

You have our FULL and CONTINUED support. Go for PAPER. We don't have to know the outcome of an election immediately and would MUCH prefer it be CORRECT than quick.

From: jocari@cox.net  
Sent: Thursday, August 09, 2007 8:49 AM  
To: Voting Systems  
Subject: Thank you, Debra Bowen

Thank you for your "Red Team" review. Your efforts are truly appreciated.

Carl E. Williams

From: jkgillies  
Sent: Wednesday, August 08, 2007 8:42 PM  
To: Voting Systems  
Subject: Thank you

Dear Secretary Bowen:

Thank you for courage in protecting our right to secure elections. I can't tell you what a relief it is to have an elected official who is dedicated to doing what is right. Please, stay strong until you get California as secure a voting system as possible. If there is anything I, as a citizen, can do to help, please let me know. You have my vote for any office you pursue from here on out.

Thank you again

John Gillies

**From:** dolsandiego  
**Sent:** Wednesday, August 08, 2007 5:37 PM  
**To:** Voting Systems  
**Subject:** voting machines

Thank you! Continue to be courageous in the face of opposition.

Blessings,  
Dolores Smith

**From:** Marion Pack  
**Sent:** Wednesday, August 08, 2007 4:37 PM  
**To:** Voting Systems  
**Subject:** Thank you!

Dear Secretary of State Bowen,

Thank you so very much for following through with your campaign pledge to investigate and take action to protect our vote. Your stalwart commitment in spite of political and corporate pressure is laudable!!

Thank you again.

Most Sincerely,

Marion Pack

**From:** Armida Brashears  
**Sent:** Wednesday, August 08, 2007 2:56 PM  
**To:** Voting Systems  
**Subject:** voting machines

Thank you for taking such a bold stance and insisting on accuracy and privacy in the performance of the voting machines.

Voting is very important to our democracy.

Sincerely,     Armida Brashears  
                  72 year old Great Grandmother

**From:** Pat Sica  
**Sent:** Wednesday, August 08, 2007 1:33 PM  
**To:** Voting Systems  
**Subject:** voting machines

Debra Bowen,  
Thank you so much for your courage and high standards.  
Pat Sica

From: joan bleu  
Sent: Wednesday, August 08, 2007 12:54 PM  
To: Voting Systems  
Cc: joanwisebleu@yahoo.com  
Subject: Voting machines

Dear Deborah, Thank you so much for your courageous action in changing the voting machines so we can have clean elections. Joan Bleu

**From:** mgerbm  
**Sent:** Wednesday, August 08, 2007 11:13 AM  
**To:** Voting Systems  
**Subject:** Thanks!

As a California voter, I thank you for your recent decision to de-certify questionable touch screen voting machines. Your efforts to insure the integrity of the vote is greatly appreciated.

Thank you.

Sincerely,

Marlene Gerber

From: Richard Ascher  
Sent: Wednesday, August 08, 2007 10:50 AM  
To: Voting Systems  
Subject: voting systems

Thank you for your couragous stand on voting machines. For once all of our efforts to expose the faults in the voting machines have finally paid off. I am glad I had worked for your election, you make us all proud to be Democrats again.

From: Elaine & Howard Maltz  
Sent: Wednesday, August 08, 2007 10:12 AM  
To: Voting Systems  
Subject: Thanks

Dear Ms. Bowen,  
We wish to thank you for your courageous and correct decision with regard to the electronic voting machines.  
Sincerely,  
Dr. & Mrs. Howard Maltz

**From:** Kimberly Salter  
**Sent:** Wednesday, August 08, 2007 9:48 AM  
**To:** Voting Systems  
**Subject:** Your job

Thank you so much Secretary of State Deborah Bowen - You are the best! Your decision to do the right thing is a bold move at a time when too many 'deals' are made behind the scenes. The voters in California trust you to ensure our system is safe and accurate and you are doing just that.

Thank you.  
In peace  
Dr. Kimberly Salter  
Chair  
California Women's Equality Day Parade & Rally

From: Wjgoeken@cs.com  
Sent: Wednesday, August 08, 2007 8:45 AM  
To: Voting Systems  
Subject: Thanks

Happy that you gave your approval to the paper ballot for Ca. voters. I work at polls and I'm encouraging voters to vote absentee. Wanda Goeken

From: Martha Weesner  
Sent: Wednesday, August 08, 2007 8:18 AM  
To: Voting Systems  
Subject: Voting machines

Dear Ms Bowen -

Truly: thank you very, very, very much!

Sincerely,  
Martha Weesner

**From:** patricia law  
**Sent:** Wednesday, August 08, 2007 7:02 AM  
**To:** Voting Systems  
**Subject:** voting

thank you for protecting our rights to a fair and free elections. please continue to work for even more protections.... patricia law

**From:** Kathleen Blavatt  
**Sent:** Wednesday, August 08, 2007 4:33 AM  
**To:** Voting Systems  
**Subject:** Thank you very much

Debra Bowen,

Thank you very much for helping clean up our voting system.  
In San Diego we need all the help we can get.

Keep up the good work. It is appreciated.

Sincerely,  
Kathleen Blavatt

**From:** Simon Mayeski  
**Sent:** Tuesday, August 07, 2007 9:52 PM  
**To:** Voting Systems  
**Subject:** Thank you for your stand for election integrity!

To Secretary Bowen:

It is much appreciated; you did the right thing, as usual. Thanks for being our Secretary of State! I am speaking as an interested Californian and a computer professional.

- **Simon Mayeski**

**From:** Cessresnic  
**Sent:** Tuesday, August 07, 2007 9:04 PM  
**To:** Voting Systems  
**Subject:** To Debra Bowen

Thank you for your courageous stand to protect the accuracy of our elections.

Yours truly,  
Cecily A. Resnick, PhD

From: MPENNY  
Sent: Tuesday, August 07, 2007 8:15 PM  
To: Voting Systems  
Subject: your investigation of our voting machines

Dear Secretary Bowen,  
Thank you for all your efforts to keep our elections clean and accountable. The San Diego Registrar of Voters has very slipshod methods in his office. Your work to show what can be done to rig votes with our current machines makes it hard for him to claim that we are a bunch of hysterical residents complaining where there is no cause for complaint.

Maria B Penny

**From:** Barb Parcels  
**Sent:** Tuesday, August 07, 2007 9:08 PM  
**To:** Voting Systems  
**Subject:** Thank You!

Dear Secretary of State Bowen:

Thank you for your decision to hold our voting systems to a tight standard, and to decertify those which don't meet it. As a programmer myself, I am well aware, for example, of how easy it is to write code that displays one thing to the viewer and writes different information to memory.

The "bubble" paper ballots used with optical scanners in San Diego County were, in my experience as a poll worker, simple and easy to use, both for the poll workers and for the voters. This might be a good system for other counties to use.

San Diego County is also planning to encourage as many of our voters to vote by mail as possible. It might be useful in the future for the state of California to go to a system much like Oregon's, in which all elections are by mail, use paper ballots, and give the voters a month to fill out and return their ballots.

Sincerely Yours,

Barbara Parcels

**From:** John DeLand  
**Sent:** Tuesday, August 07, 2007 7:36 PM  
**To:** Voting Systems  
**Subject:** Thank you

Thank you for doing the right thing (decertifying electronic voting machines) in the face of incredible pressure!  
I am an automation engineer, and I know how non-robust computer control can be. That is why industrial control is seldom left to computers.

John DeLand

**From:** news  
**Sent:** Tuesday, August 07, 2007 6:07 PM  
**To:** Voting Systems  
**Subject:** Thank you!

Dear Secretary of State Bowen,

We are proud of your recent decision to return San Diego County and other election locations in the State to paper ballots! Thank goodness that someone finally is on the side of our Constitution and the voters to protect our votes. The simplicity of hacking into voting machines, and the willingness of so many in our government and offices of the registrars to let this happen, was appalling.

We applaud you for your courage and want you to know that there are millions of Californians who support you.

Best regards,

Diane and George Ohanian  
Permanent Absentee Ballot voters

**From:** Roland Bleu  
**Sent:** Tuesday, August 07, 2007 5:00 PM  
**To:** Voting Systems  
**Subject:** Thanks to you

Deborah , I`m deeply indebted to you and grateful for your courageous and decisive action re: the voting machines` decision you made last Friday. I went to a Bowen house party in Oceanside in your last campaign,donated, picked up 10 of your bumper stickers,handed them out,and requested 10 more from your office and handed them out also. I could not have campaigned for a person of greater integrity and savy on the integrity of voting procedures and the validity and verifiability of the

machines so used or abused in such. Thanks again,  
Roland Bleu

**From:** Eleanor Egan  
**Sent:** Tuesday, August 07, 2007 4:45 PM  
**To:** Voting Systems  
**Subject:** Thank you!

Thank you for protecting the integrity of elections in California. The decertification of hackable machines took courage, and the recertification with security conditions was wise. I wish we had more public officials like you

From: vmooberry  
Sent: Tuesday, August 07, 2007 4:01 PM  
To: Voting Systems  
Subject: Thank you!

Debra Bowen, my gratitude and respect for your actions will remain long after this has gone away. Thank you so much for persevering to see the voting methods of California corrected. You, an elected official, did what you said you would do when you were running for office! We thank you!

Vi Mooberry

From: Sarah Lifton  
Sent: Tuesday, August 07, 2007 3:16 PM  
To: Voting Systems  
Subject: THANK YOU!!

Secretary of State Bowen--

I can't tell you how pleased and relieved I am that you did the right thing--if not the popular thing--and decertified the various voting machines. Your job is not to make life easy for the registrars of voters, many of whom enjoyed significant "gifts" and perks from the manufacturers, but to ensure the integrity of our democratic system. I contributed to your campaign precisely because of this issue, and I'm so glad I did. Stand firm!!!!

Sincerely,  
Sarah Lifton

**From:** dennywelch  
**Sent:** Tuesday, August 07, 2007 2:45 PM  
**To:** Voting Systems  
**Subject:** Voting Machines

Thanks for taking action on this very important issue! Hackers could run our government if you hadn't step in!

Denise D Welch

**From:** Ekwhin  
**Sent:** Tuesday, August 07, 2007 2:21 PM  
**To:** Voting Systems  
**Subject:** Thank You

Thank you for helping to insure that the integrity of our voting system remains intact and credible. You have done what most others would not do. Please continue to stand up for the people.

Sincerely,  
Eric Whinston

**From:** Joan and David Little  
**Sent:** Tuesday, August 07, 2007 2:21 PM  
**To:** Voting Systems  
**Subject:** RE: Thank You!!!

Dear Secretary Bowen:

Thank you so much for your recent actions on electronic voting systems. You are exhibiting the kind of leadership that is needed to restore our democracy!!!! A million thank yous!!!!

Joan Little

**From:** Irene Dunny  
**Sent:** Tuesday, August 07, 2007 2:15 PM  
**To:** Voting Systems  
**Subject:** THANKS

Dear Debra,

Thanks you so much for decertifying the voting machines that have been undermining our elections. I support you completely in making it possible to have fair elections.

Irene Dunny

**From:** Ronnie Friedman-Barone  
**Sent:** Tuesday, August 07, 2007 2:07 PM

**To:** Voting Systems  
**Subject:** thank you!

Debra,  
Heartfelt thanks from our family for helping to make our votes count. It is very good news amid all the other awful news.

We are very pleased we voted for you.

Sincerely,  
Ronnie Friedman-Barone & Joseph Barone

**From:** Joanne Goodwin  
**Sent:** Tuesday, August 07, 2007 12:51 PM  
**To:** Voting Systems  
**Cc:** Goldberg, Evan  
**Subject:** What a blogger wrote about our Secretary of State

**I thought you might enjoy this from a blogger in salon.com:**

At this point in time, I would have absolutely no problem voting for Debra Bowen for Goddess Of All The Earth. She is one fine public servant, in a time when...well, you know the rest.

**Joanne Goodwin**

**From:** Marilyn Cummings  
**Sent:** Tuesday, August 07, 2007 11:06 AM  
**To:** Voting Systems  
**Subject:** Re: Thank you for your email message.

Please thank Debra Bowen for decertifying the machines and taking a step toward restoring the democracy of the United States of America per the Constitution and Bill of Rights which are under attack!  
Marilyn Cummings  
Patriot

**From:** Cathy Cook  
**Sent:** Tuesday, August 07, 2007 11:03 AM  
**To:** Voting Systems  
**Subject:** Thank you

Debra – I have read that you are a thorough and detailed person who really gave a lot of time and energy to this decision. Thank you for being courageous.  
Cathy

**Cathy M. Cook**  
**PWC & Associates**  
**Financial Executive Search**

From: Cindy Marzolf  
Sent: Tuesday, August 07, 2007 10:52 AM  
To: Voting Systems  
Subject: Thank you to Debra Bowen

Dear Secretary Bowen,  
Thank you very much for your decision to eliminate electronic voting in California on Sequoia and Diebold machines. Those of us who support fair and honest elections know paper ballots are the way to go at this point. Many citizens have grave concerns over e-voting machines, specifically those made by Diebold, and as a former software developer myself, I know how easy it is to program software to do whatever you want.

Thank you again for your decision to have fair and honest elections in California via paper ballot, and for your support of voters' rights.

Sincerely,  
Cindy Marzolf

From: Frances Costikyan  
Sent: Tuesday, August 07, 2007 9:35 AM  
To: Voting Systems  
Subject: thank you! thank you! thank you!

Dear Secretary Bowen; I am so proud you are my Secretary of State!  
thank you  
for your stand on the voting machine fracas, and don't give up. the  
entire  
country depends on your courage and we Californians stand behind you.  
frances costikyan

**From:** Diana D. Light  
**Sent:** Tuesday, August 07, 2007 9:02 AM  
**To:** Voting Systems  
**Subject:** Thank you Secretary on State Bowen

**Thank you to Secretary on State Bowen! I support you under tremendous political pressure from the machine corporations and the Republican Party operatives to reverse or water down this decision. Let's hope California will lead the way for national election reform.**

**Thank you for your courageous decision to decertify the Diebold and Sequoia machines.**

**Doing the "right thing" is not easy and you are doing it! I support you!**

**Diana Divine Light  
4th Generation CA Citizen**

**From:** Norrie Robbins  
**Sent:** Tuesday, August 07, 2007 7:46 AM  
**To:** Voting Systems  
**Subject:** Thank you thank you thank you Debra Bowen

Debra Bowen--you are a true Hero of Democracy.

Eleanora (Norrie) Robbins

**From:** Katrina Anne Foley, Attorney at Law  
**Sent:** Tuesday, August 07, 2007 7:34 AM  
**To:** Voting Systems  
**Cc:** womenforoc@aol.com  
**Subject:** Thanks

Dear Secretary Bowen:  
Thanks for all of your hard work on ensuring we have a secure and fair election voting machine system.

Katrina Anne Foley, Attorney at Law

**From:** Gail Moore  
**Sent:** Tuesday, August 07, 2007 6:23 AM  
**To:** Voting Systems  
**Subject:** voting machines

It's high time to get these voting machines shut down an the people who run them are not trust worthy. That has already been proven.

Now , lets get down to the nuts an bolts of this opperation an close down those machines

**From:** Lois Gregory  
**Sent:** Tuesday, August 07, 2007 2:11 AM  
**To:** Voting Systems  
**Subject:** Voting System

Dear Secretary Bowen:

Thank you for your courageous decision last Friday to require a "Top to Bottom Review" of our voting machines! Your strength in this decision is unprecedented ... and necessary. As a result we should have a fair election in California!

Thank you so much.

Sincerely,

Lois Gregory

**From:** Jcusrus@aol.com  
**Sent:** Tuesday, August 07, 2007 12:16 AM  
**To:** Voting Systems  
**Subject:** Re: Thank you for your email message.

Dear Madam Secretary,

Don't you worry about sending an answer to my e-mail. I am just so proud of you and so happy, delirious, to know that you ran on the promise to bring back votes that cannot be stolen, jimmied, or blatantly x'ed out!!

And you did it, God bless you. Thank YOU for bringing a breath of fresh air into the stink that the Republican Party has brought upon us.

Sincerely,  
Joan G. Rusnak

**From:** Mary Chittenden  
**Sent:** Monday, August 06, 2007 10:45 PM  
**To:** Voting Systems  
**Subject:** Voting systems certification

Dear Secretary Bowen,

I support your decision to decertify the voting systems used in the State of California.

Mary

**From:** L. Eleanor Finney  
**Sent:** Monday, August 06, 2007 10:32 PM  
**To:** Voting Systems  
**Subject:** Voting Systems Decision -Thank You

Dear Secretary of State Bowen:

I can't thank you enough for doing the correct thing. Please hang tough because we know there will be pressure placed upon you by the machine corporations and the Republican Party operatives to reverse or waterdown this decision. You have the full support of the people of this state and you will also have the support of the people of the nation as other states follow your lead. Thank you, thank you, thank you.

It is people like you that give hope, pride and inspiration to the rest of us working so hard to keep our democracy and the value of one person one vote the true beacon it has always been.

We are so proud of you for the integrity and commitment to do the correct thing.

Sincerely,

L. Eleanor Finney

From: Dianne PunKay [mailto:dpunkay@yahoo.com]  
Sent: Monday, August 06, 2007 9:28 PM  
To: Voting Systems  
Subject: Thank you

Dear Ms Bowden,

Thank you for your recent ruling requiring higher standards on the electronic voting machines. Finally there is a public official who appreciates the situation and is willing to do something about it.

Thank you. Thank you. Thank you!

And keep up the good work You have my vote forever!

Sincerely, Dianne PunKay

From: Elaine  
Sent: Monday, August 06, 2007 9:17 PM  
To: Voting Systems  
Subject: Thank you!

I appreciate your stand regarding voting machines in CA. We need to go back to paper ballots! Voting machines, as you pointed out, are too susceptible to hackers.

Elaine Echenique

**From:** Janet Otsuki  
**Sent:** Monday, August 06, 2007 9:14 PM  
**To:** Voting Systems  
**Subject:** voting reform/machines

Secretary of State Bowen,

I have heard about your brave and ethical move to decertify the voting machines here in the state. Thank you for "doing the right thing" in the face of political pressure. A move like this ensures the integrity of our democracy and may motivate disgruntled citizens to keep voting!

Sincerely,  
Janet Otsuki

**From:** J H  
**Sent:** Monday, August 06, 2007 9:05 PM  
**To:** Voting Systems  
**Subject:** THANK YOU

Dear Secretary,

Thank you for your politically courageous act in facing up to ROVs and Vendors. You did a wonderful thing and we are grateful.

Sincerely,

Jim and Shar Hamilton

**From:** Elaine Booth  
**Sent:** Monday, August 06, 2007 8:27 PM  
**To:** Voting Systems  
**Subject:** Thank you

Dear Secretary of State Bowen,

Thank you for your courageous decision to de-certify the voting machines!

Elaine Booth

**From:** J H  
**Sent:** Monday, August 06, 2007 8:20 PM  
**To:** Voting Systems  
**Subject:** Thank You, Thank You, Thank You

Dear Secretary of State Bowen,

**THANK YOU, THANK YOU AND THANK YOU** for your courageous act. We know that this was not an easy decision to make and that you will be fighting the wrath of the vendors and Registrars of Voters as well as an uninformed media.

Please know that there are an awful lot of us here to help in any way we can. We are encouraging everyone in our Secure Accurate Elections group to write letters of support to newspapers, sign support petitions and generally spread the word regarding your fight for the security, accuracy and integrity of our votes here in California.

Please let us know if we can be of help in any way.

Sincerely,  
Sharlene and Jim Hamilton

**From:** Felicitynf  
**Sent:** Monday, August 06, 2007 8:18 PM  
**To:** Voting Systems  
**Subject:** Thanks again!

**Dear Sec. Bowen:**

**Thank you for your courageous decision to decertify the Diebold and Sequoia machines. We stand behind you all the way!**

**Sincerely,**

**Felicity Figueroa**

**From:** Susan Fischer  
**Sent:** Monday, August 06, 2007 5:21 PM  
**To:** Voting Systems  
**Subject:** Thank you

Dear Secretary of State Bowen--

There are no words to express the respect and gratitude I want to extend to you for your extensive and diligent examination of all aspects of the electronic voting machines, thus arriving at your decision to decertify machines used in 39 counties---(with certain exceptions).

I can only imagine the intensity of your examination of all of the issues and reports which led you to your decision---an exhausting and truly remarkable feat, and I commend you!

Of course there will be criticism, but you are so highly respected for your integrity and thoroughness by so very many of your constituents throughout this state and others throughout the country--any criticism is inconsequential in light of your great achievement.

Thank you, Secretary of State Bowen, you have renewed my faith in the integrity of our governmental systems.

Sincerely,  
Susan B. Fischer

From: Gerald Driessen  
Sent: Monday, August 06, 2007 4:28 PM  
To: Voting Systems  
Subject: Your Decision Last Friday

Dear Debra Bowen,

HURRAH for you. GREAT DECISION!!! You took a complex





**From:** R Castro  
**Sent:** Tuesday, August 14, 2007 2:43 PM  
**To:** Voting Systems  
**Subject:** Debra Bowen, Secretary of State

Hurray! for Debra. She did the right thing and we're very proud of her. Keep up the good work Debra. Americans in general and Californians in particular are grateful to you for your smart, ethical and patriotic performance! Sincerely, Richard & Ruberta Castro

**From:** Sybertel  
**Sent:** Tuesday, August 14, 2007 10:31 AM  
**To:** Voting Systems  
**Subject:** Wise Decision

Dear Debra Bowen:

Thank you very much for a great job investigating the insecurity of DRE electronic voting machines!!! Your findings were thorough and comprehensive. You decertified these machines for the most part and by doing so, helped to preserve the integrity of our democracy!

Please work to re-institute paper ballots for all voters. We continue to need a ballot that can be easily recounted and verified by the average citizen using the naked eye. Paper ballots are the only option that can achieve this fundamental check and validation of election integrity.

Again, thank you for your comprehensive and courageous work investigating the defects, flaws, and ready hackability of the DRE electronic voting machines.

Thank you for having the courage to stand up for the California voters. And, thank you, for not yielding to the corrupting weight of corporate demands that were brought forward to subvert the integrity of your wise decision.

Thank you,  
Deborah Mecum

**From:** jlkelsberg  
**Sent:** Monday, August 13, 2007 11:40 PM  
**To:** Voting Systems  
**Subject:** Decertify the Hackable Voting Machines

Ms. Jane Kelsberg

From: Joyce Van Kolken  
Sent: Tuesday, August 14, 2007 3:43 AM  
To: Voting Systems  
Subject: Your Voting Machines Action, THANK YOU DON'T GIVE UP!!!!

Dear Debra Bowen:

I am SO GRATEFUL that you have taken a major step forward in restoring election integrity by decertifying electronic voting machines with the "potential for serious security breaches. I wrote, and called our registrar of voters in San Diego County Deborah Seiling yesterday, and I must say she is 1000% against what you are doing. I can fully understand that because she was a sales rep for Diebold before coming to san Diego. That should give you a hint of how badly San Diego County needs your help.

PLEASE, PLEASE, DON'T GIVE UP ON THIS BADLY NEEDED ACTION. "We The People" of California ARE SO BEHIND YOU. THANK YOU.  
Sincerely,  
Joyce Van Kolken

From: mail  
Sent: Monday, August 13, 2007 1:19 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Dear Debra Bowen,

Thank you for conducting the "Red-Team" review, and please de-certify voting machines that do not meet reasonable security standards.

Sincerely,  
Shawnee Undell

**From:** Mhgeorgia  
**Sent:** Monday, August 13, 2007 8:20 PM  
**To:** Voting Systems  
**Subject:** (no subject)

Dear Secretary of State Debra Bowen;

I regret that I received the PDA email regarding the "Red Team" very late. I want to thank you for taking action to check out the reliability of the machines. It is a problem that is serious enough to threaten our democracy.

You may have already decided what action is needed. In case you are still able to consider California voters opinions, I wanted to let you know that I feel that the machines and the vendors that manufacture them are so flawed that we need to eliminate electronic voting all together and reinstitute paper ballots. If the machines that count the paper ballots (and absentee ballots) are even mildly flawed, we should reinstitute hand counting and sequestering the paper ballots in

secure facilities with access only to certified counters and with transportation to and from storage facilities carried out by bonded and licensed firms. Our one man, one vote tradition demands it.

Thank you for considering my wishes, Mark Georgia

From: Hollis via Rubicon Recluse  
Sent: Monday, August 13, 2007 6:49 PM  
To: Voting Systems  
Subject: Permit no-justification "absentee ballots"

I know I'm late in commenting, but I just read an article about your efforts to protect election integrity.

I live in a no-polling district so get an automatic absentee ballot. I feel much more secure handing in my absentee ballot than trusting an unaudited e-voting machine. Given your short timeframe, maybe this will increase voter trust.

Sincerely,  
Hollis Johnson

**From:** Lowell & Pam Klosky  
**Sent:** Monday, August 13, 2007 5:16 PM  
**To:** Voting Systems  
**Cc:** Pam and Lowell Klosky  
**Subject:** Thanks for the Decertification

Dear Ms. Bowen,

We're so pleased with your actions in decertifying insecure voting machines in California. It was a brave, and very correct, step. We commend you for insisting on high standards to ensure that our votes are accurately counted.

Here's to more secure and accurate elections thanks to your efforts!

Lowell and Pam Klosky

**From:** Scott Currier  
**Sent:** Monday, August 13, 2007 3:30 PM  
**To:** Voting Systems  
**Subject:** Debra Bowen

Just wanted to say thankyou for your stance on voting machines. Our right to have our ballots counted correctly and our ability to believe in our system of government are the corner stones of this country.

THank you again  
Charles Currier

From: ed mcfadd  
Sent: Monday, August 13, 2007 1:01 PM  
To: Voting Systems  
Subject: Voting rights

To: Debra Bowen  
From: Edward McFadd  
879 Hymettus Ave., Encinitas, CA 92024-2151  
emcfadd@flash.net  
Date: August 13, 2007  
Subj: Voting Machines

Thank you so very much for preserving my right to vote and have the vote counted. Our democracy depends on leaders like you who will take on the special interests for our interests, the people's interests. Perhaps at some point electronic voting will be the best method but clearly it is not yet ready. I know in San Diego our voting machines did not work, were not ready at the opening of the voting day when people had to get to work, were malfunctioning with a long delay for knowledgeable service personnel, were not trusted by many in our community. Please, please, do not give up or give in, ever, to the business and political interests that want to destroy our basic political rights.

Thank you.

Sincerely,

Edward McFadd

From: Marilyn Perona  
Sent: Monday, August 13, 2007 11:59 AM  
To: Voting Systems  
Subject: Thank you, Secretary of State Debra Bowen

Dear Secretary Bowen,

We thank you for helping maintain the integrity of voting in the State of California and in our country. I have not used an electronic machine for several years because of all the problems. It is imperative that we have verifiable, countable paper ballots to back up the electronic numbers.

Thank you for your part in maintaining free and fair elections.

Sincerely,  
Mae Perona and Marilyn Perona

From: booker  
Sent: Monday, August 13, 2007 9:20 AM  
To: Voting Systems  
Subject: voting machines

Thank you for your courage and integrity in decertifying insecure voting machines. Audrie and Steven Clark

**From:** Joanne Goodwin  
**Sent:** Sunday, August 12, 2007 8:19 PM  
**To:** Goldberg, Evan  
**Cc:** Voting Systems  
**Subject:** 'Red Alert' Sent Over Touchscreen Use In Iowa GOP Straw Poll

Ron Paul's campaign was afraid of the Diebold TS machines and warned that they could be used to manipulate the vote. Well, they didn't use the TS machines, but DID use Diebold's optical scan machines and 2 machines malfunctioned, so they had to count those paper ballots by hand. That dlayed the results. One machine tallied 498 votes, but there were actually 500 votes registered from that machine, after the hand count.

below, this column was written on 7/15/07:

<http://www.bradblog.com/?p=4818>

BLOGGED BY **John Gideon** ON 7/15/2007 10:34AM  
Ron Paul Supporters Concerned Diebold DREs Will be Used to Deny 'Groundswell of Support' for Surprisingly Popular Candidate...

*Guest Blogged by John Gideon, [VotersUnite.Org](http://VotersUnite.Org)*

August 11 is the date for the Iowa GOP presidential "straw poll." In this "straw poll" Republican voters from all over Iowa will walk, drive, or share a bus to the campus of Iowa State University where they will be allowed to pay \$35 each for the honor of casting a ballot for their choice for President.

This "poll" is semi-important within the world of Republican politics. Both McCain and Giuliani have decided to pass and will not participate. However, for the candidates who are lower down in the polls this "straw poll" may be all important. The supporters of Dr. Ron Paul, for instance, claim that he has thousands of supporters within the state and that they are going to do all they can to get them to Ames.

With all of that the supporters of Paul have got another gripe and concern that sounds much like the same concern many in the Election Integrity community have; the poll, which used to be done on paper ballots, hand-counted in public, will be conducted on Diebold Direct Recording Electronic (DRE) voting machines. The Ron Paul group is very concerned that the machines will be gamed in order to make their candidate's showing less than what it should be and in order to inflate the results for those whom the Republican National Committee (RNC) want to have a good showing.

The following email was sent by a member of Paul's support group to a large list of Election Integrity groups:

From: Ron Paul NoHo Meetup  
Sent: Saturday, July 14, 2007 9:51 AM

Subject: VOTE FRAUD RED ALERT: Diebold electronic voting machines to be used at Iowa straw poll!

The Iowa GOP has decided to use Diebold electronic voting machines at the Iowa straw poll on August 11th. The straw poll has always been counted in the open with paper ballots...until now. They are about to deny the people the vote again, this time to turn back the popular groundswell of support for Dr. Ron Paul.

Please investigate and spread the word! Please reach across the aisle and help! This affects ALL Americans! PLEASE MONITOR THIS STRAW POLL!

Yours in support of Ron Paul for President,

Steven Vincent

North Hollywood Ron Paul Meetup

<http://ronpaul.meetup.com/104/>

"First they ignore you, then they laugh at you, then they fight you, then you win."  
Gandhi

Vincent is incorrect when he says that the straw poll has **always** been counted in the open and with paper ballots. In 1995 voting machines were used and there was some dispute because Sen. Dole and Sen. Graham got the same number of votes exactly.

Nonetheless, we'll keep our eye on this one, as it could be an interesting moment with touch-screen Diebold DREs at the center of national attention on that day. Particularly if something goes --- obviously --- wrong. Unfortunately, the trouble with DREs, is that most of the problems aren't obvious at all. Hence, the grave danger they pose to democracy...

[Here's a pretty good comment by a blogger on Bradblog.org:](#)

COMMENT #2 [[Permalink](#)]

... [DREDD](#) said on 7/15/2007 @ 12:25 pm PT...

John and Onyx,

I like the concept of "counted in public". But lets add "stored in a third-party location", "with sign in and sign out sheets", and "store them in tamper proof, locked boxes".

And video the whole damned process.

Yes I am a skeptic who has little faith in the system. Instead I have science in the system. Evidence chain of command procedures are not overly complicated.

So paper ballots stored by an independent agent (bi-partisan sane committee), locked in tamper proof boxes, with sign in and sign out ledgers, no access except to store them on election day, count them in the open on election day, and store them. All on video.

That is the american way ... to remove as much temptation and security weakness as possible.

If software driven machines are to be used, then they must meet the same criteria.

---

**Sent by:**

**Joanne Goodwin**

**From:** Joanne Goodwin  
**Sent:** Sunday, August 12, 2007 8:16 PM  
**To:** Goldberg, Evan  
**Cc:** Voting Systems  
**Subject:** Diebold Optical-Scan System Fails in Iowa GOP Straw Poll!

<http://www.bradblog.com/>

[Diebold Optical-Scan System Fails in Iowa GOP Straw Poll!](#)

Results Delayed as Atleast 1500 Paper Ballots Re-Counted By Hand (Fortunately, There WERE Paper Ballots To Re-Count!)  
Ron Paul Supporters Were Right to be Worried About Republican's Choice of Diebold to Tally Votes...

*Guest Blogged by John Gideon of [VotersUnite.org](http://VotersUnite.org)*

As [we reported](#) on July 15, Ron Paul's supporters were concerned that Diebold touch-screen voting machines were going to be used in the Iowa Republican Straw Poll. Well, it turns out the concerns about touch-screens were misplaced, as the GOP chose paper-based Diebold optical-scan machines instead. But their fears of Diebold may well have been justified as two of their op-scan systems failed and delayed the reported results.

While GOP candidate Mitt Romney may have walked away with a winning edge in the Iowa Straw Poll, Diebold was true to form as their voting system failed to count ballots correctly. As the [Des Moines Register is reporting](#) two of Diebold's optical scanners failed and 1500 paper ballots had to be manually recounted by hand...

Voting machine difficulties delayed the announcement of the vote totals. About 1,500 ballots needed to be recounted, said Mary Tiffany, a spokeswoman for Republican Party of Iowa.

Two machines caused the problem, said State Auditor David Vaudt. "What likely happened is someone submitted their ballot too quickly after the other," he said. The ballots from those machines were hand counted, then re-fed into the system to recalculate the vote. A campaign poll-watcher said in one instance, a black box contained 500 paper ballots but the machine's memory said it had scanned in 498.

*(One has to wonder how many OTHER Optical Scan machines failed to register the proper number of votes. If only those 2 machines were examined, how would anyone know? With only 6 candidates and no referendums, it seems to me it should be really easy to count, and yet, those machines STILL couldn't get it right the first time around. Joanne)*

At least there were paper *ballots* that could be hand counted when the machines failed. Had the Republican's used Direct Recording Electronic (DRE) voting machines --- as millions of Americans are forced to do each Election Day --- there would have been nothing to go back to when the machines failed.

**UPDATE:** [The Atlantic is reporting](#) the number of ballots which had to be "re-run" as "about 4,500".

Either way, there were reportedly 14,203 total ballots cast. So going by the *Des Moines Register's* reported numbers, more than 10.5% of the ballots had to be recounted. If we go by *The Atlantic's* reported numbers, nearly 32% of the ballots in the Iowa Republican Straw Poll had to be recounted by hand.

Sent by:

**Joanne Goodwin**

From: [conniemessina@cox.net](mailto:conniemessina@cox.net) [mailto:[conniemessina@cox.net](mailto:conniemessina@cox.net)]  
Sent: Sunday, August 12, 2007 7:14 PM  
To: Voting Systems  
Subject: voting integrity

Debra, keep up the high standards. When we lose fair elections in this country, we lose democracy. You are doing a great job. Connie Messina, San Diego County  
P.S. I ran for a seat on my city council last year, so I know how important every vote is.

**From:** Judy Ki  
**Sent:** Sunday, August 12, 2007 4:26 PM  
**To:** Voting Systems  
**Subject:** Thank You so much, Ms. Bowen!

Dear Ms. Bowen,

Thank you so much for having the wisdom and the courage to stand up for our democracy! All the precinct walking etc. really paid off for us. You are there to advocate for us, the voters.

Regardless of what the biased media, the ROVs, and the DRE vendors say, please know that We, the PEOPLE, are behind you 100%. Many of us admire your courage and wisdom.

THANK YOU! THANK YOU! THANK YOU!

Sincerely,  
Judy

Judy Ki

**From:** Steve Eklund  
**Sent:** Sunday, August 12, 2007 4:09 PM  
**To:** Voting Systems  
**Subject:** Thank you

Secretary Bowen -

Thank you for decertifying the DRE machines. I hope we can still save our democracy. If more public servants had your sense of integrity, it would be easier.

Again, thanks,

Steve Eklund in Salinas

**From:** Joanne Goodwin  
**Sent:** Sunday, August 12, 2007 4:50 PM  
**To:** Voting Systems; Goldberg, Evan  
**Subject:** Three Letters to the Editor today.

**Three letters to the editor in today's NC Times that I thought you might like to read. I added my comments to the last one (shown in italics and blue print.):**

**Convenient and provably secure voting**

Is it reasonable to expect and to have convenient, provably secure voting? Currently your vote is neither provably secure nor convenient, but is provably not secure and inconvenient.

With the current voting fiasco our elected officials have clearly demonstrated their

incompetence in providing this fundamental and absolutely vital democratic process. In a sincere democracy the people's vote is sacred and highly valued because it reflects the will of the people, not special interests or of those in power. We must hold accountable those officials who have failed in their responsibilities, demand that we have convenient, provably secure voting and will not entertain or accept any excuses that it cannot be done.

Provably secure voting is the how, and the hardest part (but not that hard). The when we vote part is the other persistent obstruction to our voting. Why on Tuesday and not Saturday or Sunday when it would be much more convenient? Is Tuesday sacred? No. Would this change increase voter turnout? Yes. Would it be difficult to do? No.

This continuing corruption of our democracy will never be truly fixed, only patched up, until we, the people, incessantly demand and have an authentically convenient, provably secure vote.

William Stephenson

### **Bowen's decision is applauded**

We applaud the courage displayed by Secretary of State Debra Bowen to finally deal with the appalling lack of security of electronic voting machines in this state (["Restrictions set for voting machines," Aug. 5](#)). A return to paper ballots and encouraging Californians to become permanent absentee ballot voters is a major step to protect the constitutional right of voters to have their votes accurately counted.

Debra Bowen has finally done what needed to be done. There was overwhelming evidence that the voting machines planned for use in our next election were easy to hack into, so, for those in registrars' offices and elsewhere who oppose her decision, one can only imagine their motives.

Diane Ohanian

### **Ultimately, we have to have faith in system**

*You bet you do, and from the history on these electronic machines, I don't see how anyone can have faith in them or who handles them.)*

There is much controversy in regard to the trustworthiness of electronic voting machines. Unfortunately, we have to accept the fact that there is no fail-safe method for any man-made process.

Opponents tell us that the machines are subject to hacking. Most computer hacking is by way of the Internet. The only part of the system that uses the Internet is the transmission of vote totals to a central location. If what I read is correct, even the paper ballots are counted electronically and sent, via the Internet, to a central registrar of voters. *(and that's WHY we can NOT have electronic machines in any form, counting our votes! And*

*please remember that at every turn, our RoVs have insisted, as well as Diebold, that no modem was ever used and no internet connection, period. Remember all that? I, for one, am sick and tired of being lied to.) If precinct workers were to enter the machine and change vote totals, then what would prevent those same precinct workers from using a variety of methods to change the paper ballot totals? Exactly... that's why PROPER monitoring is absolutely necessary, as well as a secure chain of custody, which is very much easier to achieve than bulky electronic machines, and hand-counting done by selected volunteers trusted by each party, and overseen by different groups of concerned citizens. And the money SAVED would be unbelievable in comparison to what we have now. No more electronic machines!)*

Yes, it is possible that the machines could be tampered with during transit to the precincts, but there are methods to assure that does not happen. It should be obvious to all that the history of voting procedures indicates paper ballot voting can be untrustworthy. It doesn't make any difference which voting method is selected if it will be necessary to accept some faith in the integrity of all who are involved in the voting process. *(Sorry, but I DO expect the utmost trust in anyone involving my vote and will not ever accept anything less.)*

Marion Wetter

**Sent by:**

**Joanne Goodwin**

**From:** Joanne Goodwin  
**Sent:** Sunday, August 12, 2007 2:30 PM  
**To:** Goldberg, Evan  
**Cc:** Voting Systems  
**Subject:** Please read--Paper Ballots Necessary to Preserve Democracy

**Please be sure and read this. It says what so many of us have been fighting for the last 5½ years here in San Diego County. It's really difficult NOT to get a deaf ear from our FIVE Republican Supervisors. Please know that so many really concerned voters are 100% behind Sec. Bowen, and other states are closely watching. I just watched a part of "Election Integrity" on C-Span this morning (tuned in too late to get it all) and Sec. Bowen was mentioned a lot and there were people from Florida who spoke of how they got rid of their touch screen machines, and why...and one man got up and said that there was a case in Florida and a study subsequently done, where, after they went to paper ballots and allowed them to be counted on optical scan machines...they found that the memory card in those could be changed to alter the votes, and it is UNDETECTIBLE. The study completely backed that fact up. So paper ballots and hand-counting is the only way we'll ever believe that we have a chance of having all our votes counted...and counted accurately. The Election Director of the Election Technology Council, David Berne, said he was very aware of the case in Florida that that man was speaking about. These vendors ALWAYS promise to "fix" the problems, and then it's ALWAYS discovered after another election that the same problems still existed. How many YEARS they've done this, and always got away with it. ENOUGH. Computers, in whatever form, can be manipulated, and/or "lose" votes, overcount more votes than actual voters, just freeze altogether, and on and on. Just think of all the money that could be saved by having a system of paper ballots and hand-counting. Please read this column by Ken Karen. It is excellent.**

**GREAT, GREAT COLUMN TODAY, August 12th, IN THE NORTH COUNTY TIMES--  
"PERSPECTIVE" SECTION, written by a co-founder, Attorney Ken Karen, of the magnificent  
group, called PSEPHOS, a really special elections watchdog group. The other founder is Attorney  
Paul Lehto**

**From:** Richard J.Thompson  
**Sent:** Sunday, August 12, 2007 1:22 PM  
**To:** Voting Systems  
**Subject:** Voting Machines

**Thanking you for conducting the "Red-Team"  
review, and decertifying the  
machines that do not meet reasonable  
security standards and hold the companies  
accountable for lying and deceiving the  
state officials.**

**From:** Karen Achor  
**Sent:** Sunday, August 12, 2007 7:31 AM  
**To:** Voting Systems  
**Subject:** Thank you so much

Debra Bowen,

**Thank you so much for your courage and intelligent action!  
Your brave stand allows up a great chance for fair elections in California.  
This is a historical event.**

**Thank you again,  
Karen Achor**

**From:** delightedeye  
**Sent:** Saturday, August 11, 2007 12:59 PM  
**To:** Voting Systems  
**Subject:** Decertify the Hackable Voting Machines

Thanks Debra for doing this. I worked for your election. Bless you  
for following through and serving the People.

Ms. Katherine Woodford

From: jmp852  
Sent: Saturday, August 11, 2007 10:18 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

No computerized voting at all! Too easy to cheat like in the last two presidential elections. W should never have been president at all.

Mr. Jeff Potter

From: bev  
Sent: Saturday, August 11, 2007 7:08 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Ms. Bev Huntsberger

From: mpalladine  
Sent: Friday, August 10, 2007 7:20 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Ms. Michelle Palladine

**From:** Angelo Vassos  
**Sent:** Friday, August 10, 2007 7:54 PM  
**To:** Voting Systems  
**Subject:** Thank you

Thank you for decertifying the Diebold and Sequoia machines.

Angelo Vassos

From: gnierman  
Sent: Friday, August 10, 2007 9:48 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Our democracy is only as strong as the integrity of our elections, and our elections have become tainted with scandal this decade. To save our democracy, we need to protect the accuracy of elections, and since electronic voting machines have proven to be easily tampered with, we need to banish computer voting. In my court we traditionally mark paper ballots. The whole country should go back to paper ballots, to keep it from going to the dogs.

Dr. G.L. Nierman

**From:** J H  
**Sent:** Friday, August 10, 2007 2:38 PM  
**To:** Voting Systems  
**Subject:** Thank You Debra Bowen

Thank you Debra Bowen for your stand on  
bogus electronic voting in Ca  
Shirley Weaver

**From:** Cathy Miller  
**Sent:** Friday, August 10, 2007 2:00 PM  
**To:** Voting Systems  
**Cc:** Goldberg, Evan  
**Subject:** Thank you and we are behind you!

Dear Secretary of State Debra Bowen,

We have worked so hard for so long with so little forward movement (until now!) that your announcements on August 4 seemed like a wishful dream in the mind and heart of a very dedicated election integrity activist. But after pinching myself several times, I found that it was all true!

Your integrity, high standards, determination, and courage have made you the heroine of the day for all of us dedicated to preserving democracy--because that is how we see this fight over our election systems. By decertifying all touch-screen machines, you have made huge strides in rolling back the problems and threats posed by the DREs.

To say thank you seems like a paltry way of expressing how I and all my fellow activists are feeling right now--but just the same: thank you from the bottom of my heart.

I've been reading what the election officials have been saying, what the Diebold and other election machinery companies are saying, what Conny McCormack down in LA has been saying about your rulings. I know you expected a fight, and I'm going to guess that your opponents may hand you a very unpalatable one. Is there anything that we, as citizens and as activists, can do to show our support? Writing an email of thanks is a positive gesture, but I've always believed in showing my gratitude by the actions I take. You have a veritable army of citizens who are rallying around you--I feel certain all of us together could surely do something to help. I'll go further--I think we're all anxious to help and would jump at any and all suggestions. All we need is for you to let us know what we can do.

I believe you were elected on the promises you made to clean up election systems. Now that you've made good on those promises, you have a \*majority\* of the people of California behind you, a majority that includes some of the finest election integrity activists in the nation. Just let us know what we can do.

Thanks again for what you've done, are doing, and will do to return our elections to safety, security, transparency, and accuracy.

Warmest regards,

Cathy Miller

From: beads

Sent: Friday, August 10, 2007 5:45 AM

To: Voting Systems

Subject: Decertify the Hackable Voting Machines

Our confidence in the right to vote is being comprimised my computerized hackabke voting machines! I wnat my vote to count, not erased by someone who does not agree with my vote! Please have the courage todo the right thing and get rid of hackable voting machines!

Ms. Charlotte Silverstein

From: agnes pennington

Sent: Friday, August 10, 2007 12:15 PM

To: Voting Systems

Subject: Thanks

Dear Debra Bowen.

Thank you so much for your courageous decision to decertify the voting machines. I am proud to have voted for you. Please keep up the good work, we have your back.

Agnes Pennington

From: Marilyn Vassos

Sent: Thursday, August 09, 2007 10:10 AM

To: Voting Systems

Subject: Voting in California

Dear Secretary of State Bowen:

Many thanks to you we can hopefully look forward to fair elections in the state of California. I appreciate all you have done to bring

this about and wish you success in your future efforts to keep our elections clean.

Sincerely,

Marilyn Vassos

From: Barbara Davenport  
Sent: Thursday, August 09, 2007 8:35 PM  
To: Voting Systems  
Subject: Stand fast!

Dear Ms Bowen  
\*I'm delighted with your decision to restore election integrity and ban unsafe voting machines. I'm a resident of San Diego County, & I'll weigh in with my local registrar in praise of your decisions. \*  
\*Thank you.\*  
\*\*

**From:** J H  
**Sent:** Thursday, August 09, 2007 7:06 PM  
**To:** Voting Systems  
**Subject:** Thank you again

Dear Secretary of State Bowen,

We are sending the email address out to people we know who wish to thank you for your courageous act.

Sincerely,  
Sharlene Hamilton

From: rchiersch  
Sent: Thursday, August 09, 2007 11:14 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Mr. Richard Hiersch

From: gcarcher  
Sent: Thursday, August 09, 2007 10:59 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Thank you for your courage!!! please, now, decertify the hackable voting machines and get back to community counting of our votes. We don't want fascist corporations telling us who we voted for.

Mr. greg clever

From: moonglum8  
Sent: Thursday, August 09, 2007 10:14 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Ms. Amber Cannon

From: beverlyscuff@comcast.net  
Sent: Thursday, August 09, 2007 8:00 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

We must have a voting method we can trust, with a paper trail to verify it. We urge careful consideration to be sure the method chosen is not corruptible

Ms. Beverly Scuff

From: Jerry Earll  
Sent: Thursday, August 09, 2007 2:46 PM  
To: Voting Systems  
Subject: Count every vote - fairly

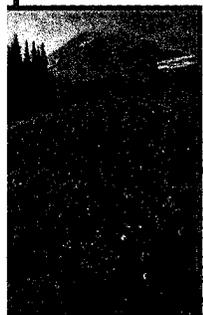
We must stop the manipulation and risk faced with electronic machines. We must make it possible for every eligible voter to vote and know that the vote will be properly counted. They shouldf be able to vote on one of several different days, absentee ballot - anything that makes it possible for non affluent people to get to the polls. Thank you for caring. Jerry Earll

AUG 1 1987

Dear Debra Basson,  
Just a few lines  
to let you know I'm  
concerned about people  
with voting.

Some from Washington  
State originally. They  
all vote by absentee  
ballot so you really  
have to think and talk  
about who to vote for.

They have a lady  
governor now, but I  
don't know how long they  
have voted this way.



Some a senior citizen  
so he vote absentee, so  
many of us are off to a  
good start there, I'm sure.

Arlene Wasson  
Ventura



Robert K. Zentmver

August 8, 2007

Honorable Secretary of State  
1500 11<sup>th</sup> Street  
Sacramento, CA 95814

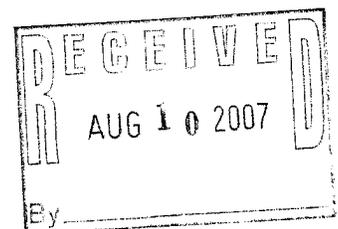
Dear Ms. Bowen,

I am writing this letter to express my dismay, if not anger, at your decision to decertify electronic voting machines throughout California. This decision seems to be motivated purely by politics, certainly not on actual facts regarding the integrity of the voting system in California. If your decision, in fact, had been based on actual facts, you would have announced your tentative decision enough in advance to allow the various local registrars to demonstrate how their ongoing procedures make subverting the system very difficult, if not impossible.

I have been a poll worker for several years and, for the past two years, my garage has been a polling place. I have had experience with both paper ballots and the electronic machines and can tell you that the security procedures used in San Diego County make tampering with electronic machines physically impossible without the subverting of all the members of a polling place. Furthermore, in neither of the two times I had experience with paper ballots was my team able to balance at the end of the day. This last election we balanced on the first try.

On the remote chance that you might be interested in facts rather than politics, let me enumerate the methods used in San Diego County to ensure the integrity of the process.

- All members of polling teams receive several hours of training.
- All materials, including the cards for the electronic machines are maintained in the custody of the senior precinct member
- The electronic voting machines, with seals affixed which cannot be removed without destroying them, are in the custody of the assistant precinct leader for machines and are kept in his personal custody in his home until election morning. Please note that this individual does not have the cards to activate the machines even if he or she could figure out a way to open them without destroying the seals.
- On election day morning, the machines are brought to the polling place, are set up by the other members of the team and zero balances are verified by the team AND by the first voter to vote. The seals are verified against a list provided to the senior precinct worker at the time he or she received the remaining materials. At the time the machines are activated, a zero paper report is run which goes into the SEALED receptacle on the machine.



- At the end of voting, final reports are run on all machines and signed by three members of the polling team. These reports are verified against the voters' roster and the totals must match.
- The memory cards are then removed from the machines and placed in a sealed pouch which is hand-delivered to representatives of the Registrar of Voters along with previously removed (and destroyed) seals.

As you can deduce, if you are so inclined, while it certainly is possible, in a laboratory setting with trained technicians, to tamper with the electronic machines in San Diego County, the procedures put in place by the Registrar of Voters would require the collusion of a large number of people to even get access to the machines.

Finally, your ruling is an insult to the many hundreds of poll volunteers who man the polls on Election Day and it denigrates the security and honesty of the entire voting system because of a handful of anomalies. You would be far wiser and perhaps more courageous to keep the election process up to date rather than retreating to an earlier method which also is not foolproof, has many problems of its own, and will most assuredly delay the counting of votes significantly without materially improving the integrity of the system. I, for one, will not be a poll worker again with paper ballots and my garage will not be a polling place until you reverse this ill-conceived decision.

With disappointment,



Robert K. Zentmyer

P.S.: This decision makes me a bit ashamed to be a fellow Democrat.

August 6, 2007

The Honorable Debra Bowen  
California Secretary of State  
1500 11<sup>th</sup> Street  
Sacramento, CA 95814

Fair and Transparent Elections in California

Dear Secretary of State Bowen:

Though I reside in Salt Lake City, Utah, I want to thank you for your astounding courage, wisdom and leadership in severely curtailing any further abuses by the DRE voting machines (and their related hazards).

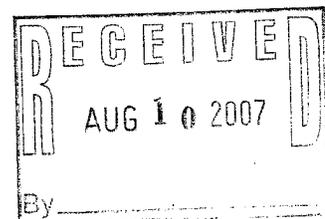
I can only hope your actions are an inspiration to Utah officials, Sen. Dianne Feinstein, Rep. Rush Holt, et al.

Again, you should be remembered as one of the stellar heroes of California's effort to revive and maintain honest elections.

My sincerest thanks and appreciation for your wonderful bravery!

Sincerely,

  
William L. Alder



August 8, 2007

Debra Bowen  
California Secretary of State  
1500 Eleventh Street  
Sacramento, CA. 95814

Dear Secretary of State Bowen

Thank you for testing and then decertifying the defective electronic voting machines which can be hacked.

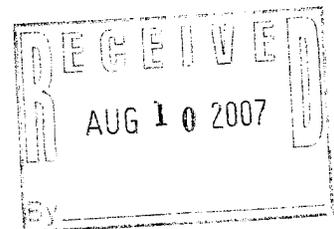
You are a hero to stand up against the political power that these companies have. I support you in your efforts to have honest elections.

If there is any way we can help in the efforts to have honest government please let me know.

Sincerely,

*Jean H. Beek*

Jean H. Beek



Andrew Chandler

8/31/2007

Debra Bowen  
California Secretary of State  
State of California  
1500 11th Street  
Sacramento ca 95814

Dear Secretary of State Bowed,

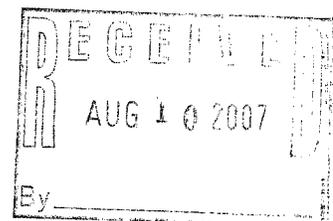
I am as you, very concerned about the fairness of elections and find the notion that an electronic voting machine being hacked to be unacceptable. For this reason I am requesting that you maintain your position that electronic voting machines that compromise our election process be decertified and that a paper trail be provided on all elections.

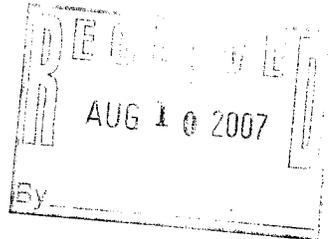
We cannot in this state have any issue regarding the fairness of the vote, that looks anything like Ohio or Florida in previous elections.

A paper trail is important and only way to maintain confidence in the voting system. This loss of confidence is the equivalent to a loss in of democracy. Mayhem and Chaos could result and it would be totally preventable.

I request that you make every effort to maintain a paper trail in any election and that you state publicly that it is a goal for this state. One of the best places to live in the world.

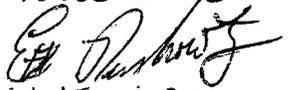
Sincerely,  
Andrew Chandler  
Orange vale, CA



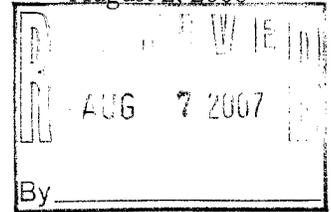


AUGUST 7, 2007

DEAR MS. BOWEN,

IN LIGHT OF ALL THE MONIED  
OPPOSITION, IT TOOK COURAGE TO DO THE  
RIGHT THING. PERSONALLY, ONCE COMPUTER  
SCREENS APPEARED AT MY POLLING PLACE,  
I BEGAN VOTING ABSENTEE; I DON'T TRUST  
THOSE THINGS NOR THE POWERS BEHIND  
THEM. THANK YOU!   
EDD RUSKOWITZ,

August 2, 2008



To: Debra Bowen, California Secretary of State  
1500 11th Street  
Sacramento, California 95814

cc: Mike Villines, Assembly Republican Leader

From: Susan Klassen

Dear Secretary of State Bowen,

I am writing to express my concern over the use of electronic voting systems in the coming elections. The attached story indicates that the systems used in Fresno, made by Diebold Elections Systems, Sequoia Voting Systems, and Hart InterCivic, are not secure from tampering. In fact, they are easily hacked into within minutes, and election results altered.

To put it lightly, I find this alarming! We are heading into the most critical elections in my lifetime, most importantly, the Presidential race. With so much at stake, an election corruption incident would be disastrous to the moral of the people of this state and country.

As Secretary of State, it is your sworn duty to protect the sanctity of the peoples vote. Otherwise, why hold elections. If these systems are not as secure as systems used in the past, let's go back to the past technologies to secure our coming elections from corruption, and thus our legal system hijacked by the unscrupulous. Technology can save money, and streamline processes, but, in this case, the highest possible security is all that matters. I ask you to diligently increase precautions from spoiled election results.

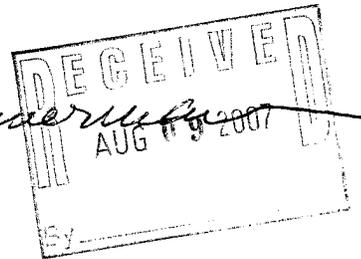
Sincerely,  
Susan Klassen

The story attached can also be viewed at: <http://www.fresnobee.com/opinion/story/101906.html>

Dear Debra Bowen,

Many Thanks for your  
action to have all  
election machines tested  
GOOD WORK !!

Patsy Bauer



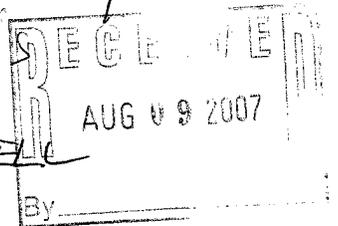
blue pond:

DEAR DEBRA

Continue your good work  
for ~~local elections~~!

Thank you for your  
great effort

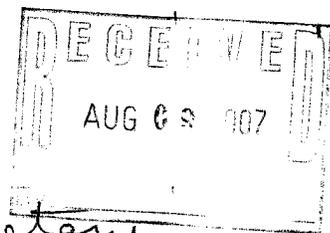
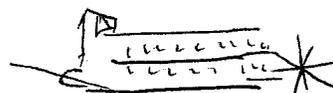
Jody FARRELL



and of my website,  
Steamboats.com

Nori J. Muster

Sincerely,  
Nori



Thank you Secretary  
Bower for restricting  
the illicit voting  
machines. God bless  
you. By the way, I  
visit Old town several  
times a year & stay on  
the Delta King. Lots

↑

RECEIVED  
AUG 09 2007  
8/6/07

Dear Ms. Bowen,

I wanted to thank you  
all your work & study on the  
tiring machines. we want a  
fe, sore way to vote everytime!  
to have done the right thing.

Sincerely,

Barbara Gaman

Barbara Gaman

Secretary of State,

8/6/07

am very pleased to  
that you are  
certifying electronic  
tiring machines that do  
" ... standards.

RECEIVED  
AUG 09 2007

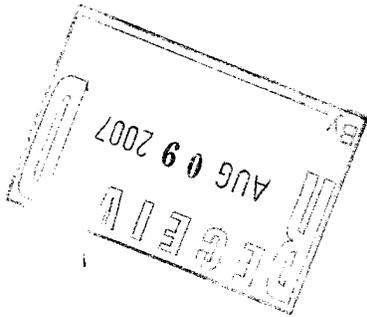
8/6/2007

Dear Ms. Brown

I was so impressed with your vigilance  
quick & responsible protection in canceling  
the use of E. Machines for voting - While the

Paper method has been used successfully for  
these years the public is increasingly suspicious  
rightfully so of the emergency force the use of  
Machines whose veracity is questioned. You did  
HERO to all of us out here who value their  
of our most cherished tradition OUR VOTE, and  
its integrity never be questioned or compromised  
indeed the "framers of our constitution" all smile  
down at you & saying "Daughter, job well done" My  
fam. & I

for Mrs. Bowen  
Thank you for having the  
average to stand up for what  
right is.



Joanne Fleming

This was in the Huffington Post blogs today.

Congratulations to you. We put our trust in the right person.

I'm sure those around you probably have already brought your attention to this article. But just in case they missed it -- I wanted you to see this, and to include this in your scrapbook of pleasant memories. One you can look at when the world around you may look gray, and you need to reaffirm the good you are doing.



Andrew Gumbel

## **A California Politician Does Her Job**

Posted August 6, 2007 | 04:30 PM (EST)

Everyone who cares about American democracy should raise a toast – or a hat, or a loud cheer – to California's Secretary of State, Debra Bowen, a politician who has somehow resisted the pressure of special-interest lobbyists, campaign fundraisers, and the rest of whole dubious cabal surrounding modern politics and actually done the job of representing the people who elected her to office.

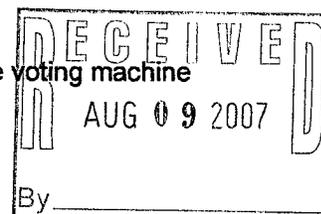
Literally minutes before a self-imposed midnight deadline last Friday, Bowen decided to decertify every last electronic voting system in California. That means, with a few exceptions to make provision for disabled voters and early voting, the country's most populous state will be reverting to paper ballot systems for the presidential primary next February and every other election thereafter.

In some ways, Bowen's decision was a no-brainer. Study after study over the past four years has shown that the systems developed by the likes of Diebold, Sequoia and Election Systems & Software are riddled with software-writing flaws and security holes, not to mention a propensity to fail catastrophically in live elections. There are any number of ways that a computer-savvy outsider could hack into the system and compromise the integrity of the vote; the opportunities only multiply if someone already working for a country registrar's office decides to dabble in a little insider foul play. Bowen herself commissioned an exhaustive review of the state's four voting systems (the fourth being from the Texas company Hart InterCivic), which not only confirmed many of the flaws previously identified by the country's top computer scientists but added a few more – most notably the fact that Diebold's and Hart's systems compromise ballot secrecy because it is remarkably easy to reconstruct who cast which ballot.

Still, it took an act of considerable political courage for Bowen to issue her ruling. In the run-up to the 2004 election cycle, her predecessor Kevin Shelley became the country's first secretary of state to insist on a paper trail to act as a back up to electronic votes, and subsequently decertified a whole class of Diebold electronic machinery in response to a litany of company lies and incompetence. Shelley was subsequently bombarded with accusations of improper conduct in office – some of them since shown to have been exaggerated or fabricated – and drummed out of office, his reputation suddenly in tatters.

Bowen, like Shelley, is facing a wall of hostility from certain country registrars as well as the voting machine

Monday, August 06, 2007 AOL: Interlude11



manufacturers themselves. They'd no doubt love to discover that she, like Shelley, has an anger management problem, or that something was awry with the accounting from her own election campaigns. Bowen, though, has a reputation as the straightest of straight arrows. And she also has time on her side. While it might have been controversial to suggest, in 2003 or 2004, that the new generation of electronic voting machines were an invitation to voter fraud on an unprecedented scale, it is now much closer to received wisdom. Florida and New Mexico are hurriedly moving away from electronic voting. Many other states are conducting reviews. Individual counties, many of them burned to the tune of tens of millions of dollars on systems they no longer trust, are running scared from one end of the country to the other.

California tends to be a bellwether in these matters, so it's a fair bet that Bowen's ruling will greatly accelerate the nationwide trend away from electronic voting to something more transparent and verifiable. (Optically scanned paper ballots seem to be more reliable, and cheapest, way to go.) In other words, she has notched an unambiguous victory for the cause of voter rights.

This is, of course, a mess the country should never have gotten itself into. But money and influence go a long way in this political system. It's to Bowen's endless credit that she has refused to be swayed and defended the public interest instead. That used to be what democratic politics was all about. These days, it's a radical act.

TexasDem0 (See profile | I'm a fan of TexasDem0)

How far our nation has fallen. Debra Bowen does her job and it truly is a radical and commendable act. Let's hope this is an early step in reclaiming our government for its rightful owners, the public.

Log in | posted 05:00 pm on 08/06/2007

IronDragon (See profile | I'm a fan of IronDragon)

Secretary Bowen will be forever praised for the totally welcome surprise she gave to voters in the Golden State. Her decision pulled me back from abject cynicism to my more accustomed skeptical stance.

Log in | posted 05:22 pm on 08/06/2007

dsenator (See profile | I'm a fan of dsenator)

Andrew Gumbel is right on in his praise for California Secretary of State, Debra Bowen's decertification of the electronic voting machines currently in use. Although the technology exists to have voting machines that are paper ballot safe, secure and reliable, none of the systems currently marketed have these capabilities, and until there is a nationally proven safe, secure and reliable system, it is both questionable and foolish for local election "officials" to spend millions for electronic voting. Unfortunately the politics of favor and funneling public funds into certain private hands is still alive and well; and the continued spending of public funds by local officials to their "connected" private friends will resist and attempt to discredit the unbiased acts in the public interest of elected officials the likes of Debra Bowen.

Log in | posted 05:58 pm on 08/06/2007

TXfemmom (See profile | I'm a fan of TXfemmom)

I find it terribly sad that the action of Secretary Brown, which are clearly legal and what needed to be done, is so remarkable, that it must be met with these remarks.

I admire this woman and I hope it creates a groundswell of court rulings and public opinion which forces the same outcome on the rest of the corrupt who have not followed her lead.

Log in | posted 08:02 pm on 08/06/2007

chharriett (See profile | I'm a fan of chharriett)

When does this happen in every state that uses electronic voting? If the Dems can't stop these criminals from expanding and abusing power, and my state (NC) uses them, why would I even bother voting? If I'm correct, Feinstein had a bill, but claimed it couldn't be done for '08. WTF??? I realize that it was for paper trails, but still...WTF??? Congress desperately needs to pass a law. Just look at what happened in Ohio.

Log in | posted 08:03 pm on 08/06/2007

youngharry (See profile | I'm a fan of youngharry)

**BRAVO, BRAVO, BRAVO, DEBRA BOWEN IS A REAL AMERICAN HERO.**

For those who would diminish Debra's contribution to this country and the safety of our elections, you are either too ignorant to understand her accomplishment or are on the take from the Electronic Voting Machine Companies.

Log in | posted 08:07 pm on 08/06/2007

freedomis (See profile | I'm a fan of freedomis)

As a Californian she makes me proud and as an American I hope this does start a landslide to take our voting rights back. Maybe we can put a few congresspersons out to pasture and get some people in that listen to all Americans not just the few who have money. Tony

Log in | posted 08:35 pm on 08/06/2007

starsnsea (See profile | I'm a fan of starsnsea)

Debra Bowen and her staff, including Lowell Finley, are the heroes of this election and this decade, that is for sure. Millions of Americans, including me, feel profoundly grateful for her tremendous courage to do the right thing for the right reasons, at the right time. May her courage inspire our own and help us to turn this great ship of our nation onto a course where we embody honor and respect for our nation's ideals.

Thank you for your succinct and timely recap on the powerful journey from the smearing of Kevin Shelley through to valiant Debra Bowen, elected for her determination to protect our elections from fraud and manipulations. In between came a sleazoid Arnie appointee, Bruce McPherson, who promptly certified any and all voting machines before his first day was over, who even had a Diebold staff member on his staff - he yanked

California open for dishonest elections. Sec. Bowen, long an advocate for election integrity as a legislator, has brightly shone light on the shadowed secrets of these infernal voting machines, upending all the smarmy false assurances and creepy apologists.

Will the registrars who took Bowen's precedent-setting decision as a personal affront please rethink their resistance and begin to deeply protect our voters, instead of currying cozy connections with the voting machine vendors. Registrar association spokesperson Stephen Weir virulently attacked Bowen right away. Perhaps his financial connections to the vendors should be investigated. Why would he so vociferously defend voting systems proven to be extremely vulnerable to hacking?

"Those who vote are not important. Only those who count the votes are important."

– Joseph Stalin

Log in | posted 08:44 pm on 08/06/2007

Jeanio (See profile | I'm a fan of Jeanio)

Those who hold Ms. Bowen's position in other states should follow her example. We don't need and should not accept election results from any state that cannot ensure that honesty will prevail.

Log in | posted 09:32 pm on 08/06/2007

PKSSK (See profile | I'm a fan of PKSSK)

Sounds like this women would make a good candidate for U.S. Senator of California. I don't think Feinstein is protecting your civil liberties and this women may be an alternative for 2008!!!

Food for thought!

Log in | posted 09:33 pm on 08/06/2007

bigirlsdontcry (See profile | I'm a fan of bigirlsdontcry)

Ms. Bowen for California Senator replacing Feinstein-- Brilliant!! We know Ms. Bowen has her principles at the fore. Bowen for California Senate! Spread the word!

Log in | Parent | posted 11:38 pm on 08/06/2007

cam (See profile | I'm a fan of cam)

Debra Bowen - well done.

With all the pressure, both left and right, it must have been a hard decision, but, speaking as an information professional, it was the right one.

Log in | posted 09:46 pm on 08/06/2007

Ms. Debra Bowen  
Secretary of State  
1500 11<sup>th</sup> Street  
Sacramento CA 95814

Dear Ms. Bowen:

*Thank you for decertifying the touch-screen voting machines and recertifying for only limited use. As one of a group who checked results of the machines in several voting places in San Diego, I am personally aware of machine problems and tapes inconsistent with results reported to San Diego election central. And that goes beyond the potential for hacking*

Sincerely yours,

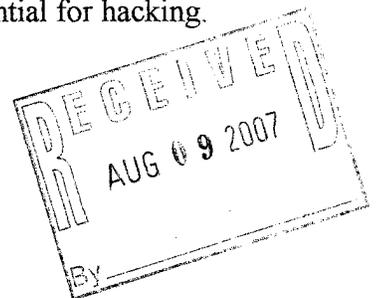
*Derek Staats*

Derek Staats

---

Typed version for ease of reading:

Thank you for decertifying the touch-screen voting machines and recertifying for only limited use. As one of a group who checked results of the machines in several voting places in San Diego, I am personally aware of machine problems and tapes inconsistent with results reported to San Diego election central. And that goes beyond the potential for hacking.



Ronald J. McMullin

Ms. Debra Bowen  
Secretary of State  
1500 11 St.  
Sacramento, CA.95814

Dear Ms. Bowen,

I want to commend and thank you for your recent decision regarding computerized voting machines.

You first came to my attention in a video used while teaching Business English to a Saudi Arabian business executive. We both were drawn to your professionalism as shown in presentations in the UCC communication materials.

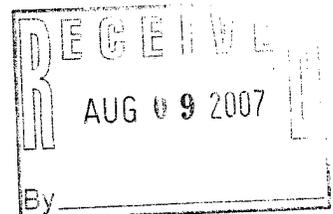
I have sent an article from the LA Times to him so he can appreciate your ethics in protecting the safety of our voting privilege.

Again, my thanks.

Sincerely,

Ronald J. McMullin

Ronald J. McMullin



8-4-07

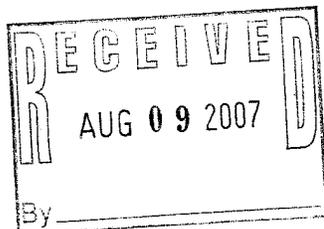
Dear Secretary of State  
Bowen,

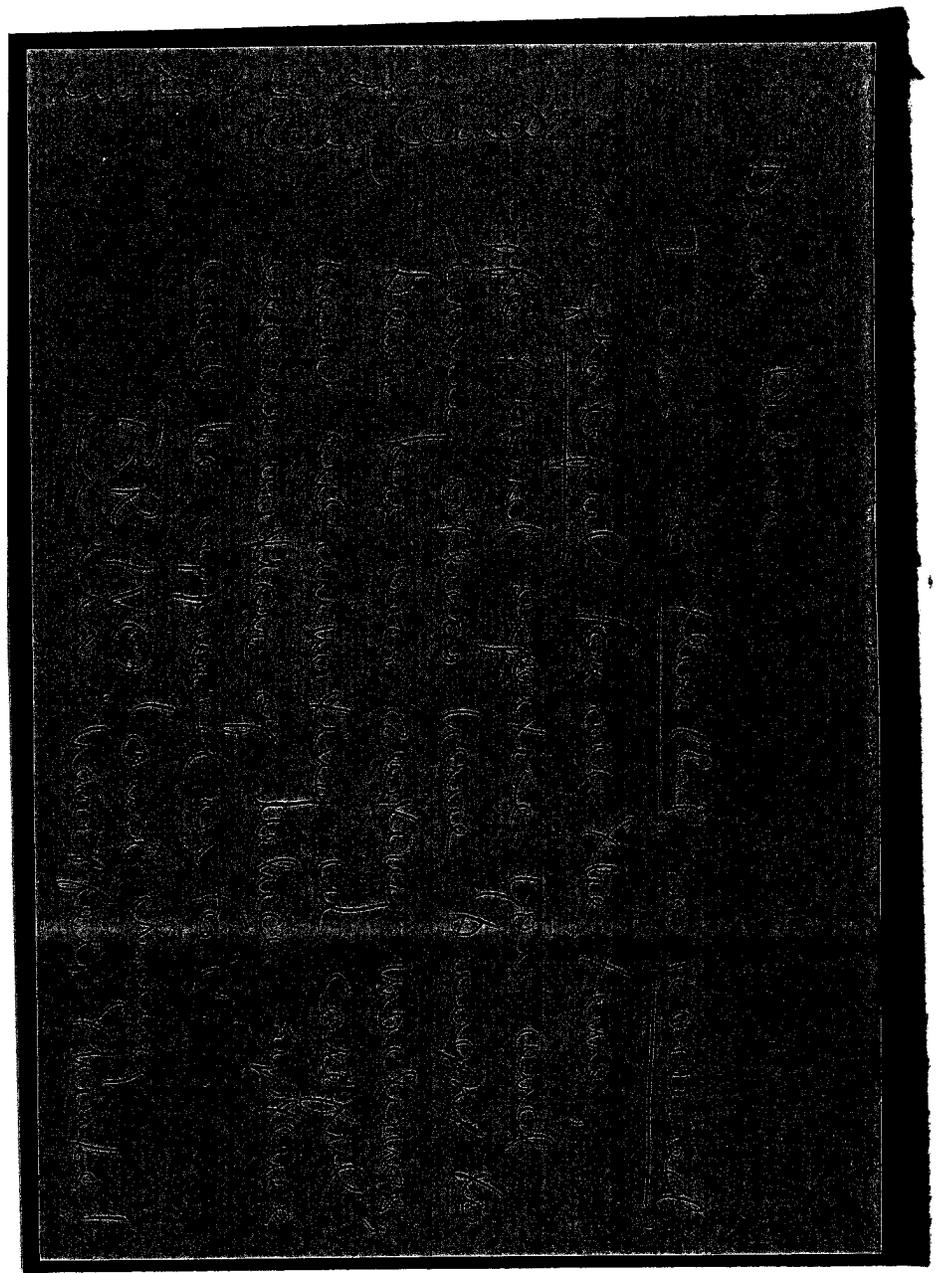
Thank you for decertifying  
the voting machines. You  
gave me a great birthday  
gift yesterday 😊.

I think your policy now  
is perfect! I can tell you  
how much I (we) appreciate  
all of your hard work and  
integrity on this issue.

Thank you, Thank you, Thank you!

Bethna Rausa

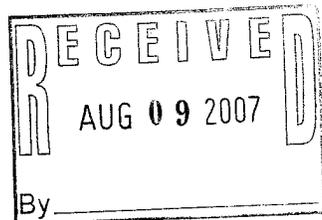




Aug. 6, 2007

Dear Secretary Bowen —

Thanks for keeping our voting machines honest. Can we get 50 of you around the nation?



Sincerely yours,  
Terry Carroll

Pacific Beach Bookkeeping

Debra Bowen  
California Secretary of State  
1500 11th Street  
Sacramento, California 95814

August 5, 2007

Madame Secretary of State:

You have recently done a most wonderful thing, by limiting the use of electronic voting machines to one per district in the State of California.

When people with whom I'm personally involved do something wonderful, I often say to them, "Go straight to heaven, and tell Saint Peter I sent you." I'd very much like to say the same to you.

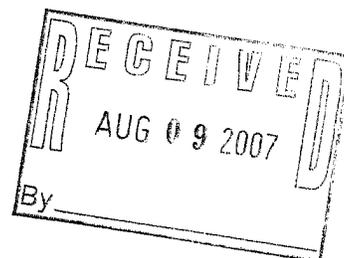
I am thoroughly impressed with your judgment, your integrity, your courage and your perspicacity.

Thank you so much for what you've done. It means everything to me and many others.

Wishing you a life full of many blessings,



Meredith Chace



August 06, 2007

Secretary of State  
Debra Bowen  
1500 11<sup>th</sup> Street  
Sacramento, CA 95814

Subject: Touch-Screen Voting Systems Decertification

Dear Ms. Bowen:

**Congratulations!**

Putting a hold on the use of touch-screen voting systems was probably a very tough decision for you to make, recognizing the substantial and competing implications.

**Background:**

My wife and I served as voting precinct workers in the November 2006 election, so we participated in the end-to-end process of education, setting up, operating, and tearing down the machines. Of course, before casting our own votes on the touch-screen machines we spent lots of time at home evaluating and filling out the sample (paper) ballot.

I regard the end-to-end process using touch-screen voting machines to be much too complex and too time-consuming, with lots of strictly-regulated steps for security and hardware safety purposes. Machines and software were not user friendly. We had to learn some "tricks" to get around quirks of the machines. The relationship between views on the sample (paper) ballot, the voting machine monitor during voting, the voting machine monitor during checking and the printer paper were frequently dissimilar. Lots of confusion.

The Good News: The people were great. The voters were patient and cooperative, with some having to wait in line at least 15 minutes, before even tackling the challenges of the voting machines and the really inefficient and cumbersome printers. We precinct workers even received compliments for our performance. I thought the precinct workers were very conscientious and helpful to the voters.

**My Plans:**

After experiencing touch-screen voting processes in the last two elections, I signed up for absentee ballots (paper) in the future. Since I have to fill out the paper ballot at home, just mailing it is a much easier step than adding the voting machine process.

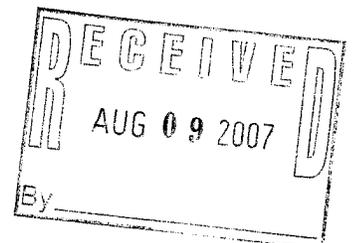
**Recommendation:**

Make mail-in paper ballots the baseline. Precinct stations could still handle the special cases, including Provisional Ballots.

Respectfully yours,

*Karl G. Reseck*

Karl G. Reseck



Linda Fowler

August 4, 2007

The Honorable Debra Bowen  
**California Secretary of State**  
1500 11th Street  
Sacramento, California 95814

Dear Ms. Bowen:

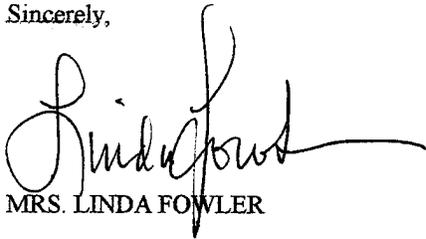
I am writing to congratulate you on your recent decision to decertify electronic voting machines in California.

I applaud your decision and commend you on the hard work it took to reveal the flaws in our voting system.

I am so happy I voted for you. I knew you would step up to the plate and do what is right for our state and our individual rights as American Citizens.

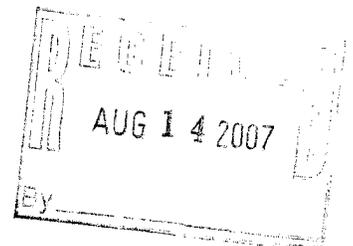
Woo Hoo, go get em girl. I am so very proud of you today.

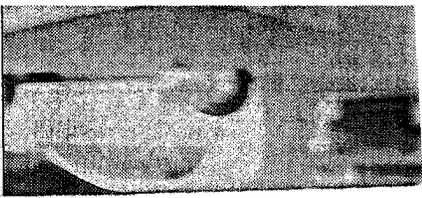
Sincerely,



MRS. LINDA FOWLER

LF





August 9, 2007

Debra Bowen  
Secretary of State  
1500 11<sup>th</sup> Street  
Sacramento, CA 95814

Dear Secretary Bowen:

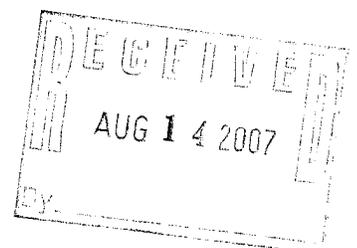
Enclosed is an article from the Fresno Bee about your recent decertification of the electronic voting machines in CA. This is to let you know that I and a lot of other people I know loudly applaud this decertification!! We are people who seek out alternative news information on KPFA and through progressive magazines. We have been greatly concerned about the 2008 presidential election, wondering what dirty tricks will happen at that time. In CA, at least we don't have to continue worrying about those "easily-manipulated to fraudulence" electronic voting machines. Thanks to you.

It is harder than usual to be an important government official just now. Thank you for your moral and efficient stand on this issue.

Sincerely yours,

*Diane Marks*

Diane Marks



Mark Bauman

8/4/07

Deborah Bowen  
CA Secretary of State

Ms. Bowen:

I VOTED FOR YOU BECAUSE YOU WERE PLEDGED TO GET RID OF CHEATING  
VIA RIGGED VOTING MACHINES....

NOW YOU'VE RECERTIFIED DIEBOLD?  
YOU ARE GIVING THESE CHEATERS A CHANCE TO REFORM THEMSELVES?

WHAT A LOAD OF CRAP!

THEY PLEDGED TO DELIVER VICTORY TO BUSH IN '04, THUS WE HAVE AN  
UNELECTED PRESIDENT RULING US....THEY HAVE CHEATED IN OTHER  
ELECTIONS....

DON'T TRUST THESE WEASELS.....

WHAT IS YOUR PROBLEM WITH FOLLOWING THROUGH ON YOUR PLEDGE  
TO GET RID OF THESE SCOUNDRELS?

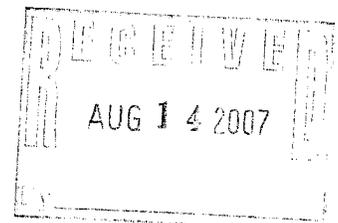
YOU ARE LETTING US DOWN!

GET ON IT, REVISIT YOUR HALF-ASSED DECISION...

I EXPECT A REAL RESPONSE FROM YOU...



Mark Bauman



Debra Bowen  
Calif Secretary of State  
P.O. Box 944225  
Sacramento CA 94244

8:30 PM Aug 5 2007

Enclosed news article interesting detail of Modern Times  
Modern Technology interesting to hear about.

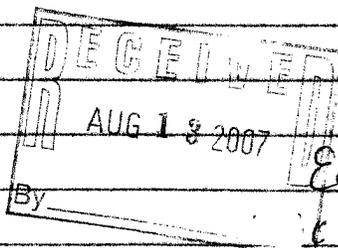
I got a little electronic Calculator with Trig functions in 1980<sup>±</sup>  
and it still works with just "solar" (electric light) panel recharge,  
It was remarkable then not to need Trig Tables.

I never got any of Modern Technology since then and  
am hoping everyone OK with working Compatibly with it all  
It's really future world

I hope solar panel costs come down so solar panels  
practical to power electric Cars (with bicycle wheels <sup>①</sup> 20<sup>±</sup> mph, local  
and Calif DMV approval. Braking recharge etc, Batteries ?? .....  
electric motor at each rear wheel ? ..... Transmission ? .....

Hope you have time to tell us a little about Modern Technology

① Two Bicycles  
Clamped Together  
about 4 feet apart



AHS 1936  
Edwin Wald CIT 1941

Some news 8.7-07

Dear Secretary of State Debra Bowen

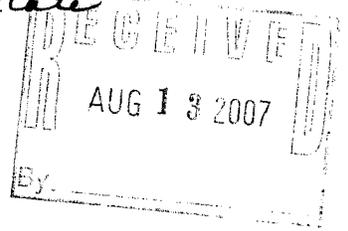
8/7/07

Thank you, Thank you,

Thank you for recognizing the  
many concerns regarding Veterans'  
Security. An important issue and  
you took a strong stand. Sincerely,  
Belma Carson

August 09, 2007

Hebra Bowen, Secretary of State  
1500 14th Street  
Sacramento Ca 95814



Dear Secretary Bowen,

I support and applaud your efforts to decertify electronic voting machines and noted for your position on this issue.

Repeated evidence of electronic machine irregularities has led to my belief that without a verifiable paper trail, there is no proof of the accuracy of the vote count.

Greater chaos ensues (Bee editorial, August 07) when the citizenry can no longer trust that all votes have been counted.

As an aside, that I now vote on an Absentee Ballot, even though I prefer going to the Polls, is only because of the paper trail it provides.

Again, thank you for your commitment and courage in defending

Sincerely,  
J

Guy Grunstein

August 4, 2007

Mrs. Debra Bowen  
**California Secretary of State**  
1500 11th Street  
Sacramento, California 95814

Dear S.O.S. Bowen,

Kudos and bravos and huzzahs and hurrays and for she's a jolly good woman, she's a jolly good woman....

Eternal respect and undying love is yours, from a dispirited populace, weary of losing fight after fight after fight..., that would have been won were politicians in general, as just, and honorable, and courageous, as you.

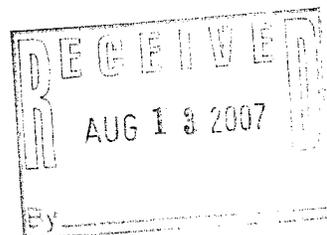
Of course I'm referring to your recent decision to decertify Diebold and Sequoia voting machines.

At the risk of being hyperbolic, it is sublimely ironic how the acronym for your office, is the exact same as the one for the international distress call; for maybe, just maybe, you more than perhaps anyone, will prove to be the lynchpin of the salvation and redemption, that our diseased once-great nation so sorely need.

Very truly yours,



Guy Grunstein



**From:** acapsis  
**Sent:** Tuesday, August 14, 2007 8:34 PM  
**To:** Voting Systems  
**Subject:** integrity in technology for government

Debra,

If we can elect a Bush once it can happen again!  
Im a programmer so I especially feel the need to set stringent standards,  
somebody's got to.

Athena Capsis

From: ljkrausen  
Sent: Tuesday, August 14, 2007 10:54 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

I worked the last elections - people were just making mistake after mistake on even the ink-blot machine because they were not being instructed well about how to put the paper in the slot. These are volunteers who are there for the money and some don't even speak english but no matter- the main thing is there is Such variation in the seriousness that people take the issue of instructing the voter on how to use the machine Several people I had to reinstruct, were wanting their vote to be for X and becausd they had the paper in slightly wrong- they actually were voting for Y. You can't make those mistakes with paper. Linda Krausen, superior court employee.

Ms. linda K

From: gigishames  
Sent: Thursday, August 09, 2007 5:08 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Let's keep the voting process as honest and decent as possible!

Ms. gigi shames

**From:** DivineChaos777  
**Sent:** Thursday, August 09, 2007 9:09 AM  
**To:** Voting Systems  
**Subject:** My Hero

Secretary of State Debra Bowen is a hero for taking steps to save our democracy while other politicians do nothing, caught like deer in the headlights.

Thank God for people like Bowen! Keep the faith, despite any squawking about costs and the like. If we can afford to spend some \$450 BILLION (to date) in Iraq, we can afford whatever it takes to keep our votes from being stolen!

Thank you!

Siddika Angle

From: mike  
Sent: Wednesday, August 08, 2007 4:13 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

I applaud our Secretary of State for holding to high standards regarding voting machines. Every caution must be taken to assure the integrity of the vote, without that, we have no voice, and no democracy.

Mr. Michael Diehl

From: james.davis25  
Sent: Wednesday, August 08, 2007 1:58 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Dr. James Davis

From: vaporfall  
Sent: Wednesday, August 08, 2007 3:51 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Flawed voting systems have caused way too many problems in the past and these upcoming elections are especially crucial to close every crack and loophole, whether the hackers end up being political operatives or regular citizens.

Mr. Gabe Shames

**From:** vic  
**Sent:** Wednesday, August 08, 2007 12:55 PM  
**To:** Voting Systems  
**Subject:** attn: Miguel Castillo

Miguel:

Here attached is a brief summary of the UBS study you allowed me to bring to your attention. It is a little dated. Last year it had been named the UPS study, and the bill number 550 referred to is the Holt Bill, which is now HR 811.

The virtue of this audit procedure, again (and for others you may wish to show this to) is that it reduces the risks associated with storing ballots out from the public view for any amount of time, where they may be tampered with or replaced so as to correspond to any fraudulent totals that may have resulted on an election day, through the use of electronic machines. Although unlikely, it could take tampering with only one precinct's votes in some cases to hide a fraud that could turn a local or state election, or potentially even a federal election, if such a precinct could be predetermined as large enough and having a race that is very closely contested. (Consider Ohio in 2004.)

Also as happened in Ohio this last election, elections officials were discovered to have tampered with ballots during the light of day and on their paid time, so as to manipulate totals and thereby avoid a full audit. So the will is there to tamper with ballots, if the opportunities are not prevented.

I would discourage the use of mail-in ballots as much as possible, as overnight storage of these is obviously unavoidable.

Your state has now successfully taken the lead in vigilance and protection against the potential hazards of electronic voting. It is only because you may now (hopefully) be viewed as the primary example to the rest of the nation on this issue that any possible vulnerabilities in your process become even more significant, if they in fact exist.

Again, congratulations to you all and particularly to your Secretary of State, Ms. Bowen.

Vic Bobnick

**September 7, 2006 --- For Immediate Release**

Attn: Political assignments

**AN END TO "FAITH-BASED" VOTING:**

**Computer Security and Statistical Analysts Describe a Simple and Powerful  
Alternative**

## **Summary**

Today the Election Defense Alliance released a report describing the practical implementation details of a simple, unimpeachable method for ensuring the accuracy of electronic voting systems by a public handcount of paper ballot records. This "Universal Precinct-Based Handcount Sample" (UPS) is a simple, feasible method of hand-counting a sample of paper ballot records in-precinct, on election night, by citizens themselves. It not only returns oversight of elections to the American people, where it rightfully belongs, the UPS is also far more accurate than alternative election audit proposals-where only a few percent of precincts are hand-counted, often in secret,

and always after the fact. (Download the full report at [www.electiondefensealliance.org/UPS.pdf](http://www.electiondefensealliance.org/UPS.pdf))

The simple, practical UPS validation approach detects fraud or error from any source altering the electronic tally by as little as one percent (1%) with a *minimum* ninety-nine percent (99%) level of confidence.

In our current political climate, any challenge to a corrupt election must be timely and have very strong justification, or candidates risk being labeled “sore losers” and accompanying ridicule. The UPS validation, by virtue of being accurate to such a high degree of confidence, enables *any* candidate of *any* party to contest *any* outcome-altering problems with the electronic tally. And since the UPS hand count is done in-precinct on election night, its findings would be available on election night, enabling candidates in federal or statewide elections to challenge a corrupted tally *before the election’s outcome becomes a foregone conclusion in the mind of the public, and before the results are officially certified.*

The report describes the specific means of effectively conducting a public hand count of 10% of the paper ballot records in 100% of the precincts in federal and statewide races. The UPS is to be conducted “in-precinct” on election night, by citizens representing all concerned political parties, and open to general public observation. Because it is conducted in-precinct, the UPS avoids the difficult task of protecting the chain of custody of paper ballot records in 180,000 U.S. precincts. In fact, all the alternative after-the-fact “spot-audit” schemes (such as HR 550, often referred to as the Holt bill) impose this monumental burden - since in all those protocols, all precincts must safeguard ballot records until just a few percent are “randomly chosen” some time after the election. Integrity of the chain of custody will be especially suspect, of course, in just those suspect elections which such audits are proposed to safeguard. Since a 10% hand-count sample would be drawn in 100% of precincts *on election night*, the UPS also eases the transition to decentralized, citizen-monitored hand-count verifications of elections, placing responsibility for the integrity of the vote count in the hands of the American people, where it rightfully belongs.

Most importantly, the UPS is inherently resistant to manipulation. The report describes how any attempt to systematically manipulate the UPS audit would be extraordinarily difficult to conduct and to conceal. Not only would it require a very large number of participants, any effort to skew the 10% paper hand count in favor of a candidate would be very likely to increase the overall discrepancy, not decrease it. The UPS provides a simple, effective, and vastly more powerful alternative for election validation than does the proposed HR 550 audit, and all such “spot-audit” proposals. The UPS provides a decentralized hand count, reduces chain of custody concerns and provides citizens and candidates a clear and timely warning of fraud or error. Therefore Election Defense Alliance recommends UPS as an alternative to the HR 550 audit.

In order to restore and maintain citizen trust in the integrity of American democracy, it is critical that wherever electronic vote tallying is performed, paper ballot records must always be produced and must always be checked by the best possible “security mechanism” - *the American people, working together in public.*

## **Background**

Despite credible reports of widespread error-prone programming and severe, inherent security vulnerabilities, millions of votes in America are now tallied by machines that lack any

independent means of verifying that they tallied the vote accurately. Even where such means exist, they are most often not employed, or not employed properly.

In response to this unacceptable risk, Rep. Rush Holt (D-NJ) recently re-introduced HR 550, “The Voter Confidence and Increased Accessibility Act of 2005”-a pending bill to require creation and auditing of a fraction of the paper record of all electronic votes cast in federal elections. According to Representative Holt, HR 550 has received “bipartisan endorsement from one-third of the members of the House of Representatives, and has been endorsed by good-government groups as the ‘gold standard’ in [election] verifiability legislation.”

A study released August 16, 2006, sponsored by the Election Defense Alliance, revealed that, despite its good intentions, the proposed election audit mechanism in HR 550 - far from protecting America’s elections - would in practice actually leave the US House of Representatives elections wide open to undetected programming error or deliberate fraud. The problems with HR 550 are so fundamental they cannot be remedied simply by auditing more precincts.

## About the authors

**Bruce O’Dell, Coordinator of Data Analysis, Election Defense Alliance.** O’Dell is an information technology consultant with 25 years experience who applies his expertise to analysis of the technical security and integrity of voting systems. His current consulting practice centers on e-Commerce security and the performance and design of very large-scale computer systems for Fortune 100 clients - recently as the chief technical architect in a company-wide security project at one of the top twenty public companies in America. ([http://www.digitalagility.com/Odell\\_home\\_page.htm](http://www.digitalagility.com/Odell_home_page.htm)).

**Jonathan Simon, JD, co-founder of the Election Defense Alliance.** Simon is a graduate of Harvard College and New York University School of Law and is a member of the Bar of Massachusetts. He applies his prior experience as a political survey research analyst for Peter D. Hart Research Associates to studies of the accuracy of exit polls and other election integrity mechanisms. He has collaborated on several studies assessing the accuracy of the 2004 presidential exit polls. (<http://www.electiondefensealliance.org/jonathansimon>.)

## About Election Defense Alliance

Election Defense Alliance (<http://www.electiondefensealliance.org>), founded July 4, 2006, is a coalition of election integrity activists working at the state and local levels across the nation to detect and counter covert, antidemocratic manipulation of voter registration databases and all electronic voting systems; to regain public control of the voting process in the United States; and to insure that the process is honest, transparent, secure, subject to unambiguous verification, and worthy of the public trust.

\_From: Brina-Rae Schuchman  
Sent: Monday, August 06, 2007 10:51 PM  
To: Voting Systems  
Subject: Re: Bowen

To: CA Secretary of State Bowen

Dear Secretary Bowen,

Thank you for your courage and persistence and leadership in having the voting computers tested.

I am still concerned about how our votes will be counted. If RoV's such as Deborah Seiler are allowed to use any secretive proprietary scanners or the Central Tabulator, whether Diebold, which is all we have in San Diego, or any other of the big 4, I would call that an election killer. Even with open source, we still can never be sure someone didn't meddle.

I think whenever election integrity advocates or voters meet with RoVs such as Seiler or the Press, we should be telling them we do not want to use scanners or the Central Tabulator or any computerized machine.

I personally believe that the 4 vendors' machines were never right for elections and that they committed consumer fraud upon the taxpayers by pushing those machines on election officials and the voters.

RoVs need to advertise and do Press Conferences and email for volunteers so there are people of all parties to hand count votes and watch the counting, in the evening at each precinct after the Polls close.

We should also be asking the Media to stop playing "gotcha" with our elections. Everyone should let the votes be counted the first night and let the RoVs report real totals by the end of the next day or the next if necessary.

This is, after all, the most important work of citizenry. It needs more respect.

We want first counts to be as complete as possible when they are reported. We don't want to have to rely on second counts, audits and recounts, except to verify that every vote has been counted as cast. Check and double-check. "Trust but verify".

It would make sense for each person, volunteer or stipend- paid, who is vote- counting or pollworking, to be vetted in some ways so they are known and asked to sign an agreement that they agree to be non-partisan while doing election work as well as to show a photo I.D. and attend a certain number of hours of training. A curriculum could be developed to be available and

Sec. Bowen, you and your staff are REALLY making a difference. You

are leading the fight to defend our country, democracy in America and the government of the United States, in a unique and vital way, and we applaud you and urge you to keep your Eyes on the Prize, and soldier on. You are REALLY saving our country. We are with you.

Sincerely,  
With Gratitude,  
Brina-Rae Schuchman  
Chair, TrueVoteSanDiego; Member EI task forces- CEPN, SAE, PDA Metro, CA50, others

**From:** Chuck Lowery  
**Sent:** Tuesday, August 07, 2007 3:13 PM  
**To:** Voting Systems  
**Subject:** Congratulations (& a personal message)

THANK YOU, Secretary Bowen, for doing exactly what you promised the voters in your November speech here at Pacific Bakery in Oceanside.

If our other elected Democrat representatives would implement our wishes like you have done, our entire nation would be in a much stronger and safer position.

You can count on me to personally and financially help your re-election campaign. Please add me to your list of future campaign supporters.

Sincerely,

Chuck Lowery  
President  
Pacific Bakery Inc.  
...a California corporation

**From:** Karen Bowling  
**Sent:** Tuesday, August 07, 2007 2:54 PM  
**To:** Voting Systems  
**Subject:** Congratulations!

After spending 7 years studying elections around the country via Bev Harris and Bradblog, I can only say hooray. Private businesses have no right to control, run, count, have voting lists, or do anything that involves our election process. For the state of Ohio to rely for tallying the critical results of the last presidential election to rely on software written by people funded by the RNC and run through computers in the basement of their offices straight to the office of Ken Blackwell leads any reasonable person to assume that the election was stolen. Isn't it nice to know, as we have discovered in the last few days, that those very votes which were ordered not to be destroyed, have been destroyed. The fraud that went on in Ohio with suppression of vote, caged voting lists, too few machines for minority areas, exit polls changing wildly late in the evening, vote totals changing that did not reflect what was printed out earlier in the evening, etc. was enough to sicken every American. I am nauseated by the way we rushed into the Ukraine to make sure they got a vote over and here in our country we have a completely dishonest and fraudulent system that our main stream media and the even the Democratic Party refuses to tell

the American people about. Howard Dean is making some noise that they are going to start looking into every single precinct in the country and that is what it will take as the Republicans have manipulated the system in literally hundreds of ways from crooked U.S. Attorneys to hacked machines and each of those all added together have enabled the Republicans to steal elections since 2000. I am so glad that I spent time working on your campaign and touting you to everyone that I could. Please help us here in San Diego --- Seiler, Vu, Townsend -- more suspect elections coming our way! Even as Seiler announced more absentee balloting, I want someone looking at how those votes are counted. I don't trust the Republican party here in San Diego as they were very suspect in the Donna Frye-Jerry Sanders Mayor race and especially in the Bilbray-Busby elections. Phony auditing in the ROV office, absentee ballots mixed in with other precincts and many never counted. We have serious problems here. Help!!

Karen Bowling

**From:** laurel granquist  
**Sent:** Tuesday, August 07, 2007 2:25 PM  
**To:** Voting Systems  
**Subject:** Deborah Bowen

THANK YOU FOR YOUR EFFORTS TO PROTECT  
OUR VOTE  
Laurel Granquist

From: Carol Benak RN MFCC  
Sent: Tuesday, August 07, 2007 9:45 PM  
To: Voting Systems  
Subject: Decertification

Dear Ms. Bowen,  
I want to thank you for decertifying Diebold and Sequoia machines. It was the best news that I received this week. It seems that California is in the lead for this and I hope other states will follow. Carol

From: Judith S Offer  
Sent: Tuesday, August 07, 2007 7:24 AM  
To: Voting Systems  
Cc: cguttman@verizon.net  
Subject: Decertification of Machines

Hello Secretary Bowen:  
In my opinion there is no real necessity for voting machines at all. This has been brought upon by the machines' manufacturers, and there is no reason we have to know all these decisions immediately. The people don't take office immediately.

Essentially these machines are expensive pieces of junk. Turn them all down.

Judith Offer

**From:** Mfbodine@cs.com  
**Sent:** Wednesday, August 08, 2007 10:40 AM  
**To:** Voting Systems  
**Subject:** ## CRITICAL ## re: Decertification of Diebold vote system

To the Office of Secretary of State:

This is a followup to a phone call to your office today.  
This matter requires your immediate attention.

I have studied the August 3rd, 2007 proclamation of Debra Bowen decertifying the Diebold voting systems. There appears to be either an error in her conditional recertification OR she has intentionally, and completely, decertified the Diebold AccuVote-OS optical scanning machine.

In the paragraphs immediately below the "Whereas" clauses, the Secretary explicitly withdraws the certification of the Diebold products listed, "EXCEPT AS SPECIFICALLY PROVIDED BELOW."

Here's the problem:

In the balance of the document, it appears the Secretary makes NO mention regarding any OTHER Diebold product beyond the AccuVote-TSX.

In other words, it appears the Secretary has withdrawn the certification for ALL Diebold products listed EXCEPT for the TSX (touchscreen) model, which can be used conditionally, per the requirements and procedures cited.

Please clarify this very important point regarding the Secretary's decertification.

Regards,

Mike Bodine

**From:** Raquel Brac  
**Sent:** Wednesday, August 08, 2007 9:12 AM  
**To:** Voting Systems  
**Subject:** Decertification of Voting Machines

Thank you for your courage in decertifying our voting machines. You will get much heat from those with a high stake in corporate control of this vital system. The people, however, applaud you for protecting our right to vote, and have it count.

Sincerely,  
Raquel Brac

**From:** Patrice Wahlstrom  
**Sent:** Wednesday, August 08, 2007 11:51 AM  
**To:** Voting Systems  
**Subject:** decertifying machines

I just wanted to say, 'thank you' to our new Secretary of State for continuing to support the principles she stood for when running for office. It was such a huge move to decertify the electronic machines, which we all know can be hacked in attempts to rearrange our votes.

I want to stay informed and participate in any way to help with this issue of preserving the integrity of our vote.

thank you  
sincerely,  
-Patrice Wahlstrom

**From:** Barbara Jenkins  
**Sent:** Wednesday, August 08, 2007 10:16 AM  
**To:** Voting Systems  
**Subject:** Red Team Review

Thank you for doing the Red Team Review. We want paper ballots again. Forget about the voting machines. They all seem to be corrupt in that no one will go with the paper trail.

Barbara Jenkins

From: pamholt  
Sent: Tuesday, August 07, 2007 9:32 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Please see HBO documentary, "Hacking Democracy" and see <http://www.blackboxvoting.org/>

It is so frightening to think along with losing our constitution, that we are also losing our democracy.

Mr. Pam Holt

From: worksalot2  
Sent: Tuesday, August 07, 2007 9:29 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Citizens of nearly every political stripe generally hold in common the view that encouraging and facilitating broad voter participation in the electoral process are vital to a vibrant democracy. Yet, unreliable election systems erode public trust in the electoral process and can discourage many potential voters from actually going to the polls. Therefore, I applaud your efforts to investigate the Diebold, Sequioa, and Hart Intercivic electronic voting systems now in use throughout California. Ms. Bowen, your "Red Team" has reported serious flaws in each of the systems it evaluated, thereby joining a growing list of critics who have expressed alarming concerns about the reliability of virtually every electronic voting system now in use in this state. Even so, those reports still vastly understate the scope of the risks posed by those systems. For I share the view of BlackBoxVoting.org that, even if all the problems identified in those reports are fully resolved, each rev!

iew only partially examines the risks of inside manipulation with these systems. Procedural remedies can be circumvented by those with some level of inside access -- of whom there are many and that the most high risk scenario of all is that of inside manipulation. I, therefore urge you to decertify, without further delay, all of the electronic voting systems in use in the State of California unless and until every one of the issues that has been identified therein which places the integrity of out electoral process, thus our very democracy, at so substantial a risk.

Ms. Joanne Gifford

From: gmd  
Sent: Tuesday, August 07, 2007 9:26 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Regarding the voting machines, I concur with the analysis and conclusions well expressed in an earlier letter to you from Paul R. Lehto, Juris Doctor, a copy of which can be read at:

[http://www.opednews.com/articles/opedne\\_paul\\_leh\\_070801\\_why\\_all\\_california\\_s.htm](http://www.opednews.com/articles/opedne_paul_leh_070801_why_all_california_s.htm)

So, please, let's keep it simple... if it ain't broke, don't fix it! Let's go back to using paper ballots. Does something prevent us from utilizing the most direct, secure and least expensive method and means to tally our votes? What? Everyone I know, in every walk of life, wants, needs and desires that we return to paper ballots.

Attempting to secure the voting machines long ago seemed too futile for any reasonable person to continue and now that the computer professionals, hackers/crackers, have proven them to be vulnerable, it is in our best interest to cease throwing good money after bad

projects, cut our losses and return to the paper ballots. They leave a paper trail and the people have confidence in them!

Ms. Gwen Dillon

From: gregstrausbaugh  
Sent: Tuesday, August 07, 2007 9:24 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

The California Secretary Of State Needs to hold the Vote Machine Companies accountable.

Last week, the results came in from California's top-to-bottom "Red Team" review of the four major vote machines used in our state.

In short, a crack team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES S.

Election fraud is a crime. The FBI should investigate if any criminal wrongdoing has occurred and prosecute those responsible.

One option for future voters is to have a numbered identifier paper receipt issued to the voter. Then each voter can go online to a secured government website and compare the online results of their vote to those generated by the voting device.

If there is a discrepancy, the voter should be able to call or record online their actual vote information. This could assist in determining if a crime may have occurred due to the Vote Machines manipulation.

Mr. Gregory Strausbaugh

From: mretc  
Sent: Tuesday, August 07, 2007 9:18 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

It is time to hold voting machine companies accountable. California Secretary of State Debra Bowen should immediatly decertify the Hackable Voting Machines.

Last week, the results came in from California's top-to-bottom "Red Team" review of the four major vote machines used in our state.

In short, a crack team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES  
S. <http://www.bradblog.com/?p>

Mr. Ed Collins

From: conlyhelen  
Sent: Tuesday, August 07, 2007 9:17 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

VOTE BLUE CENTRAL COAST  
A Political Action Committee

July 30, 2007

As VOTE BLUE CENTRAL COAST our purpose is to engage and register voters across Ventura, Santa Barbara and San Luis Obispo Counties. Our concern is that today there are 131,141 eligible citizens in Ventura County who are not registered to vote, in Santa Barbara County there are 87,395 of eligible nonvoters, particularly in the northern part of the County and in San Luis Obispo there are 34,457 eligible, but not registered to vote. \* (Report of Registration 2/10/2007, [www.sos.ca.gov/elections/elections\\_u.htm](http://www.sos.ca.gov/elections/elections_u.htm))

How can we register, engage and educate these new voters when there are serious questions about the security and integrity of electronic voting systems and particularly about Diebold and Sequoia Systems? We need to know what safeguard the County Registrar of Voters in Ventura, Santa Barbara and San Luis Obispo will use to assure us and all citizens. Two days ago in the LA Times Secretary of State Debra Bowen said. Our very existence as a democracy is dependent on our having voting systems that are secure, reliable and accurate. We ask to be part of a discussion and oversight process to assure integrity of election systems for all voters regardless of political party affiliation.

These are the questions for you as County officials:

Have you read and addressed the top to bottom review which is the subject of a hearing in Sacramento with the Secretary of State this morning?

What do you think of the problems as stated in the Red Team Reports for your systems?

#61656, Physical security of equipment

#61656, Possibility of insider tampering

#61656, Training for inspectors at polling stations

#61656, Specific security layers with electronic systems software, firmware tampering, recording of vote, tabulation and reporting of vote.

#61656, Are you in contact with Diebold or Sequoia vendor and are they helping solve these issues? (We know they were less than helpful with issue of PDF SOV formatting to the Counties and public.)

#61656, What policies and procedures can you suggest to address these problems?

#61656, Can we help you to do this by calling a Press Conference that addresses all these issues before Aug 3th the date the certification process or suggestion for procedures are due? We will lobby on your behalf because we have contact with concerned citizens who want to support their local officials.

Contact: Sue Broidy, Chairperson 805 640-7349  
Helen Conly, Treasurer 805 746-0199  
Heather Schmidt, Staff 805 340-4642

We are a California grassroots organization whose purpose is to engage and register Democratic voters, to create a powerful data base with local voter information, to deliver electronic and printed materials to educate voters, to develop media tools for organizing, to provide leadership training for local activists, and to engage the community about progressive issues.

Ms. helen conly

From: egnosis  
Sent: Tuesday, August 07, 2007 8:59 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

All the machines evaluated were hackable (<http://www.bradblog.com/?p>)

Mr. Eric Garcia

From: mlserna  
Sent: Tuesday, August 07, 2007 8:58 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Please vote to decertify these corrupt voting machines.  
This is an outrage and why we have been stuck with this disgraceful administration who is shredding the constitution.  
We must make voting a honest and fair system that is un-hackable.

Thank you-  
mlserna@aol.com

Ms. marcia loots-serna

From: tog18  
Sent: Tuesday, August 07, 2007 8:57 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Please decertify the hackable voting machines.

Toni Gilmont

From: maiapeter  
Sent: Tuesday, August 07, 2007 9:00 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Tell The California Secretary Of State To Hold The Vote Machine Companies Accountable

Last week, the results came in from California's top-to-bottom "Red Team" review of the four major vote machines used in our state.

In short, a crack team of computer scientists and professionals found massive security flaws in all the machines tested from Diebold, Sequoia, Hart, and ES S.

EMAIL CA SECRETARY OF STATE: <http://www.usalone.com/pnum688.php>

Debra Bowen, the California Secretary of State now has to make a decision about what to do about all these machines . . . and fast. Does she decertify them, conditionally recertify them if the problems are fixed, or come up with some other solution. She has asked for public comment through the end of the day today, Wednesday, August 1st. This form will sent an email directly to [VotingSystems.ca.gov](mailto:VotingSystems.ca.gov)

Obviously, the machine vendors a extremely opposed to the review results and any action by the SOS, and they are trying hard to lobby against these. So we need to let the Debra Bowen that we have her back when she makes the tough decision she must, and that decision could come as early as Friday, August 3.

So please, send SOS Bowen a little note thanking her for conducting the "Red-Team" review, and tell her what you want her to do with the vote machines that do not meet reasonable security standards. Send a your note before the end of business today. Thanks from the VR team.

Please take action NOW, so we can win all victories that are supposed to be ours, and forward this message to everyone else you know.

If you would like to get alerts like these, you can do so at <http://www.usalone.com/in.htm>

Or if you want to cease receiving our messages, just use the function at <http://www.usalone.com/out.htm>

usalone99:20386

Powered by The People's Email Network Copyright 2007, Patent pending,  
All rights reserved

Ms. maia peter

From: amichaan  
Sent: Tuesday, August 07, 2007 9:00 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Dear Secretary of State Bowen:

Thank you for having the courage to begin the process to expose the dirty secret that is known to the whole world but has been kept from the American people: America's elections are rigged! The evidence is overwhelming that the most basic cornerstone of our freedom, the right to choose representative government, has been hopelessly corrupted by the onslaught of secret source code, privately owned, highly partisan influenced, "voting" devices.

Prior to the introduction of these computers and scanners to our elections exit polls were almost always dead on accurate, amazing "upset victories" were almost unheard of and we the people had faith and trust in the integrity of our elections. This is no longer the case. The evidence is overwhelming that there are many elected offices in our nation at every level that are being occupied by "elected officials" that were NOT chosen by the voters. This fraud is nothing less than treason! This scandal is brought to us by secret unverified vote counting made possible by the very same devices that you have just tested and shown to be so devoid of security. In fact the greatest danger is not from the outside hacker but rather from the inside owners of this technology. The president of Diebold publicly promised George Bush a win in Ohio prior to the 2004 election. Obviously he felt confident in making such an assertion since his equipment was in almost every polling place in th!

at state. All evidence points to a massive fraud having occurred there in the 2004 election!

I am the owner of the Grand Lake Theater in Oakland and have been waging my own campaign on this subject since the Supreme court stopped the counting of votes in Florida in 2000. Please look at some of the statements I have made on my marquee (seen by 50,000 people a day) at:  
[www.flickr.com/photos/grand-lake](http://www.flickr.com/photos/grand-lake)

I have taken this highly public stand and endured much ridicule and criticism (as well as loss of customers) because I believe passionately that the single most important element in our democracy is free and fair elections. Without that we have no freedom and the American experiment in democracy created by the signing of the Constitution over two centuries ago will have been extinguished by ruthless and corrupt partisans that are comfortable with ignoring the will of the American people.

I beg of you, PLEASE be the patriot that rescues our freedom by DECERTIFYING all electronic voting devices that do not have absolute transparency. Optical scanning tabulators are just as dangerous and prone to manipulation as are computer "DREs".

We can have absolute honest elections by having A full paper ballot system HAND COUNTED with monitors from any interested party observing the counting. Recounts should be automatic and free of charge in any challenge of the results.

We conducted our elections this way for two centuries! It is more important to have real and verifiable results than quick results. This is our right as citizens and this right has been stolen from us.

Ms. Bowen you now have the opportunity to sieze the moment and become a giant in the history of American patriots! You hold in your hands the power and the means to blow the lid of secrecy off of our national disgrace and bring the obsenity of mechanically stolen elections into the light of scrutiny by an unawre public.

I urge you to order a return to an all paper ballot system and to restore REAL elections to the Citizens of our state.

Allen Michaan

From: d.ericson  
Sent: Tuesday, August 07, 2007 8:59 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Thanks to SOS Debra Bowen for conducting the "Red-Team" reviews of voting machines.

Although a shorter version was submitted earlier via <http://www.usalone.com/pnum688.php>, the original document was too long to submit via that link. The following is Part 1 (of4):

Verifiable Voting Machine Election System, Part 1 (of 4)

by D.W. Ericson  
(2006 Nov 28)

#### INTRODUCTION

If a voter could find/view his Voter Record on a final Precinct Printout posted, either in the local paper(s), and/or outside the Local Precinct door (soon after the precinct closed), we would have Verifiable Voting at the precinct level.

This is easily expanded to higher levels, by posting totals in the corresponding newspapers, as normally done after elections.

Such Verifiable Voting is easily accomplished by assigning a (private) random Voter Number to each voter, and printing all Voter Records, sorted by this Voter Number, thus allowing voters to easily verify their votes and also the Precinct Totals (soon after the precinct closes).

Subsequently, the voter could also, easily verify the County Totals, State Totals, and the Federal Totals by simply verifying the corresponding totals in their local press (or on the internet).

IMPLEMENTATION

Each County Precinct would require a Mini-Computer to generate random numbers for precinct Voting Machine as they request them for assignment to voters. As the vote is cast, the Voting Machine (Software) should post the Voter Number with a reminder that it remembered, so this Voter Record can be located on the final Precinct Printout to will be posted outside the Precinct's door.

This Mini-Computer is to be connected to the local intra net serving only the Precinct's local Voting Machines, and is not to be connected (for uploading voter data) until after the final Precinct Printout has been posted outside the Precinct's door.

All voting data summations are to be provided by the responsible government agencies, not any private concern/corporation.

Mr. Donald W. Ericson

From: jparsons  
Sent: Tuesday, August 07, 2007 8:58 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

You need look no further than the news yesterday about the 2004 ballots in Ohio being destroyed in VIOLATION OF FEDERAL LAW  
(<http://www.alternet.org/story/58328/?page>)

Mr. John Parsons

From: dfwells  
Sent: Tuesday, August 07, 2007 8:56 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

<http://www.dansdiatribes.com/diatribes/tenFootPoll.htm>

Mr. Daniel Wells

From: francenel  
Sent: Tuesday, August 07, 2007 11:50 PM  
To: Voting Systems  
Subject: paper ballots

Dear Ms. Bowen,

Thank you for taking the initiative to have paper ballots. The Republican's have NO boundries. If it were my party, I would be ashamed.

If you need me please contact me at, francenel@cox.net.  
Thank you.

Francene Blanchard

From: jimandmara  
Sent: Tuesday, August 07, 2007 2:58 PM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Why would anybody not want honest and verifiable election machines?  
Anybody who wants anything else is up to no good.

Mr. James Thompson

From: terryolson  
Sent: Tuesday, August 07, 2007 9:02 PM  
To: Voting Systems  
Subject: Fantastic Work!

Ms. Bowen,

You are a true patriot, and I thank you for your action in getting paper ballots in place. The rest of the country is watching, and hopefully by election '08, the whole country will be using paper.

Is there any chance that we will be giving our electoral votes by district? I hope not.

Sincerely,

Terry Olson

**From:** V.E. Lane  
**Sent:** Tuesday, August 07, 2007 8:56 PM  
**To:** Voting Systems  
**Subject:** PLEASE DEFEND OUR DEMOCRACY WITH HCPB

Dear Secretary Bowen:

We commend you for your dedication to telling the truth.

Why have you failed to hold the Vendors accountable?

They have lied to us. Their false advertising and denial of the vulnerabilities which have exposed our elections to monumental fraud is deplorable. You hold the key to returning the power of holding truly democratic elections back to the people. Please let the people count paper ballots at the precincts!

The vendors and our legislators have no liability and will not be punished for their treasonous disregard of our Constitutional rights. All of the Vendors have misrepresented their goods. They should all go to jail. The federal Independent Testing Authority is a sham. Cyber tested our Sequoia equipment, why should we have faith in a system of

testing which has been shown to have no integrity? The Vendors do not deserve a second chance. When elections can be altered without leaving any evidence you must not rely on the people to prove something which is impossible to do. There is no way we can be the watchdogs.

The National Institute of Standards and Technology can not devise a test to prove the accuracy of these machines. The county tests are a meaning less charade. In the Conclusion and Postscript of the Sequoia Source code review your Red Team tells you and us that we must not be fooled into relying on mitigating security strategies to protect our vote.

SB1487 creates a federal oversight rule that ALL International and Domestic ELECTION OBSERVERS must be "ACCREDITED BY THE ELECTION ASSISTANCE COMMISSION". We have no idea what these standards are. DO YOU? Both HR 811 and SB14487 are extremely dangerous bills, The EAC, appointed by the president has powers to ELIMINATE ALL MEANINGFUL PUBLIC OVERSIGHT which presently is just a joke. Your across the board final de-certification of ALL the equipment tested is critical to the restoration of democratic elections. The Vendors knew of these giant holes in their system security.

Your actions must uphold the power of the people. The world is watching.

SAVElections Monterey County has called for the removal of our Sequoia DRE and OP/SCAN tabulators. It is virtually impossible for us to provide any meaningful oversight of this equipment. There is no other group in sight (Rep-Dems, etc.) on election night or during the 1 % bullshit audit all through the canvas. People who are calling for open source should wake up to the fact that the county clerks have shown their allegiance to the vendors by not supporting you at the hearing on the 30th. In my opinion only Oakley in Yolo county is a representative of the people.

In Nov. 2006, I watched one county employee process thousands of paper ballots into the OP/SCAN tabulators without any oversight. My cries were silenced with the admonition that he had "taken the oath and was under video surveillance." Our new registrar, Linda Tulett, replaced Tony Anchundo who has just been released from jail. She refused to post poll closing tapes from our DRE's in June "saying it was not possible and an archaic law." Our demand for a sign to advise voters of their right to a paper ballot was denied. She refused to have incident reports written at the precincts, all problems would be written up by her.

We are not gullible enough to TRUST anyone with access to our machines. It is insider fraud that the red team cautions us against in their source code conclusion and Postscript.

The audits proposed by your review team in July are an insult to our intelligence. The op/scan tabulators are just as susceptible to insider fraud as the touchscreen DRE's. How can you believe that our election officials should audit themselves. Would Tony Anchundo have turned himself in?

To even propose that election officials from other counties audit one another is also ludicrous. So maybe we should pay an "independent" audit team to come in. WRONG!!!!!!!!!!!!!!!!!!!!

We have been stonewalled by our BOS with our request for a public hearing to air our concerns.

It is virtually impossible for us to provide any meaningful oversight of our machines. Those who support using OP/SCAN should come to Mo Co and watch what passes as a democratic election. Our elections have been privatized. How can you fail to recognize that we do not have a democracy without the people to provide the checks and balances?

People who are fighting for democratic elections should put the task of counting back in the people's hands and admit that OP/SCAN tabulating is counting our votes behind closed doors. Only then will we have a glimmer of hope that we will have accurate election outcomes.

**PLEASE, PLEASE HEAR OUR PLEA. WE ELECTED YOU TO DEFEND OUR DEMOCRACY!**

Thank you for your consideration, I am representing thousands of voters who are counting on you to protect our votes.

Valerie Lane

**From:** Roland

**Sent:** Wednesday, August 01, 2007 9:03 PM

**To:** Voting Systems

**Subject:** Election Fraud

Dear Debra Bowen, Secretary of State

I very much appreciate your Red Team Review of electronic voting machines. Based on the results to date, I'm requesting that not only should the failed vendors' equipment be decertified but that they be prohibited from future contract bidding. At the very least, the CEOs and the Chairpersons of the Board for each of these corporations should be required to sign a notarized perjury clause stating that their machines cannot be hacked in any significant way and should it turn out that during the election process that the machines were in fact hacked system-wide, that there would be imposed liquidated damages amounting to the cost of conducting another election with a substantial portion be taken directly from the personal funds of these corporate officers.

These corporations have been interfering with the election process since before the year 2000. Obviously, this represents a severe threat to our system of government. Here we are seven years after Congress passed legislation to rectify the situation and we still need election observers as though we were a third world country. Time is running out - the critical 2008 election is just around the corner on the bureaucratic time scale.

Thank you for your past, present and future patriotic efforts to ensure that, We the People, can have confidence in the outcomes of our elections.

Respectfully submitted,  
Roland Swirsky

**From:** Jim Dooley [mailto:jimfdooley@gmail.com]  
**Sent:** Tuesday, August 07, 2007 7:16 PM  
**To:** Voting Systems  
**Subject:** DRE machines

Thank you for keeping our elections secure. If I were not traveling and using a lap top I would say more.

Jim Dooley

**From:** Ellen H. Brodsky  
**Sent:** Wednesday, August 15, 2007 3:31 PM  
**To:** Ellen Brodsky  
**Subject:** VOTER ACTION CALLS FOR A FULL CONGRESSIONAL INVESTIGATION OF VOTING SYSTEMS COMPANIES

### **VOTER ACTION CALLS FOR A FULL CONGRESSIONAL INVESTIGATION OF VOTING SYSTEMS COMPANIES**

Last night's broadcast by Dan Rather Reports of "The Trouble with Touch Screens" raises serious questions as to whether US voting systems companies have engaged in commercial fraud by knowingly marketing defective products to jurisdictions throughout the country. It also serves as a wake-up call to the nation of the dangers associated with the outsourcing of key election functions to private vendors. Voter Action today calls on the United States Congress to launch a full investigation into the increasing influence and control that private companies wage in the way we conduct our elections and to determine whether certain US voting systems companies have committed crimes under federal and state anti-fraud statutes which should be referred to the appropriate authorities for prosecution.

<http://www.voteraction.org/>

Watch the whole one-hour program

Read the complete statement

<http://www.voteraction.org/release.html>

Sign the petition

<http://salsa.democracynaction.org/o/2671/campaign.jsp?campaignKEY= 12354>

--

John Gideon

From: nataliemcl  
Sent: Tuesday, August 07, 2007 11:07 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

What's wrong with hand-counted ballots? It seems to work fine in many other countries and doesn't seem to take any longer than fiddling with these ridiculous machines. Take the profit out of our most precious access to Democracy.

Ms. Natalie Cortez

From: D'Ann Paton  
Sent: Tuesday, August 07, 2007 6:40 PM  
To: Voting Systems  
Subject: SD voter

Thank you for trying to keep our votes honest. I applaud you.  
D'Ann Paton

**From:** Dean W. Johnson  
**Sent:** Tuesday, August 07, 2007 3:39 PM  
**To:** Voting Systems  
**Subject:** Go get 'em

I enjoyed the testimony on TV, but you got our vote, and that was on the basis your support for open and honest voting.

Go get 'em. You'll have my vote for as long as you need it.

Dean W. Johnson

From: vpenniman  
Sent: Tuesday, August 07, 2007 6:38 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Mrs. Vivian Penniman

**From:** Larry & Vivian Sherrill  
**Sent:** Tuesday, August 07, 2007 2:44 PM  
**To:** Voting Systems  
**Subject:** Fw: Secty. Bowen's Decision on Voting machines

I write to thank Secretary Bowen for her courageous and considered decisions regarding voting machines in California. We elected her to stand for the voters of California, protecting the integrity of each person's vote, and she has done just that.

I hope she will ignore the whining of Registrars and the moaning of media who actually had to stay up late to hear her decisions. Imagine that! An elected official who works until midnight! Gasp! What a concept!

Be assured, Secty. Bowen, that the people of California appreciate your work ethic and your smart decisions. No more Floridas, and no more Ohios!

Vivian Sherrill

From: susan baritell  
Sent: Tuesday, August 07, 2007 2:24 PM  
To: Voting Systems  
Subject: my support

Dear SOS Bowen,

Thank you! Here is my letter to the Editor of the Press Democrat:

Dear Editor:

Debra Bowen ran her campaign for SOS with the promise that she would to a top to bottom review of our election system. She made no secret of her intentions. That's why we elected her. She's smart and has the courage to stand by her convictions, in the face of big money corporate politics and negative reporting. She's a real servant of the people of California. Can you think of anyone else who has followed through on their campaign promises? Neither can I.

Susan K. Baritell

**From:** TrishBrown  
**Sent:** Tuesday, August 07, 2007 2:23 PM  
**To:** Voting Systems  
**Subject:** re: Ms. Bowen

Dear Ms. Bowen,  
Thank you very much for standing up for secure elections. You made a courageous and highly ethical decision about the voting machines. I appreciate what you've done and believe it will help make our upcoming elections more accurate and less apt to be tampered with.

Sincerely  
Trish C. Brown

**From:** David Harris  
**Sent:** Tuesday, August 07, 2007 2:20 PM  
**To:** Voting Systems  
**Subject:** Great Thanks

Great Thanks to Debra Bowen for moving to save democracy.  
Our Voting is sacred to a free people. We were losing it.

Be sure to give great Gratitude to Debra. David

From: pantheonr  
Sent: Thursday, August 16, 2007 3:28 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Please de certfy the electronic voting machines. What a disgrace.

Mr. John Hubacher

**From:** Joanne Goodwin [mailto:staynwest@cox.net]  
**Sent:** Wednesday, August 15, 2007 10:48 PM  
**To:** Undisclosed-Recipient:;  
**Subject:** Dan Rather proves that West Palm Beach Florida was given dud punch ballots in 2000 DELIBERATELY

**When will the MSM and cable channels cover THIS? CNN touched on a little of it but there is so much more. The people in this film, I'm sure, would be willing to testify before Congress. EVERYONE needs to know what a sham our election process is in this great nation and DO something about it. The media needs to get this out to the public. Or do they consider this a "good" thing?**

Dan Rather proves that West Palm Beach Florida was given dud punch ballots in 2000 DELIBERATELY. (Now, who would want to make sure that a Democratic stronghold's votes did not get recorded? Maybe the company's owner, Jefferson Smurfit, who was also a big campaign donor of Jeb Bush, and frequent target of Clinton EPA intervention?)

<http://www.hd.net/drr227.html>

**Joanne Goodwin**

**From:** EcoMom2000  
**Sent:** Tuesday, August 07, 2007 1:06 PM  
**To:** Voting Systems  
**Subject:** Diebold Voting Machines

I was just reading an internet blog. This post was on someone who wanted to show how easy it is to gain access to the Diebold Machines, and to rig an election. He just took photos. I do not know who the person is, or the accuracy of the photos. I just wanted to get the information to Secretary Bowen.

Thank you. Christine Rowe

From: swedlight  
Sent: Tuesday, August 07, 2007 4:51 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Ms. Madelyn Swed

From: dea0515  
Sent: Tuesday, August 07, 2007 4:28 AM  
To: Voting Systems  
Subject: Decertify the Hackable Voting Machines

Paperless voting is as good as removing the citizen's right to vote altogether. The system for counting votes must be inviolable. Please decertify the hacked voting machines.

Mr. D Aymett

**From:** Joanne Goodwin  
**Sent:** Tuesday, August 07, 2007 12:47 PM  
**To:** Voting Systems  
**Cc:** Goldberg, Evan  
**Subject:** THANK YOU !!

**Dear Secretary Bowen;**

**I cannot begin to express my gratitude in the decisions you made on the voting machines. In my opinion, you are the first elected official to take this issue seriously and follow-up on it. So often, as you know, politicians say all the "right" words on a topic close to the hearts of constituents, but then lapse into a memory loss after taking office. You have given me some hope, when all hope was lost, for me, in the political process.**

**Voting is the most precious right the people have. It's our only say in our government. And the process of voting has to be transparent and absolutely secure. With electronic voting machines, there is no transparency (in the mechanisms inside) and when vendors and election officials say there have never been any errors on their machines, they are not being truthful. There are loads of errors reported in many, many states, including our own when they were banned before, so extreme that some states have dumped these machines altogether, like Ohio and Florida. When more votes are tallied than the number of voters, there's a major problem. When a voter selects a candidate and the opponent comes up instead, there's a major problem. When votes go "missing," never to be retrieved, there's a major problem and on and on. But you know all this and more. I just cannot**

believe that we have RoVs who are such cheerleaders for the vendor who sold them their equipment, instead of doing their real job of protecting the voters' right for a safe, accurate, verifiable and secure election. "Sleep-overs" of machines days and/or weeks before election day just doesn't cut it. And a lack of chain-of-custody logs is appalling. The printers they've attached are just as bad as the machines themselves, as proven by your team!

The RoV whining about how 6 months is not enough time to get ready for the next election is just incredible. First of all, they've known that you were going to have the review of the voting machines and they should have had a contingency plan in place already. Wouldn't they need such a plan in place anyway, if MACHINES failed? How much time does it take to print paper ballots? I know it's not as simple as it sounds, but how many days do they actually spend at the election work place, getting ready for any election? Printing companies would not do much business if they told their clients it would take MONTHS to print out paper. Newspapers do it every single day to put on news stand the very next day! Imagine that.

You have restored my faith in knowing that there's one politician that I voted for, who actually meant what she told the people with the voting machine issue. So many do not follow through on their promises. You did the right thing and we are so proud that you are our Secretary of State. Please know we appreciate your hard work...for all of us. If only we had more like you.

**Joanne Goodwin**

**From:** mcappadocia  
**Sent:** Tuesday, August 07, 2007 11:46 AM  
**To:** Voting Systems  
**Subject:** San Diego County

I am very glad that you decided to de-certified electronic touch screen voting machines in the State of California. Last Election Day, 2006, I documented my voting experience here in San Diego County. Attached is a copy of that documentation. It shows electronic touch screen voting machines with NO security seal, and many other questionable issues that electronic machines have.

I had previously mailed you a hard copy of this document, along with discs. You did receive my document and did reply with a letter of acknowledgement. I also sent a copy to the AG's Office, who also replied noting they received my documentation. I hope that my one man research has helped you to make the decision that you did.

We have a serious problem in San Diego County with the newly appointed ROV, a former electronic touch screen machine SALES REP. I simply do not trust her.

Also on her staff is someone who worked in Ohio's Cayuga county office, where 2 co-workers were found GUILTY of fraud. I believe that it is clear the San Diego County Board of Supervisor's are attempting to fix the election results for San Diego County in 2008. I urge you to please investigate and monitor the San Diego County ROV.

Lastly - I would like to know if there is a plan for mass hand counting for next election day. I would like to volunteer. I do not trust my County Officials to handle any such counting of ballots.

--

PEACE

Matt=====

Documentation of  
San Diego County's  
Touch Screen  
Voting System

2006 General Elections

by:

Matthew Cappadocia

## Documentation of San Diego County's 2006 Touch Screen voting system

---

Prepared for: Secure Accurate Elections  
P.O. Box 56, San Luis Rey, Ca. 92068  
[saesdc@yahoo.com](mailto:saesdc@yahoo.com)  
[savervote@yahoo.com](mailto:savervote@yahoo.com)  
760.500.1927

San Diego County Registrar of Voters  
P.O. Box 85656, San Diego, CA 92186-5656  
[rovmail@sdcounty.ca.gov](mailto:rovmail@sdcounty.ca.gov)  
(858) 565-5800

San Diego County Democratic Party  
8304 Clairemont Mesa Blvd., Suite 108, San Diego, 92111  
[sdcdp@sbcglobal.net](mailto:sdcdp@sbcglobal.net)  
858.277.3367

CA State Assembly Rep Lori Saldana  
1557 Columbia Street, San Diego, CA 92101  
(619) 645-3090

CA State Senator Christine Kehoe  
2445 5th Ave. Suite 200, San Diego, CA 92101  
(619) 645-3133

CA Secretary of State Debra Bowen  
1500 11th Street, Sacramento, California 95814  
(916) 653-6814

CA State Attorney General's Office  
California Department of Justice  
Attn: Public Inquiry Unit P.O. Box 944255  
Sacramento, CA 94244-2550

Rep. Susan Davis  
4305 University Avenue, Suite 515, San Diego, CA 92105  
Phone Number: (619) 280-5353  
Senator Barbara Boxer  
501 I Street, Suite 7-600, Sacramento, CA 95814  
(916) 448-2787

Prepared by: Matthew Cappadocia

Documentation of: Precinct #263200  
Church of Christ, 2528 El Cajon Blvd, San Diego, CA 92104

## **Introduction**

I am a concerned citizen, who last year decided to document my voting experience using San Diego County's Touch Screen voting system. While I was gathering information at the polling site, I thought I was gathering more than would be needed. But when I began to compile it for documentation, I realized that I didn't have nearly enough to be able to verify anything.

The other thought that struck me, and I still hold today, is that the good people who worked at the precinct may be the only ones to suffer any blame for errors made, rather than what is really to blame: a completely inept system.

## **Documentation**

On Tuesday, November 7th, 2006, I went to my Precinct #263200 at around 7:30 pm, to cast my vote and document the experience. When I first mentioned to a Poll Worker that I wanted to photograph and document the experience, she became a bit concerned. As the word spread among them there was a sense of paranoia. Not that any of them were doing anything intentionally illegal. But rather, that they, as individuals, were under review. I assured them that I was not there to document them, but rather the entire system as a whole. After speaking with them for a while, fear turned into curiosity.

I signed the Register, and was given a voting card. The first time I slid my card through it was not valid. It had to be reset. When I finally did get to the voting process, it all went well. The screen looked good and was easy to read. The onscreen instructions were simple to follow. There is no problem with the interactive features of computer voting. What matters is the security.

As part of my documentation I took a picture of the machine I voted on. You can see the serial number, and sealed hard drive.



But as I was walking away, I noticed that the machine next to me had no security seal over the hard drive. I stopped to photograph it.



The first picture was hard to read, so I took a second.



I knew that I was going to stay until the Poll closed, and planned to take a closer look. I found a second machine without a seal.



When I asked the Poll Workers, they replied that an error occurred after setting up these 2 machines in the morning. A Technician had replaced them. I was told that he signed a form (exactly which form I do not know). And that the hard drives removed would be documented.

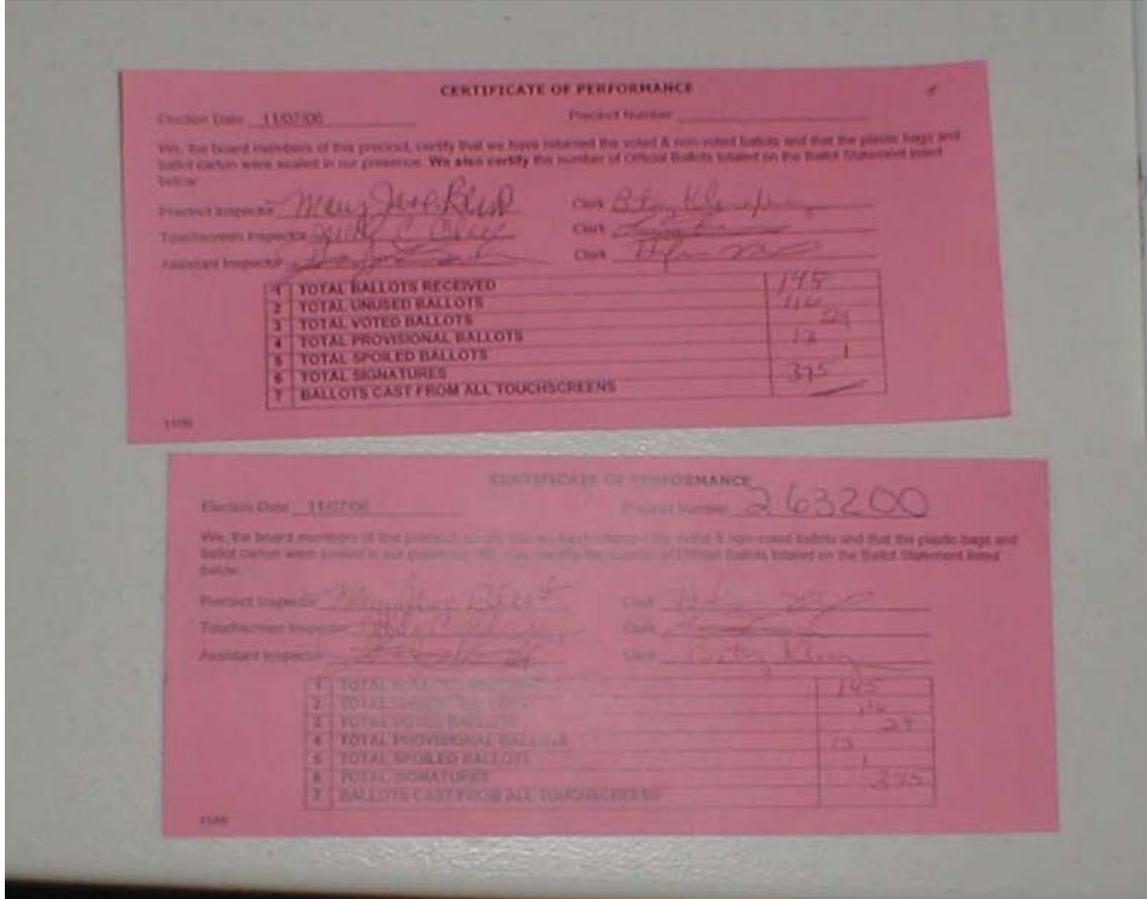
Documentation of San Diego County's 2006 Touch Screen voting system

I gathered the information from the touch screen machine printouts. I wrote down some of the figures. I quickly realized that the Public Count was the number of individual people who voted on that particular machine, and the System Count I believe is the number of individual votes.

It was then that I figured the Blank votes were the ones to watch. I was surprised at how many there were. I choose the top three races to document. Following is a spreadsheet containing that information. And apparently human error on my part must be the cause for the incomplete number of votes documented for the Secretary of State race.

| <b>Machine ID</b>         | <b>MID 0</b> | <b>MID 1</b> | <b>MID 2</b> | <b>MID 3</b> | <b>MID 4</b> | <b>MID 5</b> | <b>MID 6</b> | <b>MID 7</b> | <b>Total</b> |
|---------------------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| Serial #                  | 230596       | 229536       | 231367       | 229827       | 230642       | 229513       | 228970       | 228447       |              |
| <b>Public Count</b>       | <b>43</b>    | <b>41</b>    | <b>0</b>     | <b>46</b>    | <b>52</b>    | <b>45</b>    | <b>40</b>    | <b>36</b>    | <b>303</b>   |
| System Count              | 171          | 362          | 0            | 348          | 192          | 281          | 241          | 117          |              |
|                           |              |              | Card         |              |              |              |              |              |              |
| <b>Race/Candidate</b>     |              |              | Reset        |              |              |              |              |              |              |
|                           |              |              | Machine      |              |              |              |              |              |              |
| <b>Governor</b>           |              |              |              |              |              |              |              |              |              |
| Angelides (D)             | 19           | 26           |              | 28           | 30           | 28           | 23           | 18           | <b>172</b>   |
| Camejo (G)                | 2            | 1            |              | 1            | 6            |              | 2            | 3            | <b>15</b>    |
| Jordon (P&F)              | 1            |              |              | 1            |              |              |              |              | <b>2</b>     |
| Noonan (AI)               |              |              |              |              | 2            | 1            |              |              | <b>3</b>     |
| Olivier (L)               |              |              |              | 1            |              | 1            |              |              | <b>2</b>     |
| Schwarzenegger [R]        | 19           | 14           |              | 13           | 14           | 15           | 2            | 15           | <b>92</b>    |
| Write-In                  |              |              |              |              |              |              | 12           |              | <b>12</b>    |
| Blank                     | 2            |              |              | 2            |              |              | 1            |              | <b>5</b>     |
| <b>Total Cast</b>         | <b>43</b>    | <b>41</b>    | <b>0</b>     | <b>46</b>    | <b>52</b>    | <b>45</b>    | <b>40</b>    | <b>36</b>    | <b>303</b>   |
| <b>Secretary of State</b> |              |              |              |              |              |              |              |              |              |
| Akin (P&F)                |              | 2            |              |              | 1            |              |              | 1            | <b>4</b>     |
| Bowen (D)                 | 30           | 28           |              | 30           | 38           | 32           | 30           | 22           | <b>210</b>   |
| Hill (G)                  |              |              |              | 1            | 3            | 1            | 1            | 2            | <b>8</b>     |
| Lightfoot (L)             |              |              |              |              | 2            | 1            | 2            |              | <b>5</b>     |
| McMillion (AI)            |              |              |              | 2            |              |              |              | 1            | <b>3</b>     |
| McPherson [R]             | 7            | 10           |              | 8            | 5            | 11           | 6            | 10           | <b>57</b>    |
| Write-In                  |              |              |              |              |              |              |              |              |              |
| Blank                     |              | 1            |              |              | 3            |              | 1            |              | <b>5</b>     |
| <b>Total Cast</b>         | <b>INC</b>   | <b>41</b>    | <b>0</b>     | <b>INC</b>   | <b>52</b>    | <b>INC</b>   | <b>40</b>    | <b>36</b>    | <b>INC</b>   |
| <b>Congress</b>           |              |              |              |              |              |              |              |              |              |
| Davis (D)                 | 36           | 33           |              | 37           | 45           | 37           | 37           | 25           | <b>250</b>   |
| Lippe (G)                 | 3            |              |              |              | 2            | 1            |              |              | <b>6</b>     |
| Woodrum [R]               | 2            | 7            |              | 6            | 5            | 7            | 3            | 9            | <b>39</b>    |
| Write-In                  |              |              |              |              |              |              |              |              |              |
| Blank                     | 2            | 1            |              | 3            |              |              |              | 2            | <b>8</b>     |
| <b>Total Cast</b>         | <b>43</b>    | <b>41</b>    | <b>0</b>     | <b>46</b>    | <b>52</b>    | <b>45</b>    | <b>40</b>    | <b>36</b>    | <b>303</b>   |

As I was writing this information down, some confusion arose on the part of the Poll Workers as to how to extract the Total Ballots Cast from all Touch Screens. The Poll Workers were unable to properly witness and write down this number, as is indicated by the total left blank on the CERTIFICATE OF PERFORMANCE.



These numbers are:

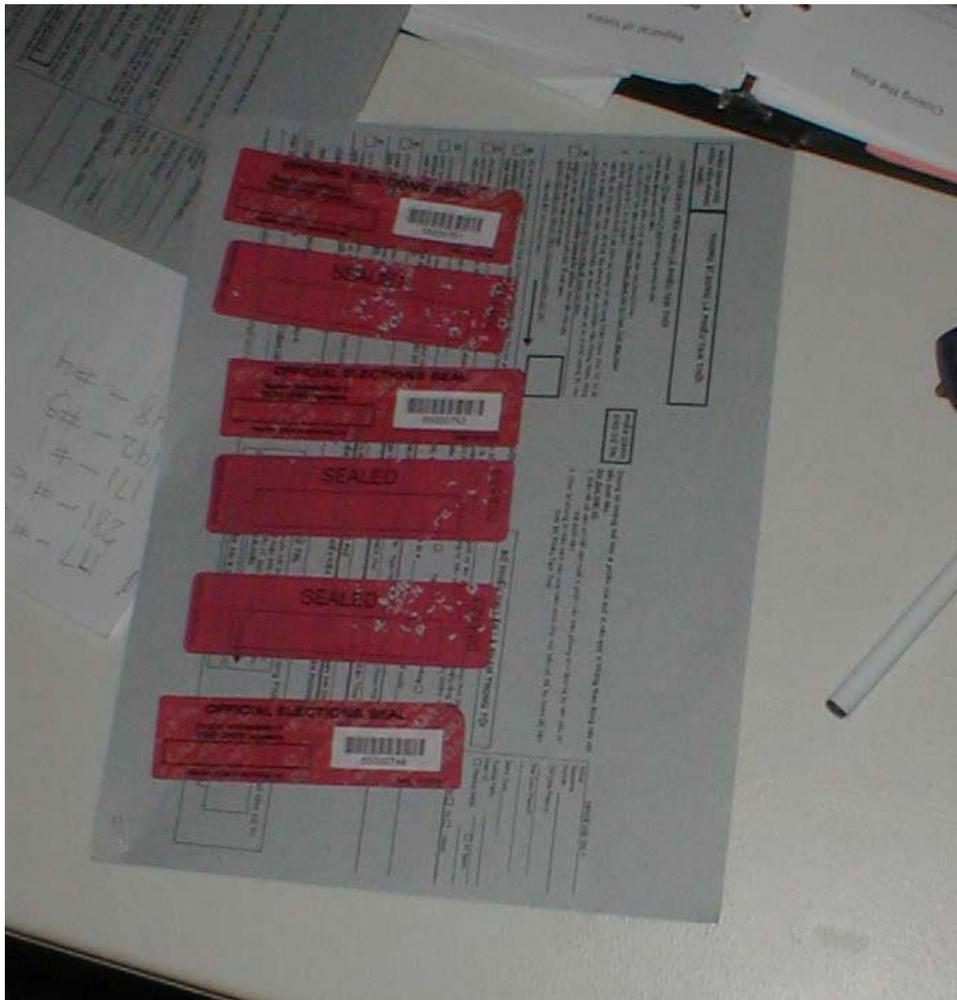
|                                           |            |
|-------------------------------------------|------------|
| <b>TOTAL BALLOTS RECEIVED</b>             | <b>145</b> |
| <b>TOTAL UNUSED BALLOTS</b>               | <b>116</b> |
| <b>TOTAL VOTED BALLOTS</b>                | <b>29</b>  |
| <b>TOTAL PROVISIONAL BALLOTS</b>          | <b>13</b>  |
| <b>TOTAL SPOILED BALLOTS</b>              | <b>1</b>   |
| <b>TOTAL SIGNATURES</b>                   | <b>375</b> |
| <b>BALLOTS CAST FROM ALL TOUCHSCREENS</b> |            |

Perhaps my record is the only one from that night that exists.

I also wrote down the total count from the register that night. I could not understand the way this was counted from the Poll Worker's explanation. I thought I might be able to balance it out later. But I am unable to reconcile the number of signatures, with the number of ballots cast at the precinct.

| <b>Register Signatures</b>            | <b>White</b> | <b>Pink</b> | <b>Blue</b> | <b>Grey</b> | <b>Total</b> |
|---------------------------------------|--------------|-------------|-------------|-------------|--------------|
|                                       | 306          | 5           | 9           | 17          | <b>337</b>   |
| <b>Number of Voters Signed Roster</b> |              |             |             |             | <b>375</b>   |
| <b>Documented Ballots</b>             |              |             |             |             | <b>345</b>   |
| Voted Ballots                         | 29           |             |             |             |              |
| Provisional Ballots                   | 13           |             |             |             |              |
| All Touchscreens                      | 303          |             |             |             |              |

The seals for only six of eight machines are submitted to the ROV. Three of them lacking any type of serial number or other identifying marker.



## **Conclusion**

Simply put, our voting system is a complete mess. There seems to be no accountability at all. Despite what the results say, there is seemingly no way to verify that the voters intent was recorded and counted properly, with any type of assurance and accuracy. We are simply at the mercy of the numbers spit out by the machine.

We need to seriously address this issue for the safety of our Democratic process. The problem is not isolated to any one thing. But rather all together, Unsecured Computer "Blank Box" voting machines, public access to the software codes that run them, the people who own and operate them, all the way down to the manner in which votes are collected, processed, and counted. There are simply too many variations, and too much room for error to firmly establish any conclusion, with any certainty, about the accuracy of any results.

I would like to petition the San Diego County Registrar of Voters to reconcile my precinct results for me.

I would like the Secretary of State to de-certify all voting machines until an open source code, publicly owned and operated system can be set into place, with a verifiable paper trail.

I would like my Congresswoman to introduce legislation to protect our voting rights.

## **Closing**

In closing I would like to thank Senator Barbara Boxer for being wise enough, and the only Senator brave enough, to stand on the Senate floor and challenge the Ohio vote count in the 2004 Presidential Election. As it has now been proven, that result was manipulated.



**PUBLIC INQUIRY UNIT**  
P.O. BOX 944255  
SACRAMENTO, CA 94244-2550  
(916) 322-3360  
TOLL FREE: (800) 952-5225  
TDY: (916) 324-5564  
or (800) 952-5548

February 27, 2007

PIU: 153603

Mr. Matthew Cappadocia

**RE: San Diego County Touch Screen Voting System**

Dear Mr. Cappadocia:

Thank you for your documentation to the Office of Attorney General Edmund G. Brown Jr. regarding touch screen voting systems.

We appreciate your taking the time to share this information with our office. It is through the special support of people like you that the Department of Justice is able to be effective in representing the interests and protecting the rights of our fellow Californians.

Again, thank you for writing.

Sincerely,

A handwritten signature in cursive script that reads "M. Vega".

M. Vega  
Public Inquiry Unit

For **EDMUND G. BROWN JR.**  
**Attorney General**

Dear Sec. of State Bower, 8/2/07

First, let me commend you for your valiant fight to protect our vote - The corrupt 'Behind-the-scenes' thugs that rule over you have managed to get their way & declare these vote machines safe & accurate but we the citizens know better from past elections.

I, as a voter, want a hand-count no machines (except for handicapped or blind) elections and by joining millions of other voters to demand it - we, the people will hold our own elections if we must no matter how long it takes to do it. In the meantime we will encourage people not to vote.

Sincerely, A very disgruntled  
voter...

AUG 07 2007

**5369 James Avenue  
Oakland, CA 94618  
28 July 2007**

**Ms. Debra Bowen, Secretary of State  
State Capitol  
State of California  
Sacramento, CA 95814**

**Dear Secretary Bowen:**

**Thank you very much for allowing some good technical research to be done on the glaring weaknesses and hackability of our lovely electronic computerized voting machines and vote tabulating machines. This research made page one, top of the fold news in both the San Francisco Chronicle and the Sacramento Bee this morning.**

**If we want to continue to allow Republican thugs, hackers and traitors to be able to hack, rig, fix and steal our elections electronically, then we should keep our present hackable system of said electronic computerized voting systems.**

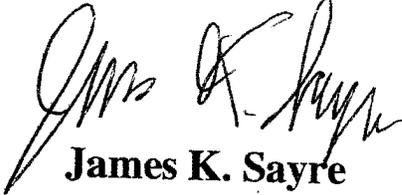
**However, I prefer democracy to electronic fascism. Dump all the electronic computerized voting machines and vote tabulating machines. into the nearest bodies of water. Then return to a traditional system of 100% hand-counted paper ballots. It works fine for Canadians. I would much rather wait a day or two for the results of an honest election, rather than have instant fascism...**

**I have no idea why California county registrars and others intimating involved with administering our elections have such a knee-jerk support of hackable electronic computerized voting machines and vote tabulating machines. Either they are**

**automatons, morons or Republicans or fools that are in denial that they have been totally suckered by electronic computerized voting machine vendors.**

**100% hand-counted paper ballots in all future California elections.**

**Yours truly,**

A handwritten signature in black ink, appearing to read "James K. Sayre". The signature is written in a cursive style with a large initial "J" and a long, sweeping underline.

**James K. Sayre**

Debra Bowen:

Thank You, Thank You

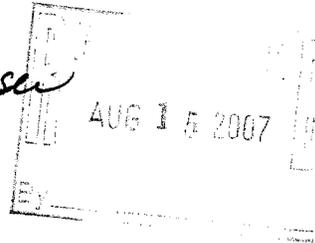
~~Thank You~~ for doing

all you have to ensure  
all votes are counted

cast! Our democracy  
depends on getting this right.

Appreciatively,

Bonnie Crossen



August 10, 2007

Ms. Debra Bowen  
Secretary of State  
State of California  
1500 – 11<sup>th</sup> Street  
Sacramento, California 95814

Dear Ms. Bowen:

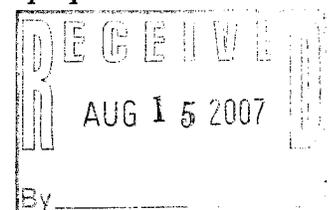
As a past long-time, and soon-to-be-returning, California resident, I appreciate and whole-heartedly support your concerns and precautions regarding electronic voting.

I am not a computer expert, by any means. However, I have seen ample anecdotal evidence that any computer system can be hacked, eventually, somehow by someone – whether it is an “inside” or outside job or whether it is done purely as a ‘lark’ or for nefarious purposes. Those who manufacture hardware and software intended for use in voting, and those who attempt to ensure the security of those systems, are, naturally, motivated by self-interest to claim otherwise...maybe even in all sincerity believing their products are the exception to the rule.

However, for all the reasons you stated on KPCC’s “Air Talk” program today, I cannot understand the apparent compulsion to institute any kind of electronic voting system at all, ever. We have, as a nation, become very used to, perhaps resigned to, the ubiquitous computer...and maybe somewhat blasé about its implications. It is certainly an invaluable technology in many applications; but the loss of privacy, lack of transparency and potential for unmonitored and uncontrolled manipulation (domestically and internationally) of mass amounts of personal data make it not only inappropriate but extremely troublesome as a mechanism for voting.

The inefficiencies and potential ‘human error’ factors of manual, paper-based processes are certainly a major factor in the interest many people and jurisdictions have for the electronic voting systems that would seemingly provide instant gratification and, theoretically, accuracy. To be sure, the ‘old-fashioned’ way is subject to oversights, negligence and fraud; but while hundreds or even thousands...conceivably more...votes might be affected, the total would still be limited and the culprit(s) would be, it seems to me, identifiable and traceable.

On the other hand, it seems a hacker could, with a click of the mouse, instantly change millions of votes...in relative, perhaps permanent, anonymity. Even if it were just an unintentional computer ‘glitch,’ the apparent proprietary provisions of the providers which limit access by public representatives to the information, the permanency (or impermanency?) of the records, and potential for immediate, wide, and possibly indiscriminate transmission and use of the data for other than their intended purposes



8.11.07

Ms. Debra Bowen  
Secretary of State

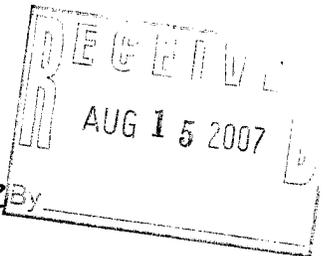
Dear Mrs. Bowen

Been reading about you "pulling  
the plug" on electronic voting machines  
in Napa.

Bravo. Way to go for discovering the  
truth. Please read:

ARMED madhouse By

By Greg Palast



Greg Palast has done extensive  
research on election electronic manipulations  
There are over 150 pages in his ~~2006~~ 2006  
Book regarding 2004 & 2008 elections, etc.  
A must read. Good Luck  
-Dan

8-12-2007

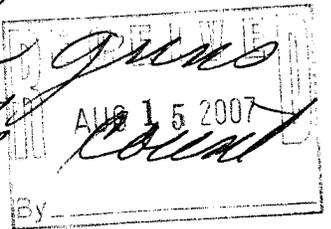


Student Union San Francisco State

Dear Secretary of State Debra

Just a note to thank you for stopping the machine vote. I am an old woman but have learned to use computers & early realized that changing the vote would be possible & the bulk of the public could not see how it was done.

Anyway speed is not necessary while accuracy is! So glad you ran the tests and stick by your guns because without proper vote count there is no democracy.



again Thanks yours truly  
Lais Roberts

California Secretary of State  
Debra Bowen  
1500 11th Street  
Sacramento, California 95814

Dear Ms. Bowen,

August 13, 2007

Thank you for decertifying electronic voting machines in light of the fact that they are prone to hacking. If we are serious about conducting fair elections then we must remove all possible circumstances enabling a person's vote to be altered. Correct tabulation of citizen's votes is the crux of ensuring fair elections.

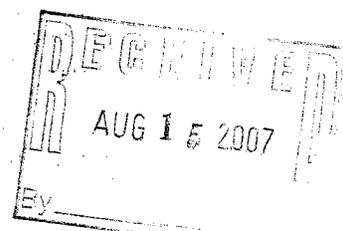
If you or your colleagues and associates have not yet seen the documentary *Hacking Democracy* I encourage you to. This documentary shows how easy it is to hack a voting machine. The Diebold machines (in Florida) were shown to have executable code within the memory card on each machine. This means that someone can manipulate the vote counts held on each machine's memory card with the executable code stored on the same memory card. This situation seems to beg for tampering.

Why are we turning our vote counting over to private corporations whose stated sole purpose is to increase profit? Can we trust a private corporation to act on behalf of the public good? Don't private corporations have political preferences, and thus, a reason to prefer the election of a certain candidate? After the fraudulent elections of 2000(Florida) and 2004(Ohio) our democracy cannot afford to wait until after the elections to discover vote tampering. We must take preventative measures, as you have done.

Requiring the use of paper ballots will help significantly reduce the chances of vote tampering and still remains a reliable way to count our votes. Thank you for protecting our votes and I hope that you can institute a policy of permanent statewide paper balloting for all of California. Thank you again for acting on behalf of the voters of California.

Sincerely,

Brian Coe



Ms. Debra Bowen – California Secretary of State  
August 10, 2007 – Page Two

are just some of the reasons I have grave concerns. I strongly believe the costs and frustrations of the traditional systems are well-worth the preservation of the overall integrity of the electoral process; that, I feel, faces a much greater threat from electronic systems, and perhaps (however unwittingly) from their purveyors, than from whatever mistakes or malfeasance might be due to an average cross-section of precinct workers.

I hope the state of California will proceed with extreme caution on the issue of electronic voting systems and will ultimately reject them completely and permanently as an alternative. I furthermore hope every jurisdiction will follow suit. To me it seems intuitively, if not demonstrably, clear such computer-based systems will never be able to provide and ensure the fundamental security required; the consequences of misplaced optimism and unfounded confidence would be far too great to risk.

Thank you for your attention and for your continued vigilance in protecting the public interest.

Sincerely,

A handwritten signature in black ink, appearing to read "David Downer", with a long, sweeping horizontal stroke extending to the right.

David Downer

Current address:

Lebra Bowen -

Thank You for testing  
all the voting machines.

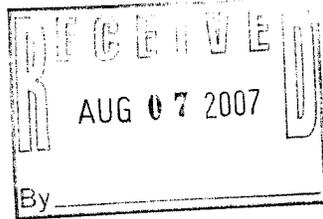
Susanna Henderson



Thank you for testing  
all the Voting machines!!

Lolbe Stein

RECEIVED  
AUG 15 2007  
BY



*From the desk of  
Sue Crittendon*

*July 29, 2007*

*Debra Bowen  
Secretary of State  
California State Capitol  
Sacramento, CA 95814*

*Dear Secretary Bowen:*

*Please decertify all electronic voting machines in California; especially Debold and especially in San Diego County, where our Registrar of Voters was a salesperson for that company. Florida has a statewide ban on electronic machines because they are so easily manipulated. What would it take for a California ban? I would like to see a national ban.*

*Thank you for your work in this area.*

*Sincerely,  
Sue Crittendon  
Sue Crittendon*