Dear Secretary Bowen:

Below are my public comments on the Draft for Public Comment published on March 22, 2007 concerning the review of voting systems currently currently certified by the State of California.

My comments are confined to the Section IV which reads:

> *Each certified voting system must be designed, configured and accompanied by sufficient documentation and training materials so that, in the absence of extraordinary circumstances, elections officials and poll workers can independently and without assistance or intervention by employees or contractors of an election system vendor, carry out all operations necessary to open the polls, set up and calibrate voting system equipment, instruct and assist voters in registering votes and casting ballots, respond to voting system error messages or temporary power failures, close the polls, print end-of-day vote totals, take down voting system equipment, transfer polling place results to central tally computers and tally final results.*
>
> *The Secretary of State will conduct a review of each voting system's documentation and records regarding the use of the voting system by elections officials and poll workers in California elections. The Secretary of State may make written findings, based on the results of the review, that a voting system does not reasonably permit such independent operation. Based on such findings, the Secretary of State may immediately initiate the process to withdraw certification from the voting system.*

Comment 1
A very significant aspect of usability is missing here; the ability of election officials to determine if a particular election system is or is not certified for use in the state. It has happened in California that a vendor has sold, installed, and misrepresented an system to election officials which was not certified for use. Demonstrating whether the system installed in Alameda County was or was not certified was difficult. This misrepresentation and the litigation which followed could have been obviated had the Alameda Election officials been able to confirm or deny the vendor claims that the system sold to them was or was not the same as the system certified by the state.
I would recommend that a physical configuration audit of the software and hardware components of each certified system be created and published by the state. So that the following system requirement can be met:

> *Each certified voting system will be accompanied by sufficient documentation and training materials so that, in the absence of extraordinary circumstances, elections officials can independently and without assistance or intervention by employees or contractors of an election system vendor, determine if a particular voting system or element thereof used within the jurisdiction of the election official does or does not belong to the certified voting system.*
> *Such identification methods and identification data shall not rely on the publication, use or abridgement of intellectual property protected by any combination of the following: trade secrets, copyrights, or patents.*

Comment 2
If Comment 1 is incorporated into the final criteria, then I would urge to Secretary to publish in a public manner both the methods for such system identification and the data used as the baseline in any such system identification.

Comment 3
If Comment 1 is incorporated into the final criteria, then I would urge the Secretary to submit any system identification information created or gathered by the state to the National Software Reference Library (NSRL) sponsored by the National Institute of Standards and Technology (NIST).

Comment 4
I am uncertain whether this comment is outside of the scope of this review, is a new section (e.g. section V), is a continuation of section IV, is a continuation of paragraph I(2)(b), or is a later implementation detail of paragraph I(2)(b). I would urge the Secretary to review the source code and election systems software escrowed by the State to confirm the source code held in escrow builds the election software held in escrow and to confirm the election software held in escrow is the same as the software of the certified systems used in the state. There is little point in performing a static source code review if there is no evidence the source code under review is or is not the source code of the software which executes on a certified system used to administer an election in the state. I would therefore suggest the following additional criterion:

> *Each certified voting system will be accompanied by sufficient documentation, tools, software, and source code such that, in the absence of extraordinary circumstances, the office of the Secretary of State can independently and without assistance or intervention by employees or contractors of an election system vendor, determine the source code held in escrow by the State of California does or does not belong to the certified voting system.*

Subject: RE: Voting Manchines
Sent: Friday, April 06, 2007 11:13 AM
To: Voting Systems
Subject: Voting Manchines

Dear Secretary Bowen:

As a citizen, I am very pleased that your office is conducting a review of the California voting system. I strongly support electronic voting systems because this technology allows for rapid vote calculation and is less susceptible to loss of voting ballots since the responses are in the computer.

However, I believe that poll workers need to be well trained in the new technology so that they can respond rapidly to voters who may be unsure how to use the machines. I sent you a proposal earlier in the year regarding poll worker training. Attached for your reference is a copy of the proposal.

Thank you for allowing a mechanism for citizen comments.

Sincerely,

Subject: Public comment re 'Top to Bottom Voting machine review'

Sent: Thursday, April 05, 2007 3:03 PM
To: Voting Systems
Cc: Secretary of State Bowen
Subject: Public comment re 'Top to Bottom Voting machine review'

Dear Secretary Bowen:
In reviewing the draft criteria for the 'top to bottom voting machine review I see several areas of concern that belies the idea of 'top to bottom'.

These areas of concern are based upon my experience, research, and knowledge. I also know from personal experience how local election officials will parse words and attempt to circumvent both the Election Code, the Procedures for Use, and conditions for use issued by the Secretary.

Please add the following to the criteria to be used for the 'top to bottom' testing.

1. Conformance to the accuracy specifications of the 2002 Voting Systems Standards. For instance, in San Diego County, which uses the Diebold Voting System(s), the voting system does NOT conform to Section 4.4.3 of the Volume 1 of the 2002 VSS (in-process audit records). Another example is the failure of the Diebold Voting System to meet the error rate specified by Section 9.4 of the Volume 1 of the 2002 VSS (Testing Scope). I know both of the examples given to be true as a result of records produced in response to public records requests I have made for both GEMS audit reports and precinct level machines.
Hopefully the Secretary will conduct the review of the voting systems reliability and accuracy by established electronic industry standards.

It is more than unfortunate that the State of California has to redo what was supposed to occur by the 'Independent Testing Authorities'. Such malfeasance and negligence by the so-called 'Independent Testing Authorities' begs that the criteria used for the 'top to bottom' review include completeness of adherence to the 2002 VSS. Failure to include the 2002 VSS as part of the 'top to bottom' review will repudiate the hearings you held while a Senator and ignore the evidence that such Federal 'certification' was nothing but a scam foisted upon the citizens of this State and country.

2. That any electronic equipment used in holding an election that is not part of a Federal qualification must be tested to standards established by the Secretary of State's office and guidelines and procedures for usage of such equipment be created by the Secretary of State's office and publicly available. Examples of such equipment would be electronic poll books and signature comparison software.

roués' of voting systems per the preparation standards deemed by the vendors -and accepted by the Secretary of State's office- as necessary for proper logic and accuracy functioning. If a vendors requirements for proper logic and accuracy functioning preclude the ability to hold an election whereby voters can trust that their vote was counted accurately, such a voting system is -obviously-not 'useable'. For example, per the IT Director of San Diego County Registrar of Voters, he only used 6 of the 10,000+ touchscreens and 80 memory cards of the 10,000+ used in last Novembers election for logic and accuracy testing despite the Procedures for Usage specified that all machines and memory cards were to be tested. He indicated it took him 2 weeks just to test the 6 machines and 80 memory cards and he also didn't use the test script as specified by the Procedures for Usage.
Simple extrapolation indicates it would take over a year to follow the MANUFACTURERS guidance for ensuring that voters votes were properly recorded and counted.
Such a system is definitely not 'useable' from an election officials duties and responsibilities perspective.

4. Changing of the phrase ".... withdraw certification FROM THE VOTING SYSTEM..." used in II (3), III, and IV and such be replaced with ".... OF the voting system...

"

Voting systems are tested and approved as a whole. If any one component or feature fails to meet the requirements of a law, regulation, or standard then the "voting system" is not approved.

5. Since it is well known that most 'hacking/fraud' occurs from 'insiders', the voting systems review that addresses 'safe from fraud or manipulation', must place the onus for such safety on the election official's shoulders. Voting systems that must be distributed on a 'sleepover' basis cannot have ANY parts, equipment, or access points by which no one other than permanent employees of the election official can use/access.
This is especially necessary as NO background checks are made of poll workers.
And that such voting systems will indicate any tampering efforts by means other than 'tape'.

6. That the "red team" exercise be conducted not only in a neutral test environment, but also with at least one deployed voting system of each model and version configured to interact with the system used by the Secretary of State's office for results reporting

7. That the following be struck from IV of the draft specifications: "in the absence of extraordinary circumstances."
The voting system should not be dependent on the vendor's assistance at an election or it's preparation for usage at all. If all equipment or power fails -an 'extraordinary circumstance'- paper ballots can be used to record voters votes.
--

Subject: Thanks for Doing a Great Job!

Sent: Thursday, April 05, 2007 6:57 AM
To: Voting Systems
Subject: Thanks for Doing a Great Job!

Dear Debra:

Congratulations on winning the race in November and thanks for scheduling the complete review of voting machines I just read about in an e-mail from Election Integrity News.

You are a breath of fresh air in the Secretary of State office and I really want to thank you for all your efforts!

A) The most secure way (for a perpetrator) to tamper with votes untraceably is to change votes at the source, DRE. If the perpetrator is successful all documentation, printed and electronic recorded, will reflect the tampered vote. The voters' real intent would be lost. For example, the DRE could be programmed to change one of every "x" votes from candidate A to candidate B when the vote is being cast. The switched vote would be recorded on the printed audit trail and on the electronically recorded vote. Program code could be embedded with rules to make the switch only if 4 conditions are met:

1. The date is the Election Day.
2. The machine is in live voting mode, not test mode.
3. The source of the input is manual, not machine entered "test votes."
4. The voter has not requested a second print out of the audit trail. (In a live situation the voter might be one of the few who actually reads the printed audit trail. He/she might have caught the switched vote on the printed audit trail and assumed that it was his/her error. The voter corrected the vote and requested a second print out.)

B) Refers to I.2.A. Red Teaming. Why should the red team approach the system knowing nothing of DREs software code? One of the greatest vulnerabilities of these systems is from the vendor's software programmers. The premise that the red team knows nothing about the software assumes that the programmers and/or machine manufactures are not the source of the attack. Not a good assumption.

C) Machine code should allow for local elections officials to test under live conditions. Election officials should be allowed to set the machines' date and time, set them in live voting mode and enter any number of transactions. Also election officials should be provided a way to automatically generate votes so that high volume testing could be performed. (Although this is not infallible, see item A condition 3 above, it does offer another level of security.)

D) ALL software changes from the time of certification, whether they are considered version changes or not, should be subject to verifying what code changes were made since the last version. The Secretary of State's future testing procedures should contain automatic identification of code change between versions. This should include changes to update ballot specifics for each county. It would be easy to slip the minor changes to the DRE code when any program change is being introduced. That could compromise an election.

E) Optical readers should determine "voter intent" considering multiple factors. "Voter intent is where a voter marked and did not mark a ballot. Some optical readers judge voter intent based only on the darkness or intensity of the mark on the paper. We used a 6% intensity guideline recommended by the vendor during testing. The machine picked up many false positives. False positives would not be identified in an actual election without a manual count unless it was an over vote. At least one additional criteria should be used, the size of the mark made. The size of the mark could be evaluated as a percent of the space filled or the percentage of the mark that is within the specified marking area.

F) Printers should facilitate reading the audit trail. Some printers are not able to print the entire office and name of candidates that have a long names and descriptions. In these cases part of the name or the office may be truncated. This makes the audit trail confusing and difficult to read. It is unacceptable.

Subject: RE: Comment on draft criteria for top-to-bottom review of voting systems
Sent: Wednesday, April 04, 2007 8:00 AM
To: Voting Systems
Subject: Comment on draft criteria for top-to-bottom review of voting systems

Secretary Bowen:

I apologize for missing the public comment period on the draft guidelines for the top-to-bottom review of California voting systems. I hope my comments may be considered before the final version is issued on April 6.

I am concerned with **accessibility and usability** of voting systems. While I was delighted to see important requirements for accessibility and usability, I think the draft falls short in a few ways.

-- There appears to be no funding for conducting usability/accessibility tests of voting systems with voters and pollworkers.

-- The Usability section focuses on elections workers, and does not mention voters. Both must be served, since both interact with the voting machine, whether it is DRE or optical scan.

-- If focuses on the machine itself, without regard to whether ballots are well-designed and usable. (This is, after all how all of this started.) The machine and the ballot (along with supporting documentation) make up a voting system.

Funding
It appears that there is funding for security testing, but not for usability/accessibility testing with pollworkers and voters. ("The Secretary of State will conduct a review...") This is a serious shortcoming. Although security clearly is an important concern, the real, documented problems in voting have come from usability issues: mainly that voters make mistakes in marking their ballots (the 2000 presidential election, the Florida CD 13 election in 2006). This problem can be minimized by usability testing ballots before they are used in elections.

Looked at another way, the design capabilities of voting systems don't produce ballots that are usable by voters. (This ripples into problems with counting, recording, and conducting recounts, as we have seen.)

Pollworker and documentation focus
Providing documentation for pollworkers will not be enough to ensure the usability of voting systems. The documentation itself must be available, accessible, and usable. The usability of the documentation can only be measured by testing it with the intended users. That said, just having usable documentation is not enough. Research in technical communication shows that people don't read and use the documentation they get.

Pollworkers are a classic case. While the classroom training I have observed for pollworkers has been very good, the training materials are supplemental to the classes. They're carried out of the classroom and never looked at again. They usually don't get to the polling place.

Voting systems *can* be designed to help pollworkers set them up, open the polls, calibrate, deal with temporary outages, generate totals, take them down, and close the polls -- without having to follow the manual or guess. California should insist on improved design in these areas rather than only demanding supporting documentation.

Efficiency and effectiveness can be measured for the interactions that pollworkers have with the voting machines in usability testing. They can also be measured for supporting documentation. But when machine and documentation are separate elements of the overall system, the overall system is less effective and efficient. We know this from 30 years of research on user assistance in the use of computers.

Usability of ballot design software and ballots themselves
Finally, I strongly urge you to go further in demanding that:

--the software for designing and generating ballots be made easy enough to use that local elections officials can use it to design their own ballots and

-- ballots themselves be usability tested with voters to identify and remedy design problems that could lead to mistakes *before* elections. (The state of Washington is beginning to include training for elections officials on usability testing ballots and other election materials.)

Most counties rely on the manufacturer (or a subcontractor) to design and lay out ballots. This is expensive, inefficient, and another possible security hole. Making the software usable for ballot design and layout gives more control to local elections officials and should shorten the process.

The state of California could also certify basic ballot templates, vocabulary, and design elements (such as type face and size, color, line height and spacing, and so on) of ballots. The EAC has already sponsored projects in this area, conducted by Design for Democracy. Oregon has been working with Design for Democracy in many aspects of its elections to improve usability and accessibility throughout the election process.

As a California voter, usability and technical communication professional, and fellow Michigan State University graduate, I am proud that you have initiated this important review of voting systems. I hope to see more forward-thinking policy and practice from your elections division.

Sincerely,

Subject: RE: Tough Standards for Voting Systems

Sent: Monday, April 02, 2007 12:03 PM
To: Voting Systems
Subject: Tough Standards for Voting Systems

THANK YOU for proposing standards that could eliminate electronic voting in CA, per article West Count Times (Contra Costa Cty) 3/28.

I think we need to return to paper, and probably hand-counted ballots to assure reliability. We must impose the same stringent standards that are used for international monitoring of new third world country elections! (Including investigations if exit polls differ from results).

Thank you Debra Bowen & staff for helping us regain our democracy!

Subject: RE: Comments on Draft Criteria for Electronic Voting
Sent: Monday, April 02, 2007 10:06 AM
To: Voting Systems
Subject: Comments on Draft Criteria for Electronic Voting

Dear Secretary Bowen & Staff:

I believe that the definitions and criteria in the draft Criteria for electronic voting are not broad enough to incorporate the use of paper systems read by optical scanners, which is the preferred current voting method in the county where I live. Specifically, in Sections I, 1. a, b, & c, there is no mention of securing paper ballots as a primary source of security. In Section IV, there should also be mention of "possess and secure auditable paper records" as one of the tasks that election poll workers can perform on their own.

I am concerned that, if all the definitions of success do not possess mention of an auditable paper trail, then only electronic systems that do not begin and end with a paper ballot marked by the voter, and possessed by the election officials, may be approved. I am also concerned that if standards of evaluation are not applied up front to Optical Scan types of systems, that manufacturers of electronic-only systems may complain that the paper-based systems were not subjected to the same scrutiny. Level playing fields lead to even competition.

Good luck in your endeavor; there is no more important function of your office than the provision of secure, auditable, trust-worthy election systems. Thank you for your excellent work.

Subject: RE: Revolutionary new electronic voting system

Sent: Sunday, April 01, 2007 9:27 AM
To: Voting Systems
Subject: Revolutionary new electronic voting system

To whom it may concern.
My name is and have a new electronic voting system that may very well revolutionize the current state of electronic voting.
The new system could save the state 10s of millions of dollars in cost, achieve all security and audit requirements, provide instant election choices, require no additional equipment or personnel at voting sites, and provide printed voter choices at the conclusion of the process.
This new system is currently in the process of patent application.

The question is how does one go about proposing such a system to the state of California for consideration ?

Subject: Public comment on E-Voting Machine Certification for California
Sent: Saturday, March 31, 2007 2:46 PM
To: Voting Systems
Subject: Public comment on E-Voting Machine Certification for California

To: Debra Bowen, Secretary of State

I am hopeful when I read that you are doing what the previous Secretary of State refused to do; take action with the PUBLIC INTEREST in mind. I appreciate your "top to bottom" review of all electronic voting systems. As an ordinary citizen I am appalled almost daily as I read about what has happened to elections in America since the introduction of E-voting. The evidence all points to a massive fraud applied to elections in America by a small group of conservatives in our country through the introduction of HAVA and E-voting. I wasn't aware of it in 2000, wasn't sure in 2004 and 2006, but now I'm convinced my vote and/or my vote count by an optical scanning machine is no longer secure and can easily be changed without my knowledge, without a trace and impossible to be verified by anyone. I no longer want my vote, even if done on a paper ballot, to be put in an optical scan machine. Those vote results can also be changed and a recount will most likely never be done, expense and time being two major factors.

I'm sure you have followed the many daily recounts of voting fraud in places like www.bradblog.com . Many citizens like myself strongly want HAND COUNTED PAPER BALLOTS. Election fraud nation wide has made many of us very angry. Thank you for your willingness to stand up to the likes of Diebold and other E-Voting Companies and take a stand for us, the public. I and everyone I know want to think that we still live in a country where we have the right to vote AND THE RIGHT TO HAVE OUR VOTES COUNTED ACCURATELY.
Without that confidence, we have all turned down a dark alley in America and the future is frightening.

Below is an article I read and saved because the information in it seems so very important. Please read and consider the facts as you make your decision.
Thank you for all you are doing for all of us ordinary citizens.

112 November 2006/Vol. 49, No. 11 COMMUNICATIONS OF THE ACM

During the U.S. 2006 primary election season, there was a flurry of media attention about electronic voting, when it was revealed that Diebold Election Systems had erroneously reported to a testing authority (CIBER) that certain Windows CE operating system files were commercial-off-the-shelf (COTS) but in fact also contained customized code. This is important because, remarkably, all versions of the federal voting system guidelines exempt COTS hardware and software from inspection, whereas modified components require additional scrutiny. This loophole is anathema to security and integrity. In other critical computer-based devices (such as medical electronics or aviation), COTS components may be unit-tested once for use in multiple products, with COTS software typically integration-tested and its source code required for review. In contrast, for voting equipment, this blanket inspection exemption persists, despite having strenuously been protested by numerous scientists, especially in the construction of guidelines authorized by the Help America Vote Act

(HAVA). Nevertheless, special interests have prevailed in perpetuating this serious backdoor in the advisory documents used for U.S. voting system testing and certification programs.

Indeed, Diebold dismissed the discovered customizations as presenting only "a theoretical security vulnerability that could potentially allow unauthorized software to be loaded onto the system"; a Diebold spokesman commented "for there to be a problem here, you're basically assuming ... you have some evil and nefarious election officials who would sneak in and introduce a piece of software. ... I don't believe these evil elections people exist." But such naiveté is laughable, as there is a long and well-documented history of such "political machines" and operatives in the U.S.

Uninspected COTS has caused other serious voting equipment problems to go undetected, even if tampering is not an issue, as reported in 2001 to the U.S. House Science Committee by Douglas Jones, when he related a 1998 example of "an interesting and obscure failing [with the Fidlar and Chambers EV 2000] that was directly due to a combination of this exemption and a recent upgrade to the version of Windows being used by the vendor ... the machine always subtly but reliably revealed the previous voter's vote to the next voter."

The strong resistance to closing this COTS backdoor was illustrated by the activities of the IEEE's P1583 Voting System Standards working group, while they were drafting a document to be submitted as input to the Election Assistance Commission's (EAC) Technical Guidelines Development Committee. A Special Task Group (STG) was formed to resolve COTS-related issues in the draft. Although all issues were resolved with strong consent by the STG's members, P1583's vendorpartisan editing committee unabashedly repeatedly refused to incorporate any of the substantial COTS review requirements into the draft. Therefore, the version of the document released to the EAC still contained the exemption for COTS components, even though the working group had decided otherwise.

Numerous other aspects of U.S. voting equipment certification process are similarly lax. Another P1583 working group member, Stanley Klein, repeatedly pointed out to the EAC that the legacy low 163-hour Mean Time Between Failures rate specified in all versions of the voting system guidelines translated to an Election Day malfunction probability (potentially resulting in unrecoverable loss of votes) of 9.2% per machine, to no avail. Attempts to require a Common Criteria style evaluation were frustrated. Bizarrely, the guidelines allow for the risky use of wireless transceivers in voting machines, but do not require that the ballot data be provided in a format such that it is independently auditable. And although there is a federal certification process, there is no provision for decertification, even when a major security flaw has been exposed. The fact that any changes, including security-related ones, require recertification, has even been used as an excuse to avoid making needed updates. Indeed, the nature of U.S. elections is such that federal certification, as poor as it is, is not mandatory; one-fifth of the states have chosen to disregard it, some in lieu of even more haphazard and obfuscated examination processes.

This distressing situation will likely continue until large numbers of citizens, especially those with technical expertise, hold government officials accountable. You can help by communicating with your elected officials, beseeching them to do something about this now.

Rebecca Mercuri (mercuri@acm.org) is a forensic computing expert who has been researching electronic voting since 1989. **Vincent Lipsio** (vince@lipsio.com) is a software engineer who specializes in realtime and life-critical systems. **Beth Feehan** (bfeehan@comcast.net) is a researcher focusing on HAVA implementation issues.

c

COTS and Other Electronic Voting Backdoors

PAUL WATSON

Inside Risks Rebecca T. Mercuri, Vincent J. Lipsio, and Beth Feehan

Subject: RE: Top to Bottom Review
Sent: Saturday, March 31, 2007 1:15 PM
To: Voting Systems
Subject: Top to Bottom Review

To: Debra Bowen CA SOS

I voted for you because you appear to recognize that the software dependent e-voting systems are not a secure or transparent method to use for our elections in a democratic nation.

Avi Rubin has just testified before Congress and advised them that DREs with or without a VVPAT are UNACCEPTABLE FOR USE IN A DEMOCRACY. Do you know of any one who has better credentials who can legally refute his statement? If you do please present their argument, or immediatly decertify all the software dependent machines.

The NIST declared in their recent report, Jan. 2007, that they COULD NOT DEVISE A TEST TO PROVE THE TALLIES ARE ACCURATE ON ANY SOFTWARE DEPENDENT MACHINES. They stated that the DRES should not continue to be used and that paper rolls should not be used on new machines. You should be aware of this report. THESE TWO STATEMENTS ALONE SOULD BE ADEQUATE EVIDENCE TO IMMEDIATELY DECERTIFY ALL THE SOFTWARE DEPENDENT EQUIPMENT IN CA.!!!!!!

Ciber was found by the EAC last AUG. to have failed to provide proper test records and were suspended from continuing to test. We believe this testing to be irrelevant and inconclusive to begin with, however our Sequoia machines were tested by Ciber and we therefore believe they shoud be immediately decertified.

While Avi Rubin has determined that the software vulnerabilities he has acknowledged are unacceptable in the touch screen DREs, he has failed to heed the warning of the GAO Report of 2005 which stated that it is "unrealistic and impractical to expect mitigating security measures to protect our election system from manipulation and fraud."

I would advise that it is not only UNREALISTIC but IMPOSSIBLE and an INSULT to the American citizens to make any attempt whatsoever to attempt to provide protection for this machinery from fraud or manipulation . I would remind you that the CA CODE 19205 requires that the voting system be" free from fraud and manipulation."

The mitigating security measures devised by McPerson are a coverup for the use of equipment that is ABSOLUTEY an assult on the integrity of our election process. Please STOP THE CHARADE.

SAVElections Monterey County is an action committee sponsored by the Womens International League For Peace and Freedom. Members of SAVElections Montery County have called for the removal of all software dependent e-voting equipment. We are circulating a petition which demands that this equipment be replaced with paper ballots hand counted at the precinct level. We have the support of many thousand concerned individuals who share our call for a ban on all this equipment in CA and the nation.

We are working with other citizen activist groups in CA to remove software dependent e-voting machinery throughout the state and across America.

Please hear our plea, and use your authority to return our democracy to the people. Our elections are now under control of the vendors who supply the machines and anyone who has access to the software. As you well know, anyone who has access to the software has THE POTENTIAL TO MANIPULATE THE RESULTS OF AN ELECTION WITHOUT LEAVING A TRACE OF EVIDENCE.

Professor Appel of Princeton U. has demonstrated on the Sequoia machines he purchased on e-bay in March 2007 that these machines can easily be hacked WITHOUT LEAVING A TRACE OF EVIDENCE! Since there were at least 100 more machines offered in that sale I would suggest that there are plenty of others who have now had the opportunity to practice hacking these machines.

Since you must proceed with your review please engage the following experts to review the Sequoia machinery. Jeremiah Akin-Joseph Holder-Jim Soper. We believe their review will be accurate. Also please make results of all tests public immediately.

Please review WinEDS/BPS Application .
We specifically request the results of this Ballot Printing Software which is being purchased by our ROV.

Thank you for your consideration of our request. We would appreciate an acknowledgement of this letter.

Subject: Comments on Draft Guidelines for Voting Systems Review

Sent: Friday, March 30, 2007 10:48 PM
To: Voting Systems; Secretary of State Bowen; Finley, Lowell
Subject: Comments on Draft Guidelines for Voting Systems Review

Secretary Bowen,

I sent my comments in at 4:57 today to votingsystems@sos.ca.gov,
but did not get an automated reply.
Since I know did get an automated reply, this makes me
uneasy, so I am resending my comments on the Draft Criteria both to
votingsystems@sos.ca.gov, to your address, and to Lowell Finley's
address.

I'm copying the text below, and also it is available at:

http://election-reform.org/california_review/jerry.html

which may be easier to read.

Thank you both for working to restore integrity to our elections.

Comments on Draft Criteria of March 22, 2007 in:

TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS
CERTIFIED FOR USE IN CALIFORNIA ELECTIONS

Page 1, Title:

The Draft Criteria's title says:
"Electronic Voting Systems Certified"
while the first paragraph says:
"voting systems currently certified".
"Electronic Voting Systems" may be interpreted as excluded optical scan systems. All voting systems certified for use in California should be reviewed. Delete the word "Electronic" in the title.

Page 1, paragraph 1:

The first paragraph says:
The goal of the review is to determine whether currently certified voting systems provide acceptable levels of security, accessibility, ballot secrecy, accuracy and usability under federal and state standards.
The draft criteria include sections/criteria for security, accessibility, and usability, but not sections/criteria for ballot secrecy and accuracy.
Pages 1, 2, and 4, use of word "standards"

Page 1, paragraph 1: "federal and state standards" should be "federal and state laws and guidelines". Page 2: "voluntary federal voting system standards" should be "federal voluntary voting system guidelines".
Page 2: "Security Standards" ... "For purposes of these standards ..."
Page 4: "Disability Access Standards". I would use "requirements" instead of "standards" in these three places. "standards" might have a legal meaning and requirements for setting.

Page 2 and 3 Vote Tampering:

"untraceable vote tampering" is defined and then used in 4 additional

places. Vote tampering, whether traceable or not, must be prevented. This is especially true as the public is not allowed to look at the logs or other places traceable vote tampering might have left its mark. So, I'd recommend changing the definition to:
"vote tampering" means preventing the accurate electronic recording of votes, or altering the record of votes, to change the result of an election."
After changing the definition, change "untraceable vote tampering" wherever it occurs later in the document to "traceable and untraceable vote tampering" or just "vote tampering".
Pages 2-3. I. 1. Security Standards

I'd like a subsection d. which would apply to any part of the voting system not covered by a., b., and c. In particular, some optical scanners may just convey ballot images or ballot selections and not do any counting and may not be covered by a., b., and c. Also the voter access card enablers wouldn't be covered.
Page 3. I. 2. b. Source Code Review

This says "prior to, during or after completion of the risk assessment", but that is the only place "risk assessment" appears; i.e. it is not defined and therefore I don't know what this sentence means.
Also, in my opinion, it will be impossible to review all the source code of all the certified systems. Perhaps the paragraph should be rephrased to indicate partial source code review, as time and resources permit. The findings at the end of the process must make clear exactly how much source code review was done. We don't want a partial source code review with vendors claiming California proved the code is bug free and vulnerability free. Actually, they probably will whatever you do, but you should try to make it clear that your source code review is incomplete.

Page 5. II. 2. (f) Accessibility

II.2.(f) states:
(f) In the case of a DRE, the capability to permit a voter to verify electronically, through a nonvisual method, the information that is contained on the voter verifiable paper record copy of that voter's ballot. This requirement is satisfied by a method of nonvisual confirmation that draws the information provided to the voter from either (1) the paper record copy itself or (2) the same electronic data stream used to print the voter verifiable paper record copy.
II.2.(f)(2) is not sufficient. The Elections Code says that the voter may verify:

"the information that is contained on the paper record copy" (19250(d))
"the information provided on the paper record copy" (19251(a))

via a nonvisual means.
II.2.(f)(2) at best conveys to the voter the information the machine expects to be on the paper record copy, regardless of what actually is on the paper record copy.

There are many situations in which the paper record copy does not contain the proper information:

if there is a paper jam
if the paper was inserted backwards or upside down, as happened in Ohio
if the printer runs out of ink or the ink supply is blocked
if the printer/computer connection is faulty or the printer driver or printer firmware is buggy
if there is malicious code to "game" the VVPAT
For how to "game" the VVPAT, see:
David Dill's paper, "VVPR Attack with Misprinted VVPAT",
http://vote.nist.gov/threats/papers/misprintedVVPAT.pdf
Ted Selker's paper, "Security Vulnerabilities and Problems with VVPT",

http://vote.nist.gov/threats/papers/vvpt.pdf
for more info.
Actually, I'm not even sure what "the same electronic data stream" means. When the VVPAT is printed, the "electronic data stream" is not saved. If you mean recreating the data stream sent to the printer, that stream will contain printer control characters, so it can not be sent to an audio device. If you mean the data stream before it gets to the printer driver, this would not protect against malicious code in the printer driver or sending a different data stream to the audio device.

Page 5. IV. Usability

"respond to voting system error message" - these should be in comprehensible English, not just error numbers.
"print end-of-day vote totals" - this should be independent of other printouts; i.e. not on sealed VVPATs.

Counties should also be able to set up elections, e.g. ballot definition files, etc. to avoid problems like those with ES&S being so late in the last election.

I've heard counties using ES&S systems have to have ES&S in Omaha, Nebraska, program the firmware for their county's machines before each election. If that is true, the software for programming the firmware may not be in escrow in California and may not even be certified for use in Claifornia. That can be tested simply by testing creating a new election.

Not Covered in the Draft Criteria:

1. Ballot Secrecy/Privacy

An item needs to be added as to how well the equipment preserves the secrecy of the ballot, as required by the California Constitution.
The continuous roll VVPAT does not seem to protect the secrecy of the vote, since: - anyone can observe at the polls (EC 2300 and EC 19362), - each voter must audibly state their name before voting (EC 14216), - anyone can request a recount of a precinct (EC 15620 and 15621), and - anyone can watch the recount of the precinct (EC 15629),

Michael Shamos, Pennsylvania's Certifier of Election Systems, won't certify any continuous roll VVPATs due to concerns about the secrecy of the ballot.

This is an even worse problem in counties like Alameda County, where on election day, only the disabled will use the DRE. Last November, most of the DREs in Alameda County held only one or two votes. If the results tape for the DRE is posted as required by the Elections Code and only one person used the DRE, then that person's ballot is displayed.

2. Security - Testing if code is escrowed.

EC 19223:
19223. The Secretary of State shall conduct random audits of the software installed on direct recording electronic voting systems, as defined in Section 19251, to ensure that the installed software is identical to the software that has been approved for use on that voting system.
Although required, I doubt the random audit has been performed recently. To do this, take random machines from the Counties and compare the software to that in escrow. To make a true comparison, you must company binary executables. According to "Voting System Requirements", 10/5/05, http://ss.ca.gov/elections/voting_systems/requirements.pdf, these should be on file with the Secretary:
VOTING SYSTEM REQUIREMENTS

Any new voting system to be considered for certification for use in California elections will be required to have the following features:

...

5. In addition to depositing the source code in an approved escrow facility, each vendor must deposit a copy of the system source code and binary executables with the Secretary of State. ...

There have been articles stating that ES&S installs a different version of the executable in each precinct, e.g.:
"ES&S Programming Is Unverifiable", by John Washburn,
http://www.washburnresearch.org/archive/ESSFirmware/ESS-Firmware-001.pdf

This can be tested by comparing the binaries and firmware on several machines used in different parts of a county or in a different county. If true, this would violate EC 19103. (a):

No voting system may be used for an election unless an exact copy of the ballot tally software program source codes is placed in escrow.
3. Security - Code on removable media.

The security tests and code review should include testing whether there are binaries/executables/scripts or equivalent on removable media, or whether the machine would use such code if it were there. If so, this is a security risk and should result in decertification.
4. Security - Testing mode

All testing should be done in election mode, not test mode.
5. Suitability/Usability - MTTF

The MTTF (Mean Time to Failure) in the VVSG would allow 10% of the machines to fail on an election day, where the machines are used for about 15 hours. This is far too many failures, putting stress on pollworkers and elections department staff. We must require a higher MTTF; a machine with a 163 hours MTTF may be suitable for a polling place at the elections department office, but is not suitable for offsite polling places.
6. Suitability - Calibration

Test how often a machine requires recalibration. Test to see if transportation affects calibration.
I don't think pollworkers should need to do recalibration. If that is the case, the MTTF of the machine with respect to calibration must be evaluated, and should be on the order of 100 hours or more, or this is not a suitable machine.

If pollworkers are expected to do recalibration as needed, the recalibration procedure must be simple. Otherwise, it fails the suitability requirement. After a machine is recalibrated, I would expect Logic and Accuracy testing to be redone. Is this required by the procedures?

7. Security - Storage/Sleepovers

How does this security review relate to how machines are stored between elections, transported to the polls, stored at election sites (often in public places), and so-called sleepovers with pollworkers?
8. Security - Early Voting and Absentee Vote Counting

For early voting, equipment must be secured for days or weeks after voting has begun. The equipment is probably left unattended overnights and weekends. Likely the equipment in the Registrar's main office is well secured, but the equipment in satellite locations is probably much less well secured. I have heard some counties have portable absentee voting stations on buses. Use conditions must spell out what security precautions

are necessary.
Tabulating of absentee voting has similar problems when done before election day. Since the optical scan equipment is left unattended and vote counts are not allowed to be accessed until 8p.m. election day (EC 15101.), stringent security precautions are necessary to protect the vote. Since many counties have purchased new high speed scanners, it may no longer be necessary for them to start tabulating votes before election day.

9. Suitability - SOVC

In larger counties, the Statement of Votes Cast (SOVC) is huge. It should be simple for interested parties to access the numbers in the SOVC and put them in spreadsheets, etc. However, the SOVC is often only provided as a PDF file which can not be processed electronically. In Alameda County in the 2004 general election, the SOVC was 75 Megabytes, 6600 pages. Most of the data is just zeros, e.g. listing zero vote counts for Oakland precincts for a Livermore council race.
The SOVC should also be available in a more usable format, preferably as a CSV (comma separated value) file. In the current environment, I would say any system which can not do this would fail the suitability requirement.

If this can not be required as part of the current review, it certainly should be made a requirement for any future certifications.

10. Suitability - Recounts

The continuous paper roll VVPATs must be tested for how hard it is to count the votes by hand, as is done in the 1% manual tally and recounts. Registrar Jill LaVine tested one vendor's equipment in early voting in Sacramento County. As a test, they manually counted the VVPATs for one of the early voting polling places: It took 127.5 hours to recount the 114 ballots, or approximately an hour and 15 minutes for each ballot. (http://www.eac.gov/docs/LaVine%20Testimony%204-20-06.pdf)

This would fail the suitability requirement for any county with significant early voting or vote centers.

11. Accuracy - Optical Scanners

The optical scanners should be tested for accuracy. Testing should include how dark and what sizes marks must be to register as votes, whether there is a difference when ballots are flipped end-to-end or upside-down or both.
Testing of this type is described in:

"Regarding the Optical Mark-Sense Vote Tabulators in Maricopa County" by Doug Jones, University of Iowa.
http://www.cs.uiowa.edu/~jones/voting/ArizonaDist20.pdf

In addition, there should be testing with of various types depending on the types of choices on the ballot.

This is described in John Washburn's Election Integrity site:
"Testing Voting Equipment",
http://www.washburnresearch.org/ElectionIntegrity.html

12. Accuracy - DREs

There have been many cases of vote flipping. The DREs must be tested for vote flipping and whether the VVPAT agrees with the voters choices and with the electronic ballots.
13. Security - Logs, Data files

File of vote totals, logs, data files, etc. must be public. Otherwise there is no transparency and no real security. These files must be available electronically and at nominal, if any, cost.

14. Usability - California AVVPAT Standard

California develped a standard for AVVPATs. The June 15, 2004 version is no longer available on the Secretary of State web site. However, it is available via the "WayBack" archives at:
http://web.archive.org/web/20051124102850/http://www.ss.ca.gov/elections/ks_dre_papers/avvpat_standards_6_15a_04.pdf

This includes more details than the Elections Code, e.g. it says in section 2.4.3 that the Paper Record Display Unit must include an audio component.

This standard disappeared from the web without notice. Is that appropriate? Is this still a standard?

15. General Thoughts

I find it ironic that the Government Code, Secretary of State Duties, section 12168.7, wants the Secretary of State to develop standards for a "trusted system" for electronic storage of records:
"trusted system" means a combination of techniques, policies, and procedures for which there is no plausible scenario in which a document retrieved from or reproduced by the system could differ substantially from the document that is originally stored."
The "no plausible scenario" seems a much stronger criterium than that accepted by most for election equipment.

16. General Thoughts

Once a system passes this test, what sort of upgrades will be allowed? Will minor upgrades be allowed without federal testing, or will any upgrades require compliance with the VVSG 2005?

From: on behalf of Voting Systems
Subject: Added Comments on Top-to-Bottom review

Sent: Friday, March 30, 2007 11:06 PM
To: Voting Systems
Subject: Added Comments on Top-to-Bottom review

Hello,
After further consideration I have a few more comments on your review plan for electronic voting systems. My apologies for not including them all in my previous message.

1. Will there be tactile ballots or any other voting system to allow profoundly deaf-blind voters to vote privately and independently or to allow voters with visual impairments and other disabilities to privately and independently vote absentee?
2. Will any blends of different voting equipment be allowed to meet the criteria as a blended voting system?
3. Will currently fielded versions of equipment be considered for meeting your criteria for certification, and would available, shipping, but not ordered options be considered for meeting certification? For example, if a county has not ordered jelly or sip and puff switches to use on a Sequoia Edge II equipped with supporting audio/tactile keypad and software be decertified, if they don't take corrective action to procure the switches before the February election? What about "coming soon" options that are not yet shipping but are promised by vendors?
4. For new options that are promised to be "ready in time" to meet state certification needs, what would be the deadline for any required federal certification, in time to meet Calif. state testing and certification?

Thank you for taking the time to consider my comments.
Sincerely,

Subject: Impt. PS re Voting Systems Review Comments
Sent: Friday, March 30, 2007 8:55 PM

Cc: Voting Systems;
Subject: Re: Impt. PS re Voting Systems Review Comments

On Friday, March 30, 2007, at 06:22 PM, wrote:

> Second, related to voting machines is the auditing process which is meant to provide a check and balance against machine results. Audits are currently being done with minimal chain of custody security, if at all, and with the 1% minimum required percentage that is statistically unreliable. We need a 10% random, mandatory audit of all precincts to provide a meaningful data set against the machines.

Hi --

Great letter! I would just add to the above that the audits MUST occur at the PRECINCT. After reviewing audits for a few years now, it has become clear to me that this is the only way to ensure, at LEAST, a 99% statistical confidence in our election results.

In fact, it's more important to do a 10% audit at the precinct than a 100% hand count at the county site.

Why? Because once the voter verified ballots leave the citizen-controlled purview, which confers an equal partnership between the citizens and the controlling government, then they become anonymous in a plumbing system that is impossible to completely control. A 10% random audit at the precinct, as described in the Titanium Standard (which also outlines a whole host of checks and balances) confers confidence that there is, indeed, an exact 1-to-1 correspondence between the ballot cast vs. the ballot tabulated.

And any "citizen oversight" at the county site is nothing but a charade, because you can never be certain that all the ballots are included, and even if they are, you cannot be certain that they have not been manipulated. Also, there's the fact that what you can view, as an observer, at the county site is incomplete. But even if you could see something, it is cryptic and really only a charade to gain consensus from the public. Because, again, you have no way of knowing all the ballots are included (except for assurances by their paperwork) and you have no way of knowing there has not been any manipulation of the ballots or their data.

As Elaine Ginnold and Michael Smith of Marin County admits, "Well, you've got to trust your institutions."

I say bloody hell we do! That is NOT the American way. Instead, it's our government, and we must: Trust but verify.

I'm writing up an article about this, and I'd love a quote from you or Dennis about your appalling experience with the L&A testing and your frustrations.

So, never without an opinion,

#:)

Subject: Voting Systems Review Comments

Sent: Friday, March 30, 2007 7:23 PM
To: Voting Systems

Subject: Voting Systems Review Comments

Secretary of State Debra Bowen
1500 11th Street
Sacramento, CA 95814
Attention: Voting Systems Review

I agree with the comments made by and on improvements needed to our voting systems here in California.

In addition I would like to add a few comments please:

First, I heartily congratulate you for the top to bottom review of voting systems as this is sorely needed. Your courage in challenging the security of the current systems is a testament to the quality of your leadership and dedication to integrity in elections.

Second, related to voting machines is the auditing process which is meant to provide a check and balance against machine results. Audits are currently being done with minimal chain of custody security, if at all, and with the 1% minimum required percentage that is statistically unreliable. We need a 10% random, mandatory audit of all precincts to provide a meaningful data set against the machines.

Third, citizen access is severely or completely restricted in most counties at this time. Observers are limited to see only what the Election Officials think would not produce evidence of system problems. It becomes a PR game of when and where the Observers are allowed to actually see what is going on. This has created an opaque election environment ruled by county officials who at times don't even follow our minimal laws.

Fourth, underlying all aspects of election problems is the fact that transparency and checks and balances are the key to integrity. Without transparency we are being asked to trust the process, without being able to verify that the trust is actually warranted. Privately owned and controlled proprietary software is the greatest threat to our democracy and voter confidence. We must move toward transparency at every step of the elections process.

Fifth, election advocates need to have access to observe elections for the presidential race in 2008. If you leave it up to the counties, they would again bar the voters from full observation and subsequent enforcement of the law. Consider how you can use the power of your office and your vast staff to create opportunities for citizen participation at the county level.

Sixth, election are being privatized. We need limits on how much the private vendors can run our elections, are given access, and running the IT support that most election offices don't have in house. This gives far too much power to entities who are often partisan, profit driven and not public servants.

Thank you for all you are doing for our democracy Debra.

Sincerely,

California Secretary of State Top to Bottom review
of Electronic Voting Systems

My comments will be enclosed in "**" prefix and suffixs.
** Comments:
Generally, it appears that BMD and BOD systems were specifically left out of these considerations. Will they not be tested?
Also, there appears to be no testing for usability and accuracy.
Write-in input method and the write-in verification from the ballot do not appear to be discussed.
**

untraceable vote tampering:
** Comment: There are forms of detectable or traceable vote tampering which can alter the result of an election, so the system should be tested for these threats too. Some means of tampering can be detected after the fact, but leave no means for vote recovery or correction.
**

Denial-of-service means disabling a voting system other than through sheer physical destruction in a manner that renders the voting system inoperable for voting.
** Comment: Why not include physical damage that isn't obvious? For example, dribbling salt water into openings or cracks in the case, or zapping exposed connectors with high voltage static discharges.
Will your denial of service vulnerability testing include prolonged power outages?
**

source code review. The objective of the source code review will be to identify anything
in the code that could be used maliciously to interfere with the accurate recording of
votes or alter the record of votes to change the result of an election.
** Comment: Why not also check for improper code that can accidently corrupt the vote? **

** Comment: What about examining vendors' recommended corrective procedures for malfunctions? **

Security:
** Comments:
Chain of custody access control should also include vendors and contractors for any maintenance or support services.
Systems should not use any wireless communications links.
Systems shall not use public telephone lines without secure scramblers and other privacy/security protection.
**

For purposes of this review, a voting system complies only if
it provides all of the following features and capabilities in at least one voting system available for use in every polling place:
(a) A dual-switch input control interface that permits use of "sip and puff" or other
adaptive devices by voters with paralysis or severe manual dexterity disabilities who are unable to use touch screens or tactile key inputs.
(b) The capability for the voter to select simultaneous and synchronized audio and visual outputs, audio outputs only or visual outputs only.
** Comment: and not be forced to use the audio-output-only mode when they are using tactile key input or dual-switch input controls.
(c) Voter-adjustable magnification, contrast and display color settings to improve the readability of text on the video displays.
(d) Variable audio output levels and playback speed for voters with hearing impairments.
** Comment: Audio volume and rate controls are not just for voters with hearing

impairments. Built-in volume and rate controls should reset to normal at beginning of each voter's session. Minimum high volume output, as per VVSG. Speech rate control without chipmonk pitch distortion. **
(e) Privacy curtains or shields that effectively prevent others from observing or hearing the selections of a voter using such features as audio output, simultaneous, synchronized audio and visual output, display magnification or modified
display font, contrast or color settings.
(f) In the case of a DRE, the capability to permit a voter to verify electronically, through a nonvisual method, the information that is contained on the voter verifiable paper record copy of that voter's ballot. This requirement is satisfied
by a method of nonvisual confirmation that draws the information provided to the voter from either (1) the paper record copy itself or (2) the same electronic data stream used to print the voter verifiable paper record copy.
** Comment: verification from a printer data stream has serious drawbacks.
1. It does not detect failure of the printer to ink properly.
2. Does not confirm that the ballot was not pre-marked.
3. Does not give software independent verification with module isolation between vote selection/marking and verification modules.
4. Because data stream verification appears only to work for text data streams, not bit-mapped image streams, it cannot be used to print optical scan mark sense ballots. This results in a segregated ballot system, if the rest of the voters are using OS ballots.
**

III. ACCESS FOR MINORITY LANGUAGE VOTERS.
HAVA requires that every voting system used in an election for federal office "shall provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a)." Every certified
voting system will be tested to determine whether it provides alternative language accessibility in the federally mandated language or languages for each county that uses or intends to use the system.
** Comment: What about precinct signage and procedures that may accommodate language access needs? **

IV. USABILITY FOR ELECTIONS OFFICIALS AND POLL WORKERS.
** Comment: How much training can or should be required for proper training of the average poll worker. Does the system require unreasonable amounts of poll worker training? **
Each certified voting system must be designed, configured and accompanied by sufficient
documentation and training materials so that, in the absence of extraordinary circumstances, elections officials and poll workers can independently and without assistance or intervention by employees or contractors of an election system vendor, carry out all operations necessary to open the polls, set up and calibrate voting system equipment, instruct and assist voters in registering votes and casting ballots, respond to voting system error messages or temporary power failures, close the polls, print end-of-day vote totals, take down voting system equipment, transfer polling place results to central tally computers and tally final results.
** Comment: and be able to follow all required security procedures. Required systems and procedures should be simple enough for poll workers to be trained up on it in a reasonable
amount of time. **

March 30, 2007

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

ATTN: Voting Systems Review, 6th Floor

Enclosed are my comments on the Draft Criteria for the Top-to-Bottom Review of Voting Systems. Thank you so much for your effort to bring back integrity to our elections.

Comments on Draft Criteria of March 22, 2007 in:

> TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS
> CERTIFIED FOR USE IN CALIFORNIA ELECTIONS

Page 1, Title:

The Draft Criteria's title says:
"Electronic Voting Systems Certified"
while the first paragraph says:
"voting systems currently certified".
"Electronic Voting Systems" may be interpreted as excluded optical scan systems. All voting systems certified for use in California should be reviewed. Delete the word "Electronic" in the title.

Page 1, paragraph 1:

The first paragraph says:

> The goal of the review is to determine whether currently certified voting systems provide acceptable levels of security, accessibility, ballot secrecy, accuracy and usability under federal and state standards.

The draft criteria include sections/criteria for security, accessibility, and usability, but not sections/criteria for ballot secrecy and accuracy.

Pages 1, 2, and 4, use of word "standards"

Page 1, paragraph 1: "federal and state standards" should be "federal and state laws and guidelines".
Page 2: "voluntary federal voting system standards" should be "federal voluntary voting system guidelines".

Page 2: "Security Standards" ... "For purposes of these standards ..."
Page 4: "Disability Access Standards".
I would use "requirements" instead of "standards" in these three places. "standards" might have a legal meaning and requirements for setting.

Page 2 and 3:

"untraceable vote tampering" is defined and then used in 4 additional places. Vote tampering, whether traceable or not, must be prevented. This is especially true as the public is not allowed to look at the logs or other places traceable vote tampering might have left its mark. So, I'd recommend changing the definition to:

> "vote tampering" means preventing the accurate electronic recording of votes, or altering the record of votes, to

change the result of an election."

After changing the definition, change "untraceable vote tampering" wherever it occurs later in the document to "traceable and untraceable vote tampering" or just "vote tampering".

Pages 2-3. I. 1. Security Standards

I'd like a subsection d. which would apply to any part of the voting system not covered by a., b., and c. In particular, some optical scanners may just convey ballot images or ballot selections and not do any counting and may not be covered by a., b., and c. Also the voter access card enablers wouldn't be covered.

Page 3. I. 2. b. Source Code Review

This says "prior to, during or after completion of the risk assessment", but that is the only place "risk assessment" appears; i.e. it is not defined and therefore I don't know what this sentence means.

Also, in my opinion, it will be impossible to review all the source code of all the certified systems. Perhaps the paragraph should be rephrased to indicate partial source code review, as time and resources permit. The findings at the end of the process must make clear exactly how much source code review was done. We don't want a partial source code review with vendors claiming California proved the code is bug free and vulnerability free. Actually, they probably will whatever you do, but you should try to make it clear that your source code review is incomplete.

Page 5. II. 2. (f)

II.2.(f) states:

> (f) In the case of a DRE, the capability to permit a voter to verify electronically, through a nonvisual method, the information that is contained on the voter verifiable paper record copy of that voter's ballot. This requirement is satisfied by a method of nonvisual confirmation that draws the information provided to the voter from either (1) the paper record copy itself or (2) the same electronic data stream used to print the voter verifiable paper record copy.

II.2.(f)(2) is not sufficient. The Elections Code says that the voter may verify:

> "the information that is contained on the paper record copy" (19250(d))
> "the information provided on the paper record copy" (19251(a))

via a nonvisual means.

II.2.(f)(2) at best conveys to the voter the information the machine expects to be on the paper record copy, regardless of what actually is on the paper record copy.

There are many situations in which the paper record copy does not contain the proper information:

- if there is a paper jam
- if the paper was inserted backwards or upside down, as happened in Ohio
- if the printer runs out of ink or the ink supply is blocked
- if the printer/computer connection is faulty or the printer driver or printer firmware is buggy
- if there is malicious code to "game" the VVPAT

For how to "game" the VVPAT, see:

David Dill's paper, "VVPR Attack with Misprinted VVPAT", http://vote.nist.gov/threats/papers/misprintedVVPAT.pdf and Ted Selker's paper, "Security Vulnerabilities and Problems with VVPT", http://vote.nist.gov/threats/papers/vvpt.pdf for more info.

Actually, I'm not even sure what "the same electronic data stream" means. When the VVPAT is printed, the "electronic data stream" is not saved. If you mean recreating the data stream sent to the printer, that stream will contain printer control characters, so it can not be sent to an audio device. If you mean the data stream before it gets to the printer driver, this would not protect against malicious code in the printer driver or sending a different data stream to the audio device.

Page 5. IV. Usability

"respond to voting system error message" - these should be in comprehensible English, not just error numbers.

"print end-of-day vote totals" - this should be independent of other printouts; i.e. not on sealed VVPATs.

Counties should also be able to set up elections, e.g. ballot definition files, etc. to avoid problems like those with ES&S being so late in the last election.

I've heard counties using ES&S systems have to have ES&S in Omaha, Nebraska, program the firmware for their county's machines before each election. If that is true, the software for programming the firmware may not be in escrow in California and may not even be certified for use in Claifornia. That can be tested simply by testing creating a new election.

Not Covered in the Draft Criteria:

1. Ballot Secrecy/Privacy

An item needs to be added as to how well the equipment preserves the secrecy of the ballot, as required by the California Constitution.

The continuous roll VVPAT does not seem to protect the secrecy of the vote, since:
- anyone can observe at the polls (EC 2300 and EC 19362),
- each voter must audibly state their name before voting (EC 14216),
- anyone can request a recount of a precinct (EC 15620 and 15621), and
- anyone can watch the recount of the precinct (EC 15629),

Michael Shamos, Pennsylvania's Certifier of Election Systems, won't certify any continuous roll VVPATs due to concerns about the secrecy of the ballot.

This is an even worse problem in counties like Alameda County, where on election day, only the disabled will use the DRE. Last November, most of the DREs in Alameda County held only one or two votes. If the results tape for the DRE is posted as required by the Elections Code and only one person used the DRE, then that person's ballot is displayed.

2. Security - Testing if code is escrowed.

EC 19223:

> 19223. The Secretary of State shall conduct random audits of the software installed on direct recording electronic

> voting systems, as defined in Section 19251, to ensure that the installed software is identical to the software that has been approved for use on that voting system.

Although required, I doubt the random audit has been performed recently. To do this, take random machines from the Counties and compare the software to that in escrow. To make a true comparison, you must compary binary executables. According to "Voting System Requirements", 10/5/05, http://ss.ca.gov/elections/voting_systems/requirements.pdf, these should be on file with the Secretary:

> VOTING SYSTEM REQUIREMENTS
>
> Any new voting system to be considered for certification for use in California elections will be required to have the following features:
> ...
> 5. In addition to depositing the source code in an approved escrow facility, each vendor must deposit a copy of the system source code and binary executables with the Secretary of State. ...

There have been articles stating that ES&S installs a different version of the executable in each precinct, e.g.:

"ES&S Programming Is Unverifiable", by John Washburn,
http://www.washburnresearch.org/archive/ESSFirmware/ESS-Firmware-001.pdf

This can be tested by comparing the binaries and firmware on several machines used in different parts of a county or in a different county. If true, this would violate EC 19103. (a):

> No voting system may be used for an election unless an exact copy of the ballot tally software program source codes is placed in escrow.

3. Security - Code on removable media.

The security tests and code review should include testing whether there are binaries/executables/scripts or equivalent on removable media, or whether the machine would use such code if it were there.
If so, this is a security risk and should result in decertification.

4. Security - Testing mode

All testing should be done in election mode, not test mode.

5. Suitability/Usability - MTTF

The MTTF (Mean Time to Failure) in the VVSG would allow 10% of the machines to fail on an election day, where the machines are used for about 15 hours. This is far too many failures, putting stress on pollworkers and elections department staff. We must require a higher MTTF; a machine with a 163 hours MTTF may be suitable for a polling place at the elections department office, but is not suitable for offsite polling places.

6. Suitability - Calibration

Test how often a machine requires recalibration. Test to see if transportation affects calibration.

I don't think pollworkers should need to do recalibration. If that is the case, the MTTF of the machine with respect to calibration must be evaluated, and should be on the order of 100 hours or more, or this is not a suitable machine.

If pollworkers are expected to do recalibration as needed, the recalibration procedure must be simple. Otherwise, it fails the suitability requirement. After a machine is recalibrated, I would expect Logic and Accuracy testing to be redone. Is this required by the procedures?

7. Security - Storage/Sleepovers

How does this security review relate to how machines are stored between elections, transported to the polls, stored at election sites (often in public places), and so-called sleepovers with pollworkers?

8. Security - Early Voting and Absentee Vote Counting

For early voting, equipment must be secured for days or weeks after voting has begun. The equipment is probably left unattended overnights and weekends. Likely the equipment in the Registrar's main office is well secured, but the equipment in satellite locations is probably much less well secured. I have heard some counties have portable absentee voting stations on buses. Use conditions must spell out what security precautions are necessary.

Tabulating of absentee voting has similar problems when done before election day. Since the optical scan equipment is left unattended and vote counts are not allowed to be accessed until 8p.m. election day (EC 15101.), stringent security precautions are necessary to protect the vote. Since many counties have purchased new high speed scanners, it may no longer be necessary for them to start tabulating votes before election day.

9. Suitability - SOVC

In larger counties, the Statement of Votes Cast (SOVC) is huge. It should be simple for interested parties to access the numbers in the SOVC and put them in spreadsheets, etc. However, the SOVC is often only provided as a PDF file which can not be processed electronically. In Alameda County in the 2004 general election, the SOVC was 75 Megabytes, 6600 pages. Most of the data is just zeros, e.g. listing zero vote counts for Oakland precincts for a Livermore council race.

The SOVC should also be available in a more usable format, preferably as a CSV (comma separated value) file. In the current environment, I would say any system which can not do this would fail the suitability requirement.

If this can not be required as part of the current review, it certainly should be made a requirement for any future certifications.

10. Suitability - Recounts

The continuous paper roll VVPATs must be tested for how hard it is to count the votes by hand, as is done in the 1% manual tally and recounts.

Registrar Jill LaVine tested one vendor's equipment in early voting in Sacramento County. As a test, they manually counted the VVPATs for one of the early voting polling places:

> It took 127.5 hours to recount the 114 ballots, or approximately an hour and 15 minutes for each ballot.

(http://www.eac.gov/docs/LaVine%20Testimony%204-20-06.pdf)

This would fail the suitability requirement for any county with significant early voting or vote centers.

11. Accuracy - Optical Scanners

The optical scanners should be tested for accuracy.
Testing should include how dark and what sizes marks must be to register as votes, whether there is a difference when ballots are flipped end-to-end or upside-down or both.

Testing of this type is described in:

"Regarding the Optical Mark-Sense Vote Tabulators in Maricopa County"
by Doug Jones, University of Iowa.
http://www.cs.uiowa.edu/~jones/voting/ArizonaDist20.pdf

In addition, there should be testing with of various types depending on the types of choices on the ballot.

This is described in John Washburn's Election Integrity site:

"Testing Voting Equipment",
http://www.washburnresearch.org/ElectionIntegrity.html

12. Accuracy - DREs

There have been many cases of vote flipping. The DREs must be tested for vote flipping and whether the VVPAT agrees with the voters choices and with the electronic ballots.

13. Security - Logs, Data files

File of vote totals, logs, data files, etc. must be public. Otherwise there is no transparency and no real security. These files must be available electronically and at nominal, if any, cost.

14. Usability - California AVVPAT Standard

California develped a standard for AVVPATs. The June 15, 2004 version is no longer available on the Secretary of State web site. However, it is available via the "WayBack" archives at:

http://web.archive.org/web/20051124102850/http://www.ss.ca.gov/elections/ks_dre_papers/avvpat_standards_6_15a_04.pdf

This includes more details than the Elections Code, e.g. it says in section 2.4.3 that the Paper Record Display Unit must include an audio component.

This standard disappeared from the web without notice. Is that appropriate? Is this still a standard?

15. General Thoughts

I find it ironic that the Government Code, Secretary of State Duties, section 12168.7, wants the Secretary of State to develop standards for a "trusted system" for electronic storage of records:

> "trusted system" means a combination of techniques, policies, and procedures for which there is no plausible scenario in which a document retrieved from or reproduced by the system could differ substantially from the document that is originally stored."

The "no plausible scenario" seems a much stronger criterium than that accepted by most for election equipment.

16. General Thoughts

Once a system passes this test, what sort of upgrades will be allowed? Will minor upgrades be allowed without federal testing, or will any upgrades require compliance with the VVSG 2005?

Subject: Comments on your top-to-bottom voting systems review

Sent: Friday, March 30, 2007 4:55 PM
To: Voting Systems
Subject: Comments on your top-to-bottom voting systems review

Dear Sec. Bowen:

This is an addendum to my comments on your top-to-bottom voting systems review criteria.

In my original note, I indicate that the security review criteria were too narrow, but I did not say how I would have phrased them. Probably it would be best to broaden the criteria to cover "any attack or defect that could infringe the fairness of any election," and to include versions of "untraceable vote tampering" and "denial of service attacks" -- broadened as indicated in my original note -- as examples of the kinds of attacks that the criteria are meant to prevent.

Sincerely,

Subject: voting systems review

Sent: Friday, March 30, 2007 4:42 PM
To: Voting Systems

Subject: voting systems review

Dear Secretary Bowen,

Congratulations on your intent to do a thorough review and hold our voting systems to the highest standards.

The lack of security and accuracy of electronic voting machines is deeply disturbing and a direct attack on the basic tenets of democracy. Without citizen oversight of vote counting and without trust that our elections are tamper proof, we cannot have confidence that our government represents the voice of the people.

Since the NIST and GAO reports verify the unreliability of electronic machines for voting, and since a MIT/Cal Tech report declared hand counted paper ballots to be the most secure system, I believe those who say we do not have enough time before the 2008 elections to change do not understand that democracy is at stake.

I trust the committee reviewing the Sequoia machines that are used in Monterey County will read and consider all of the reports of problems with the Sequoia system around the country and that the top experts, like Jeremiah Aiken, Joseph Holder and Jim Soper, will be involved and consulted.

The optical scan machines and tabulators should also be reviewed for the potential for being intercepted.

Please make the results of the testing public immediately.

Subject: RE: Comments on your top-to-bottom voting systems review
Sent: Friday, March 30, 2007 4:40 PM
To: Voting Systems
Cc: Open Voting Consortium discussion list
Subject: Comments on your top-to-bottom voting systems review

Dear Sec. Bowen:

Attached are my comments on your top-to-bottom voting systems review criteria. These comments are not comprehensive of my concerns, since I know that others (e.g., the Open Voting Consortium) already have submitted comments that raise some of those concerns. Thank you for making this review a priority, and for soliciting public comments.

Sincerely,

---

1. The review defines the potential attacks upon voting systems too narrowly, thus omitting many attacks that can prevent an election from being conducted fairly. "Untraceable vote tampering" does not include, for example::

a. Attacks that attempt to deceive the voter about the proper contents of the ballot. These can include reordering the ballot, dropping candidates from the ballot, deleting or de-emphasizing headers between races, and possibly other more-subtle attacks. While some consider these to be "fringe" attacks that are unlikely to affect an election's fairness, I believe that the evidence rebuts this view. For example, Sarasota, Florida experienced a mysterious 13% undervote in the highest-profile race on the ballot, an event widely considered to have changed the race's outcome. [1] Many now attribute the undervote to officials' failure to program their DREs to adequately visually separate the undervoted race from another race. [2] Officials claim that the omission is innocent, but an attacker could program a DRE to wage an identical attack.

b. Attacks that attempt to affect a voter's choice of candidate, such as by selectively modulating the sensitivity of a touch-screen device, or selectively mis-aligning it, to make it easier or more difficult to select certain candidates.

c. Attacks that attempt to deceive the voter about the appropriate procedure. In one such attack, the attacker programs a DRE w/VVPT to selectively skip printing the VVPT, and also to skip displaying the corresponding prompts. When the voter finishes voting, the DRE records the attacker's selections, then prints a matching VVPT. The voter -- who might very well not understand the paper trail's purpose, or even know about its existence -- might well not detect that anything is amiss. And if she does, pollworkers may well attribute it to a "glitch". Similarly, an attacker might program a cryptographic DRE (e.g., VoteHere, http://www.votehere.com) to rearrange the procedure so that any cryptographic commitments are meaningless. Since very few voters are familiar with the proper procedure or understand its importance, this attack is likely to escape notice unless the machines are subject to rigorous random parallel testing in every election.

Similarly, "denial of service attacks[s]" is defined to omit the possibility of delay-of-service attacks. In these attacks, the attacker does not program machines to be "inoperable for voting," but instead programs them to lengthen the average amount of time required to vote, thus lengthening lines and leading to voter frustration and consequent vote loss. The attacker might lengthen voting times by introducing delays at various points (e.g., when inserting their voting card, when changing pages, when printing the VVPT, on the review screen, etc.) such that any individual delay seems acceptable, but so that the cumulative total of delays substantially lengthens average voting times. To see the effect, a simulation predicts total frustration-related vote loss of about 1% where 500 voters share 4 machines in a 14-hour voting day, voting takes an average of 5 minutes, and voters leave in frustration after a mean wait of 60 minutes with a 30 minute standard deviation. The vote loss rises to about 3% if an attack lengthens average voting times to 6 minutes, to about 7% for average voting times of 7 minutes, and to about 28% if average voting times reach 10 minutes. [3] Selective application of this kind of attack easily could skew an election.

2. Source code reviews are inadequate for many reasons. First, the source code provided by a vendor is not necessarily the same source used to build the voting application that is installed in machines on election day. Second, the tools used to build the voting application can introduce an attack program, even if the source is clean. [4] Third, the operating system, firmware, and even hardware can be engineered to load an attack program, even if the originally-loaded voting application itself is clean. [5] Moreover, the source code reviews do not permit members of the general public to scrutinize the source or to submit comments on it.

3. The criteria omit evaluation of electronic pollbooks. I do not know whether California has certified any electronic pollbooks (e.g., http://phx.corporate-ir.net/phoenix.zhtml?c=106584&p=irol-newsArticle&ID=774350&highlight), but if it has, the review has to cover them, since attacks waged upon them or using them can prevent an election from being conducted fairly. For example, an attacker might program a pollbook to impede voting by making it difficult or time-consuming to determine whether voters are eligible to vote, to falsely indicate that a certain voter is not eligible, or even -- in cooperation with an attack on associated DREs -- to stuff the ballot box by casting votes in the names of voters who did not vote at the polling place.

4. The DRE "voter verifiable paper record" criteria ((II)(2)(f)) are meaningless from a security perspective. An attacker can program the software to misrecord the voter's selections and to print a correspondingly-falsified VVPT while simultaneously presenting a "nonvisual confirmation" that accurately summarizes the voter's selections. This kind of system should be viewed -- at best -- as a means of assisting disabled voters to discover errors in their selections, and not as a security measure.

5. More generally, there also has to be a review of election procedures. Reviewing voting systems themselves is vitally important, but reviewing the procedures surrounding their use is just as important. For example, the state's mandatory 1% random hand audits are statistically insufficient to detect many potential attacks, even assuming that officials generally conduct them correctly (e.g, that they select the precincts to be audited publicly and randomly after the preliminary precinct totals are publicly posted). The number of precincts to audit should not be fixed, but should be based upon the apparent margin of victory -- closer races require more auditing. [6] Similarly, there have to be well-thought-out procedures for action when an audit discovers discrepancies, for when a voter reports a problem that could indicate an attack, and so forth. There is a tendency among some to dismiss problem reports as "voter error" or "glitches," or to "stick it out" with machines that are clearly performing incorrectly. This is inappropriate, and easily can lead to corrupted elections. For example, officials in Sarasota continued to use their DREs long after it became apparent that voters were failing to see the congressional race due to defective ballot programming. [7]

[1] http://www.cbsnews.com/stories/2006/11/11/cbsnews_investigates/main2174376.shtml
[2] http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061210/NEWS/612100869/-1/NEWS0521
[3] cheating_with_unreliability Matlab model; contact me for details.
[4] Ken Thompson, *Reflections on Trusting Trust*, http://www.acm.org/classics/sep95 , discusses this attack as applied to any kind of software.
[5] Crane, *Malware Loader*, http://vote.nist.gov/threats/papers/malware_loader.pdf.
[6] See, e.g., *The Machinery of Democracy: Protecting Elections In An Electronic World*, App.J., http://www.brennancenter.org/stack_detail.asp?key=97&subkey=36343&proj_key=76
[7] http://www.aclu.org/votingrights/gen/27476prs20061121.html (search for "early voting").

Subject: RE: Comments on Review

Sent: Friday, March 30, 2007 3:50 PM
To: Voting Systems
Subject: Comments on Review

Dear Secretary of State Bowen

I deeply appreciate your efforts to bring proper, open and fair elections to the state.

Please consider including a review of the registration database systems employed by the counties and the maintenance of the same. Electronic poll books are also highly questionable.

My daughter turned 18 in late October last year, making her eligible to vote. She used the CA SOS website to request a voter registration. The Los Angeles County registrar's office, thereafter sent her a pre-printed form only to be signed and mailed back.

This was mailed on Wednesday, 10/5/06. As the registration deadline neared, my daughter and I started contacting the registrar's office and found that she she was still not in the database.
I was told as late as on Monday November 6, 2006 they were still inputting thousands of registrations. Needless to say she voted provisional the next day.

40 days later we found out her vote was not counted. (as expected)
Worse yet, she kept receiving voter registration forms until just recently.

As of our recent Los Angeles City elections, she was still not registered. I had to yet again, call and complain - to both the County and the City. Subsequently, it appears she is now registered, 5 months after she requested to be registered. However, she never received a sample ballot for the City Election, as it was promised over the phone to me. Again, disenfranchising her.

Our experience is documented on democraticunderground.com which posts in our Election Reform Forum is attached herewith.

I am especially concerned that the county uses the Diebold registration database software which according to county documents is also "proprietary".

Considering voter registration problems being the most complained item on the EIRS system and other voting activist sites, this is potentially a huge problem.

For whatever it's worth.

Thankfully yours

A follow up on Voter Database

In the ERD News for 2/24, livvy posted "Public Monitor Reports Serious, Possibly Illegal, Security Breaches...". This is Ohio, Cuyahoga. As I have noted in my previous day News, the press releases by Diebold upon purchase of the Data Information Systems, Inc. (2003) indicated "VIMS are in use in Cuyahoga and Michigan, and throughout the nation and handles 14 Million voters". I wonder whether this software in LA also purged the 70,000 voters.

Nowadays it looks like the system is referred to as DIMS and or VIMS, but regardless of what it's called I think in light of this article below, as I feared, it is of utmost importance to truly scrutinize EVERYTHING.

http://www.votetrustusa.org/index.php?option=com_conten...

"The DESI voter-registration product (DIMS) has a "merge records" function with a hair-trigger and no "Undo" ability. This seems to have contributed to a number of voters being dropped from the rolls. The CCBOE has still not put in place any remedial processes and DESI has yet to provide a fix."

Mind you also e-pollbooks are Diebold products.

Concentrating on the end-user product of these vendors and the tabulation system leaves the integrity of the voter database in the dark without scrutiny and vulnerable at all times -

Also, from my previous post on the Feinstein hearings:

Michael Waldman of the Brennan Center thereafter (at about 1:51:00) comments about the auditability, and says, in the Lyndon Johnson' case, had there been no paper ballots, the stuffing of ballots would not stand out. Now, ranking member Mr. Bennett disagrees - to which I disagree, we have the signature pollbook (which by the way should never be made electronic either in my opinion) Bennett cites one Utah governor election, where they believe that a candidate was counted out rather than voted out. That the election official kept getting phone calls of how many votes they need.

Waldman then responds by saying, well you are talking about insider access and with that kind of access to tabulation systems machines can certainly be tampered with, such as placing a bug to be activated at a certain point...and it's completely undetectable..

Bennett cuts him off and addresses Schmidt & McCormack: Do you agree with that? - she (Schmidt)talks about having video cameras on the tabulation computer screen throughout the process and having to trust the election official.

McCormack: The point is, parallel monitoring by independent testers so you can not have a bug. All machines have an extensive logging system, so it can be tracked back, it (bug) is detectable.
http://www.democraticunderground.com/discuss/duboard.ph...

Same VoteTrust article link above, albeit in context of GEMS networking issues:

Unfortunately, the Windows Security Events log only shows one entry: cleared by an administrator on December 8, 2005. There were no security events relating to data security recorded at all in 2006. It appears that the manufacturer cleared this log and then configured it so that it would not log security-relevant events. This is unfortunate as it would help to piece together some of this puzzle.

Within our election process the officials seem to be piling on more and more vulnerabilities with each so called modernization/automation/innovation by dancing to the tune of the vendors and outsourcing what was once their function and responsibility.

Accountability? The complexity makes sure there is - None.

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=468433

The Dieboldizing of Our Elections

In Los Angeles County Ms McCormack has been staying the course towards recommending and implementing an all electronic voting system since she arrived here a decade ago. It is still underway. Prior to Los Angeles, she was Registrar in San Diego – and before that in Texas.
Los Angeles County currently has over 4 Million voters , certainly not an easy feat considering 4500 precincts and numerous different races, districts and Cities. However, automation and convenience for the registrar should not come at the expense of openness and verifiability of each vote cast.

I was under the impression that the InkaVote system was pretty decent. The switch from a punch card system in 2003 was rather smooth for the voter as it is in principle the same little box with holes where you slide your paper ballot precisely to match the numbers. The only difference is the little pen. It does not poke a hole, it creates a dot on the bubbles. This switch cost the county 3 Million. I still get my receipt. Fair enough. Meanwhile, elsewhere the controversy and problems of DRE's were raging and continues to this day.

According to various correspondences from Ms. McCormack to the County Supervisors, it is clear that she has wanted to install DRE's – the InkaVote is an interim solution. I believe that our County Supervisors have done a fairly good job of fending off the electronification of our end user voting system so far. The compromise, it seems, is to go slow and do this in phases.

Ms McCormack has consistently objected bills introduced in the State and urged County Supervisors to oppose bills that called to ban or require VVPAT DRE's. In April of 2004, in preparation of the 2004 elections the letter to the supervisors states:

IT IS RECOMMENDED THAT YOUR BOARD:
1. Approve the recommended position of OPPOSE regarding SB 530, SB 1723 and SB 1438.

The reasoning behind this opposition she says is that the Board has approved the touchscreen machines contract in 2002, (Diebold) of course her recommendation. The DRE acquisition at a cost to the county of 107 Million towards HAVA compliance, according to another letter. She cites the touchscreen systems to be the only units allowing the disabled to vote privately and unassisted and minorities can view the ballot in their language of choice.

Touchscreen early voting was installed in 2000 – hmmm the infamous 2000 Presidential elections. She cites not only the disabled and minorities but other voters, according to her survey of ten's of thousands of voters preferred the DRE's over the paper based systems. No attachments to support this statement is provided.
We can additionally glean from her comments that she was certainly no friend of our later ousted Secretary of State Mr. Kevin Shelley.

This measure would have the effect of ending the County's touchscreen early voting program until such time as system modifications are developed, tested and certified by federal and state authorities that would produce the specified AVVPAT.

This bill would, in effect, put into statute a directive previously promulgated by California's Secretary of State in November 2003 that requires:
- "...beginning July 1, 2005, no county or city may purchase a touch screen

voting system that does not include an accessible voter verified paper audit trail (VVPAT" and that

- "As of July 2006, all touch screen voting systems used in California, regardless of when they were purchased, must have a VVPAT that can be used by all voters, including the visually impaired..."

Now the DRE's and InkaVote or whatever system is the end-user part of the entire voting system, and therefore the most visible. The controversies elsewhere gave Angelenos voting on InkaVote, like myself, a false sense of assurance.
Unbeknown to me other "improvements' were long under way.

Los Angeles County, based on Ms. McCormack's recommendation dumped the IBM voter registration system that was in place since the 1970's citing maintenance costs per voter. The new VIMS, (Voter Information Management System) is a proprietary software which was installed in 1998. Interestingly this is a sole source no bid 5 year contract with a vendor, Data Information Management Systems.
The company currently services more voters than any other voter registration company in the United States, supporting information for more than 14 million voters

DIMS's software is being used according to the references below for 55% of voters in California as well as in Cuyahoga, Ohio and Michigan. In early 2003 Diebold has acquired this company. Red Flag? Diebold as of 2003 has had control of 14 Million voter registrations. The electronic poll books - those, too are DIMS inventions, a wholly owned subsidiary of Diebold.
These counties had a whole year and some to "improve" their voter registration database leading up to the 2004 Presidential elections. I wonder what caused the "glitch" or discrepancy of total registered voters reported by Ms. McCormack on October 18, 2004 to the SOS of 3,972,738 to the version of 3,901,106 upon certification of the election results? The purge of registered voters constitutes 70,000 people.

http://web.mit.edu/mit-rnr/www/lists/announce.w3archive...
bocc.cuyahogacounty.us/GSC/pdf/ elections/CERP_Final_Report_20060720.pdf
www.michigan.gov/documents/ Diebold_Cost_Detail_89491_7.pdf

Further, a bigger concern is silently brewing in an inaccessible room at the County Registrar's headquarters in Norwalk. It is the vote tabulation system. It was not long ago that citizen observers were refused entry to observe the computers tabulating the results by Ms McCormack. While it is true that starring at practically a box would not enlighten anyone as to the comings and goings inside that darn thing.
However, here are highlights from Ms McCormack's communication titled " Approve Sole Source Agreement with Data Information Management Systems for Continuation of Existing System Maintenance and Support Services of The County's Voter Information Management System", dated January 30, 2007.

Ms McCormack now has the authority to extend the contract at her or her designates sole discretion. (previously having to seek approval from the Board)
starting on page 76 of 132: Excerpts

Contractor shall provide Voter Information Management System (VIMS or System) Software, Interfaces, and related support and maintenance services to accomplish all of the Tasks and subtasks set forth in the Agreement and in this SOW. Such services shall include the following:
(1) Provide onsite support and maintenance services for VIMS.

(2) Develop, test, and implement software modifications and System enhancements to comply with requirements imposed by state, and federal statutes.
(3) Provide Interfaces to systems identified by County to automate and facilitate information exchange.
(4) Conduct training for database administration staff and end user whenever County requests such training.
(5) Develop both database-administration and end-user documentation whenever a new feature or function is implemented.

TASK 1 - SUPPORT AND MAINTENANCE SERVICES
TASK 2 - SYSTEM INTERFACE PROGRAMMING AND EXECUTION
TASK 3 - WIDE AREA NETWORK ACCESS PLAN
TASK 4 - CUSTOM PROGRAMMING MODIFICATIONS
Contractor shall use the standard RR/CC software set forth below when preparing Deliverables. Contractor shall provide Deliverables in a file format importable to the standard RR/CC software. RR/CC standard software is as follows:

- Microsoft Word 2000 - Word Processing
- Microsoft Excel 2000 - Spreadsheet
- Microsoft PowerPoint 2000 - Project Presentations
- Microsoft Access 2000 - Database Manager
- Visio Version 2000 - Illustrations, Flowcharts, and Drawings
- Microsoft Project 2000 - Project Manager

Contractor shall provide the analysis, design, development, testing, installation and installation testing, of software that will provide the Interfaces between VIMS and external systems identified by County.

Subtask 2.1 -Define and Develop Interface Software for Automated Ballot Layout (ABL) System
The Automated Ballot Layout (hereinafter "ABL") System consists of processes that define ballot styles, vote recorder assembly sequences, and political contest rules and descriptions. The ABL System programmatically produces the layout of official and sample ballot pages. The ABL System is currently hosted on a mainframe and the County is transitioning to Windows/Intel. A transaction process that shall send and receive data to and from the ABL System and VIMS in the same format and the same frequency as the existing interface process or a future process defined by County shall be developed by the Contractor. Contractor shall also build and document processing logic and map transaction files to RR/CC's existing interface or future files.

Subtask 2.2 - Define and Develop Interface Software for Candidate and Measure Filing System
The Candidate and Measure Filing System currently executes on a Hewlett-Packard minicomputer platform and County intends to replace it with a Windows/Intel based system. A transaction process that shall send and receive data to and from Candidate and Measure Filing System and VIMS shall be in a format identified and approved by County.

Subtask 2.3 - Define and Develop Interface Software for Election Tally System (ETS)
The Election Tally System (ETS) programmatically tallies election results for an election. The current ETS operates on a networked Intel client workstation platform using an internally developed tally system called "InkaVote". The County intends to replace it with a vendor developed system. A transaction process that shall send and receive data to and from ETS to VIMS in the same format and the same frequency as the existing

interface process or a future process identified by County shall be defined and developed by Contractor.

Subtask 2.4 - Define and Develop Interface Software for both the interim and permanent Statewide Voter Database
The CALVOTER System is the state of California's interim Statewide Voter Registration Database. The CALVOTER System executes on computers located in Sacramento. A transaction process that shall send and receive data to and from the CALVOTER System and any future Statewide Voter Registration System administered and maintained by the California Secretary of State shall be developed and implemented by the contractor.

TASK 3 - WIDE AREA NETWORK ACCESS PLAN SPECIFICATIONS
Contractor shall, upon County's request, submit a written report that contains specifications for a wide area network (hereinafter "WAN") including but not limited to (1) hardware requirements (2) software requirements (3) telecommunications requirements (4) routing protocols required (5) recommended network design and (6) network conceptual design. The written specifications shall make recommendations to meet the requirements listed below.

Contractor's written recommendations must include capability for a WAN such that: (1) Registrar-Recorder/County Clerk branch offices shall have full access to VIMS and (2) all of the City Clerks of Los Angeles County shall have limited access to VIMS. The WAN for the City Clerks shall allow for:

A. Capability to access the voter file, but not to edit the voter file.
B. Capability to access the full absentee voter system.
C. Capability to check signatures and an internal tracker so that the cities in Los Angeles County may be billed for signature look up but not for simply viewing voter files.
D. Capability to exchange polls and officers information.
E. Capability to send voter updates to the County system tied to automatically generated letter to voter to confirm.
F. Capability to add and access multilingual voter information.
G. Capability to add city/municipal voting history to individual voter files.
H. Capability to use electronic mail to flow documents or files to/from County system.

This contract extending now for 5 years with this wholly owned subsidiary of Diebold is a done deal.

No matter what legislation is introduced, a private vendor controls our entire election system. The so called safe guards at every point is a waste of breath and effort. The only guardian to oversee the technology in this case of Los Angeles County is in the hands of one person at the County Project Director.

In a letter to the appointed interim CA SOS McPherson supporting Diebold to be certified for use as accurate and secure, the following county Registrars have signed this letter on November 17, 2005:

William E Schultz, El Dorado County

Victor E. Salazar, Fresno County

Carolyn CRnich, Humbolt County

Ann K. Barnett, Kern County

Theresa Nagel, Lassen County

Conny B McCormack, Los Angeles County

Michael Smith, Marin County

Marsha A Wharff, Mendocino County

Kathleen Williams, Plumas County

Colleen Baker, Siskiyou County

Deborah Hench, San Joaquin County

Julie Rodewald, San Luis Obispo County

Mikel Hass, San Diego County

Hiley R. Wallis, Tulare County

Elaine Zimmel (? - can't read handwriting), Alameda County

A question to all these counties: do you use VIMS, too?

All this at a cost of hundreds of Millions of taxpayer dollars - is it worth it? For Diebold a resounding YES.

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=468282

§ 15483 Computerized statewide voter registration list requirements

I have not found one single bill addressing the single most complained voter problem: Registration related issues

HAVA mandated states to install computerized statewide voter registration systems - The only somewhat related bill was introduced by Colorado Congresswoman DeGette E-Poll Book Improvement Act of 2007 (Introduced in House)H.R.756.IH

A BILL

To amend the Help America Vote Act of 2002 to direct the Election Assistance Commission to develop and adopt guidelines for electronic poll books in the same manner as the Commission develops and adopts voluntary voting system guidelines under the Act, and for other purposes.

The Holt bill does not address these e-poll-books, and the DeGette bill does not address the inadequacies of the current EAC standards and requirements.

While this is commendable, if the underlying voter registration at the state is in such disarray as I have experienced with my daughter - voter suppression can and will occur even before election day. In the case of Los Angeles, this proprietary software is owned by none other than Diebold, which bought the firm that created it.
I found that these registration database compilation again - relies on outside vendors from software to, often, data input as well as outside vendors handling the mailings of county and state (incoming and outgoing) it would be only natural for us to scrutinize such practices.

FYI - On Friday, every voter in this household received a "Primary nominating and consolidated elections" booklet (City of Los Angeles) EXCEPT my daughter - yet again. So even going to the county registrar headquarters and witnessing the stamping of her registration with our own eyes does not guarantee your registration to be included in that wonderful electronic database. And of course the registration by mail failed in her case prior to that. I was concerned about her filling out another registration at the time and here it is in the section below "(iii) duplicate names are eliminated from the computerized list."

§ 15483. Computerized statewide voter registration list requirements and requirements for voters who register by mail
http://www.law.cornell.edu/uscode/html/uscode42/usc_sec...

Any thoughts?

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=467517

Los Angeles County voter registration saga continues

Surprise!

Some of you may remember our problems with my daughter's registration. Guess what! We received another registration!

A mailer from McCormack's office yesterday with a stamped message on top:

IMPORTANT NOTICE
Our records show that you cast a "provisional ballot" in the recent election. We are unable to locate your voter registration on our files.
You must fill out this postage paid form to vote in future elections.

emphasis theirs!

How peculiar, when you consider my daughter, under protest of mine, being told "just in case, for future elections", to fill out a second registration at the registrar's office in Norwalk (HQ) on November 6th, the day before the election. She had in fact mailed the signed registration on October 5th, 20 days before the cut-off date for the November 7th elections. "See", she said; "I am going to stamp it right now".

You may also remember, they told me that they were still inputting "thousands of registrations", (I assure you, among them my daughter's), and they expected this to continue through the 7th (election day)

You may also remember when among the County records I found that our voter registration data software is from a vendor that is now Diebold. But only did I find this out by pouring through the periodic reports McCormack files with the County Supervisors. You may also remember that I found, this process is partially outsourced to private vendors. (Mailing etc.)

Are we to take a registrar, and or it's vendors by their word? That all is fine and wonderful? With all the registration problem complaints across the country - we have to be more vigilant as to what happens at the registrar's office - before the elections.

Now that we have Ms. Bowen - I will write to her - that maybe we should send a post mortem inquiry to ALL voters in the state to see how many people had problems and if so what kind - only then can we implement changes - and prepare for a fairer election process in '08.

A third registration? So what happened to the: "I am going to stamp it right now" registration? This is beyond incompetence!

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=465855

Election Reform, Fraud, & Related News, FRI. 12/15/06 Utter Distrust

Voter Registration Database

My daughter was disenfranchised on her very first election experience through the incompetence of the Los Angeles County Registrar's office. It is official now.
I wonder how many more voted on provisional ballots which were through no fault of theirs not counted and dropped from the registered voters.
As of late November 6, 2006, I called the registrar's office, and they were still inputting data from the registrations they had received. Those would be new and address as well as name changes.
The preceding Friday, we were told still thousands to go. Worse, suggestion was made to fill another form, when in fact, California election laws would basically invalidate the first in my daughter's case, since the second one supersedes the first, this would make her registration date after the cutoff. There is no previous registration record since she turned 18 on 10/27.

My concern, from the beginning in my daily phone calls to the registrar was the possibility of a registration ending up not being logged in the database due to time constraints, man power or who knows what. And of course, leading up to the election, the periodic reports filed with the county supervisors by McCormack - everything is smooth and according to schedule.

How is it, that mailings sent out on October 5 all arrive at their destination but the registration of my daughter? Which is implied by the registrar's office. However, if in fact they were still inputting data of eligible registrants after the election, we can reasonably assume her second affidavit canceled the first, disqualifying her from voting, due to the cutoff date of October 23.

As I inquired whether her provisional vote counted - of course, they only have a record of her second registration. And even that, this registration was filled out on November 3, it shows she came in on November 9, no, then, "it shows" she came in on November 4, then, it was input on the 4th. However, I was assured at the time, that this second registration will not be input until after the election. Perhaps I am anal, but this misinformation and disarray at the office of the registrar is very disturbing to say the least. When We The People are to abide by the registration cut off date, I surely would like to see some integrity and competence on their side.

McCormack pointed out that on election night a total of 1,762,547 ballots were counted. This included 370,825 absentee ballots and 1,391,722 precinct ballots cast at 5,028 voting precincts throughout the county. However, those numbers represented only 87% of the total valid votes cast in the election. Another 270,572 votes were validated and tabulated during the four-week vote canvassing period. The following is a breakdown of the additional ballots that were tabulated countywide following election night:
160,558 Absentee ballots received the day before or the day of the election (by law, all absentee ballots received by mail must be signature-verified prior to removal from envelopes for counting).
110,915 Provisional ballots cast on election day by persons whose names were not on the voter file, requiring verification of each voter's eligibility prior to counting (NOTE: 88.3% of provisional ballots were validated and counted).

54,000 Ballots cast in the precincts on election day but which had to be re-made prior to counting (primarily due to voters casting ballots outside of their assigned voting precincts, but also due to torn/damaged ballots, etc.)

1,692 Ballots containing handwritten write-in votes for candidates who were not listed on the ballot which had to be checked and verified prior to counting.

Final election returns revealed a 52% voter turnout in Los Angeles County encompassing 2,033,119 voters. This compared to statewide turnout of 8,802,703 which represents 56% of the state's electorate. How Los Angeles County voters chose to vote - whether prior to or on election day - is shown by the statistics below:

1,501,736 Voted on election day at one of the county's 5,028 precinct voting locations, representing 73.9% of the total votes cast.

506,697 Voted by mail using absentee ballots, representing 24.9% of the total votes cast; and

24,686 Voted at one of the 17 early voting locations during the ten days preceding the election - representing 1.2% of the total votes cast.

(Emphasis mine)

http://lavote.net/GENERAL/PDFS/PRESS_RELEASES/12052006-...

This time, the total registered voters as reported on October 23 by McCormack to the State and the final certified number from the elections from LA did not differ. Should it not increase if they were still inputting data, if they were still verifying the registrations and gave themselves 10 days of mail delay (mailed and stamped on the 23rd) to be received, of which they were still inputting data on the day before the election?

All I know, my daughter's provisional was not counted, along with another approximately 13,000 provisionals if my math is correct.

The only way for We The People is mail in the registrations by certified return receipt requested or walk it in, or it is your word against theirs.

I utterly distrust this voting process from beginning to end. Do not be complacent with paper ballots. LA County uses paper ballots!

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=462545

Here is one with Diebold

I am actually on the County site - all contracts etc are there. Connie's weekly updates - I downloaded them all.

Here:

CONNY B. McCORMACK
Registrar-Recorder/County Clerk
COUNTY OF LOS ANGELES
REGISTRAR-RECORDER/COUNTY CLERK
12400 IMPERIAL HWY. - P.O. BOX 1024, NORWALK, CALIFORNIA 90651-1024

September 26, 2006

TO: EACH SUPERVISOR
FROM Conny B. McCormack, Registrar-Recorder/County Clerk

NOTIFICATION OF INTENT TO NEGOTIATE A SOLE SOURCE CONTRACT FOR CONTINUED MAINTENANCE AND SUPPORT SERVICES OF VOTER INFORMATION MANAGEMENT SYSTEM

In accordance with Board policy on advance notification of sole source contracts of $250,000 or greater, the Department of the Registrar-Recorder/County Clerk (RR/CC) intends to negotiate a non-competitive sole source agreement with the current contractor for continued maintenance and support services for the Voter Information Management System (VIMS). This contractor has provided exceptional maintenance and support services in a cost effective manner since the initial development and implementation of VIMS in 1998. The continuation of their services is paramount to the successful conduct of elections in the County of Los Angeles.

RR/CC is responsible for the registration of voters, maintenance of the voter files, precincting, absentee voting, petitions, and precinct officers/polls maintenance and the conduct of federal, state, local and special elections. On February 10, 1998, your Board adopted a five (5) year contract with three (3) one-year renewal options with Data Information Management Systems, Inc. (DIMS) for a client server environment voter information management system.

VIMS replaced the voter registration and election management system designed and developed in 1976 by Internal Services Department. This system operated on the County's IBM mainframe computer system and was cost prohibitive to continue at an average annual cost of $1.05 per registered voter, compared to the greatly reduced VIMS annual maintenance cost of $0.07 per registered voter. In addition to cost savings, VIMS enabled increased reliability, operational efficiencies, service delivery and improved automation of functions. With VIMS, the County was able to grant full on-line access for VIMS Election System use to City of Los Angeles in 1999 and City of Long Beach in 2004. These partnerships with VIMS and the cities have helped to improve the quality of the voter data, pollworker and polling place data used by all jurisdictions.

Each Supervisor
September 26, 2005
Page 2

In 2003, DIMS became a wholly owned subsidiary of Diebold Election Systems, Inc. DIMS currently provides voter information management systems for 38 counties in California, which represents 52% of the registered voters in the state of California.

The current contract will expire on February 9, 2006. Due to proprietary software issues, complexities with managing voter information system and mission critical need for uninterrupted services, DIMS is the only source that can provide maintenance and support services for VIMS.

Unless otherwise instructed by your Board within two weeks, we will proceed to negotiate the sole source contract with the current contractor.
CBM:NU:rl
c: Chief Administrative Office
County Counsel
Chief Information Office

http://lacounty.info/omd/q3_2005/cms1_034371.pdf#xml=ht...

Well combining the Diebold voter data contract with the PSI mailing

I think we have a group of not so friendlies running our elections and registrations.

All tied to Diebold

Press release of DIMS purcahse in 2003
http://www.diebold.com/news/newsdisp.asp?id=2926

and I am so uninformed, anyone knew this? The signature is verified by their software, which tolerance level can be adjusted?!

http://www.bbvforums.org/forums/messages/1954/8542.html...

Congratulations LA for a wonderful voter registration system :sarcasm:

Report revised March 20, 2005

Problems with Diebold DIMS Voter-Registration System

Through personal observations, analysis of DIMS reports or data extracts, and discussions with Cuyahoga County Board of Elections employees, I have documented the following problems with the Diebold DIMS Voter-Registration System and the data maintained within DIMS system.

1) DIMS allows the entry of bad addresses (incorrect street names). These bad addresses can be entered without notification by the system that the street name is misspelled. Only later are these bad addresses flagged as "Fatal Pending." They should be flagged at the point of data entry, or, better yet, "selected" from a set of valid county street names. Many of these "fatal pending" individuals were denied their vote because of data-entry errors of their address. (See "Fatal Pending" analysis at--
http://ohiovigilance.org/Counties/Cuyahoga/Analysis/Cuy...)

2) DIMS doesn't have a good means of preventing duplicate records for the same individual. According to a BOE manager, the system is "not very forgiving." I saw numerous examples of duplication in the poll books as well as in data extract files.

3) When I went to vote absentee, the clerk tried to find me "in the system" by my name, but couldn't. She then asked for my address, and was able to find me by my address. She related that she had to resort to that "workaround" fairly often (i.e. look up people by their address rather than their name) and said that the system was new (implemented in September 2004) and still had bugs. When I asked if they were going to fix the bugs before the election, she replied "Oh, no, there isn't time. They'll have to fix them after the election."

4) Many people tried to locate their correct precinct through the Cuyahoga Board of Elections website, but were unable to do so. I tried entering my address several times, without success, before finally locating my correct precinct. Others weren't so lucky. The data used for the website "precinct lookup" had to come from DIMS, the voter-registration system.

5) I found a handful of duplicate precincts in the database—same precinct name, but different internal precinct numbers.

6) There are several tables, where "would-be voters" are maintained: (1) valid voters, with status of "A" (active) "I" (inactive) or "C" (cancelled) ; (2) provisional voters—voters who voted provisionally on election day, probably because their name failed to show up on the voter-registration poll books; and (3) "fatal pending" individuals -- people who were ineligible to vote because there was something wrong with their registration (bad street name, missing date of birth. The DIMS database design allowed the same person to be located in two or three of these tables, each with slightly different spellings of name or address. (See "Fatal Pending" analysis at--
http://ohiovigilance.org/Counties/Cuyahoga/Analysis/Cuy...)

http://ohiovigilance.org/Counties/Cuyahoga/Analysis/Cuy...

Oh boy:
I remember this map by

By the way, who was the database company that began handling voter registration for Cuyahoga County, Ohio in 2004? It was Diebold. The county flash-cut over to the new Diebold/DIMS electronic-registration system in September.

The map shows that minority voters in Cuyahoga had to overcome more hurdles to cast a vote; were more likely to have to vote by provisional ballot. This map reflects provisional ballots accepted and counted, by census tract indicating the racial composition; these are not rejected votes, they are 'higher hurdle' votes because voters' names did not appear on the electronic registration rolls.

http://www.dailykos.com/story/2005/3/17/02212/3566

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=458059#458161

Los Angeles registration issue: Help

Edited on Wed Nov-08-06 08:43 AM by rumpel
Before I even go to the subject of my "lost" "damaged" "whatever" status of my daughter's registration, can someone explain these number discrepancies, yet again?

On Oct 3rd I downloaded the county registration statistics from the SOS site for Los Angeles the total number as of last updated (according to the site)

is: 3,869,304 out of 5,703,455 elligible

The final registration number as of October 23 deadline - finally updated prior to Nov 7 at the SOS site says:

is: 3,914,138 out of 5,708,463 elligible

As of this morning, McCormack shows a chart of the registration info (which, some of you know, when registration data were still being entered at Norwalk late Nov 6, to be

is: 3,899,397!

Which means the SOS added 5008 new eligible voters from September 8 through the deadline

Which means in LA registrations added at the SOS is 44,834

Which means McCormack did what to the 14,741 presumably new registrations?

here are the links
Los Angeles:
http://rrccmain.co.la.ca.us/0016_stat_Frame.htm

SOS:
http://www.ss.ca.gov/elections/elections_u.htm

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=457283

Now I am really concerned

Edited on Mon Nov-06-06 11:49 AM by
You may recall at the Los Angels County registar's headquarters office we were told to fill out another form.

look what I found! Legal minds please interpret, and tell me it does not say what I think it does!

§20108.60. Duplicate Registration Records. (a) Beginning January 1, 2006, the Secretary of State shall conduct weekly checks within the Calvoter statewide registration list to identify potential duplicate registrations for the same voter within that list, based on established rotating criteria. Upon identification of potential duplicate registration records, the Secretary of State shall automatically send an electronic notice to the county with the record that has the oldest date of registration.
(b) Within five (5) business days of receipt of a notice of potential duplicate registration the elections official shall take all necessary steps to determine whether or not the registration record is a duplicate of an existing newer registration, and if a duplicate registration is confirmed, shall cancel the older duplicate registration and submit a registration update file or full load file to Calvoter in accordance with Section 20108.15 and Section 20108.40.
Note: Authority cited: Section 12172.5, Government Code; Section 2124, Elections Code. Reference: Section 14310, Elections Code; Section 303, Pub. L. No. 107-252 (2002) 116 Stat. 1666, 42 U.S.C. § 15483.

which means we cancelled her eligibility to vote tomorrow?

info from:
http://www.usdoj.gov/crt/voting/hava/ca_moa.htm

for others who would like to check on the registration database system for their state it's here:
http://www.electionline.org/Default.aspx?tabid=288

problem is she is not in the database yet.

She mailed in the voter registration more than 3 weeks ago and they still do not have her in the database.

The County as of Friday, last week told me that they are still inputting data (thousands) and expect to continue through the 7th!

So while they are tallying the results - they may not have input all registrations into the database - and when they are reviewing her status as a provisional ballot voter by law, does it not mean her original registration has to be cancelled?

question is, since they are still inputting thousands of data

as we speak - the mailed in registration will be cancelled out by the on site registration which was stamped on the spot, Friday - but will not let her vote in this election - only future elections? Should the mail-in registration still be in the process of being entered into the database. She just turned 18.

The actual registration was made on the SOS website - so the registration came pre-printed with her information, requiring only additional sections including signature.

So the SOS must have her request in the database.
The county has not verfied or placed her in the database. Why out of all mailings does it take the USPS over 3 weeks to make it to the County registrar. It is there - unless something weird is going on.

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=456741

The result of my trip to the Los Angeles County Registrar with daughter

Edited on Sat Nov-04-06 12:11 AM by
Utterly useless!

The Norwalk HQ is only 30 some miles from my home. We left at 3pm, were stuck on the 405 and the 105 and again on the surface streets. We had 15 minutes until they closed for the week.

When we went up to the 3rd Floor, we were told to follow the red line drawn on the floor. The HQ still provides Early Voting and the signs are all geared towards that. The hallway is very narrow and right before we reached the room, we noticed a chair and some people standing around. It is a very short offshoot hallway, and to my surprise they had set up 3 Diebolds right in that small hallway, lined up with the backs towards us.

There were very few people in the waiting room or service area, and all the windows for other types of registrations were already closed or at least unmanned. There were several employees beyond the counter at their computers chatting and relaxed, and the man standing by the counter immediately started serving a young mother with her baby, who shared the elevator with us, but came to vote.
The place seemed...totally in a slumber mode.

We walked up to another window to tell the lady that my daughter is still not in the database, even though we mailed it now over three weeks ago, well before the October 23rd deadline. So she went to check on her computer. While she was checking, I had ample time to look around and saw maybe 2 more people walk in to vote. They checked in, and after verification they received a computer card and left the room. A sole test voting machine is placed near the check-in window, and I was thinking - so this is the infamous Diebold unit, and it proclaimed it's name as the most prominent and memorable as the rest appeared quite flimsy and unimpressive.
I noticed a small porcelain bowl, which is probably normally used for cereal, oatmeal or grits, on the counter and above it: "Please return cards here". No one really watching - no one really nearby, but sitting quite pretty with blue design bands near the top.
And my mind says: Did I not just post an article that some cards were missing....yes- in Tennessee.

The lady returned to confirm my daughter was not in the database. They are still, and will be inputting data now even through the 7th!
She was certainly unclear about the printing of the poll books, but assured me "they have a way." She stopped short of telling me: "what way". By the time I got to question her about the day of polling and her possibly not being in the poll book or whatever "other way", of course the suggestion was "provisional".
"I don't want her to vote "provisional", I complained. By then, two other guys walked closer to listen in and all three of them suggested we vote right there and then and she can use the provisional. We repeatedly declined and I made clear we Will not vote on those machines either.

However, what I found out is that the ballot (when paper is requested) is on InkaVote. It is not on "provisional", as the SOS's e-mail stated and we feared, at least in LA County. As I turned around, I saw three InkaVote units along one wall, with their backs into the room and 2 or 3 more Diebolds.

In any event, there is nothing that can be done until they complete the inputting of data, not even figure out whether they received it or not. The registration receipt stub is

worthless - the number imprinted is worthless - unless they have in fact put her into their database.
So, my daughter is now freaking out that all of her information is floating around somewhere lost between the mailbox right by our house and who knows where or lost inside the registrars office. She now wants to change her ss#. "Child, and ss# is for life". :)

They suggested she fill out another registration to make sure she can vote in the next election. I opposed it, as there would now be 2 numbers, which could cause problems again.
"No", she assured me, "it will not be recorded until after the 7th".

That sent shudders down my spine, as I glance over to those employees sitting at their computers, chatting quietly and their computer screens have not really changed one keystroke in all the last 20 minutes we have been there- Could it be equally slow wherever they are inputting the data, I thought? If they do not complete the data input on even several hundred - those are the people, come Tuesday, who will be surprised having to vote on provisional - and ballots rejected thereafter during counting? There is no 1% audit of "provisionals", McCormack said. The *pile.

"Are you sure, there will not be any confusion?"
By then the other 2 employees also chimed in and my daughter filled out another one right there.
"This one", she said, "I make sure, and see - I am stamping myself." Little solace, I thought.

On the way out, I glanced into the small hallway with the machines. There was a man voting alone on the very last machine. The man sitting in the chair, had his back to the machines but facing the foot traffic = us - and was preparing to read.

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=456427

Election Reform, Fraud, & Related News, FRI. 11/3/06 Power To The People

The concerns surrounding this election is large and personal. Back in 2004, I was one of many here trying to help scrutinize the raw data. I downloaded the election results data as reported on the Secretary of State website, which was broken down into counties and compared them with the registration data base also posted on the site. I continued updating this until all counties posted certified results.

Oddity that stood out was the fact, that in an overwhelming number of counties people voted for Barbara Boxer, however the same people did not seem to have voted for Kerry according to the results. Why?
Further, the final registered voters posted by the Secretary of State's website for my county, Los Angeles, did not reflect the same number later posted as final and certified by McCormack, registrar of Los Angeles. There were 70,000 less voters registered, as previously stated on the SOS website.

This year, my daughter has turned 18, just in time to vote. She has been wanting to vote now for 2 years now, patiently waiting to have a say in the process.
She did what all new registrants and people changing addresses do. Requested a registration form and mailed it in, kept a stub. The registration was mailed three weeks ago.

As of yesterday, she was still not in the database. I was told, the county is still inputting thousands of registrations, according to that particular division, into the database. Are they going to finish in time?
So, today, I will have to drive an estimated 45 minutes according to mapquest, which implies no traffic, (highly unlikely) to Norwalk, and assert her right to vote. What happens, will remain to be seen.

However, the bigger picture here is, are people being denied the right to vote, because of ignorance, incompetence or apathy at the registrar's office? Did they not project a high rate of requests and are understaffed? Are they by "error", disqualifying registrations? I did not have the impression that people answering the phone, knew much about election laws or anything at all. So how are they going to answer voters questions?
Is this business as usual, at the registrar's office? and is this leading to people, who are absolutely within their right to vote, denied a vote at the polls on Tuesday 2006, is this what happened to the 70,000 in 2004 in Los Angeles?

What is going on? When are they printing the poll books, are all these people, who are yet to be placed into the database going to be on an addendum sheet or a separate book? Are they going to have to use provisional ballots? I will ask them this, when I go and will report back on this.

The Secretary of State, (at this time, McPherson, who, as in my previous posts of his e-mail responses tend to delegate his responsibilities to each registrar), and certainly the registrars have a duty to inform us in a professional manner as to how they are handling the elections, from the registration intake to the final certification. We have the Sunshine Law, and everything they do should be made available for the public to see and be informed about.

Let's all cover each others' back, I care for your right to vote, I care for my daughter's right to vote just as I care for my right to vote, and have them counted.

To all candidates:

As I cast my vote for you to act as an elected official, I expect you to make decisions and suggestions based on the highest principles of benefiting All that harms no one.
You are to uphold the US Constitution in it's entirety.
As a public servant, you vow, you will leave your self-interests behind, and you understand that I will hold you accountable, if you breach your vows to me for my vote.

Power To The People

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=456337

CA: My daughter is voting for the first time and has not received

confirmation of her registration.

The phone numbers 800 and regular (posted on the SOS site), as well as the number posted on the lavote.net are not working!

This is incredibly incompetent!

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=454543

Update

Edited on Wed Oct-25-06 02:35 PM by
The 800 number DID work today, albeit there was a long wait and listening to repeated "you can vote early" until 10/25 etc.

Perhaps - their "computerized" phone system shuts down when it's overwhelmed as well as for a good nights sleep....

This is what my daughter did;
4 weeks ago, she registered online at the SOS website
2 weeks later she received the hard document from the LA County Registrar, to fill in and sign.
Exactly 2 weeks ago she mailed it back, and properly retained the stub with a number -

As per my phone call just now, the computer does not show the Registrar having received the signed document. Neither by name nor by the stub number does she come up. However, I am told, it may be still processing: in which case it will not show up in the computer. Suggestion was made, to call back on Friday or Monday.

I asked what to do, if the mail is lost.
Answer: Hmmm - I don't know.

So, I am going to bug them again.

Aside from this problem - does this mean we have a surge in registrations and they are overwhelmed? That's good. :)

Thanks for all of your suggestions!

on edit: an afterthought - considering the incredible number of registration related complaints in 2004, is it possible - that the SOS enters the registrations as they received it in the total tally on their website. But subsequently, the county through delays, for "whatever" reason, failed to confirm those registrations (in 2004, 70,000 voters) ?
Is that how the discrepancy occurred? Is that how 70,000 voters were disenfranchised in LA in 2004?
People not realizing - just waiting - not complaining - just trusting and then giving up?

Perhaps something to look out for...

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=454543

Election Reform, Fraud, & Related News, FRI. 2/2/07

Several points today to report...I just report what I got (don't shoot me) you may not like some of it or the source

However, it is of great importance to lay it all out there and discuss as we prepare for 2008

First, again - the continuing saga of my daughter's voter registration.

On Tuesday January 30, 07 my daughter received a Birthday Card from the Secretary of State, "Bruce McPherson"! How sweet

You change your socks every DAY
You change your ringtone every WEEK
You change your calendar every MONTH
You change your New Year's
Resolution every Year

You just turned 18.

Now on

Election Day,

you can change California

Happy 18th Birthday

REGISTER AND VOTE
:eyes:

and it is a registration card. Aside from the unimpressive "poem" or whatever it is supposed to be, the exact mailing date of this registration form is impossible to determine as with many mailers, "first class mail, US postage paid and permit # " pre-printed.

The problem is, my daughter turned 18 on October 27, 2006, and the appointed Mr. McPherson was voted out of office on November 7, 2006, and just last month our new Secretary of State was sworn into office.

In addition, she started the registration process on the Secretary of State website in September 2006, which later referred it to the Los Angeles County Registrar, which sent her a pre-printed registration - pretty much only to penn her signature and mail back - which supposedly never arrived - she filled out another registration at the County Registrar's office - only for her to receive a notice in January - that they noticed she voted "provisional" urging her to register yet again- and now this?

Who handles these mailers? Which subcontractors? Is this why voter registrations are so screwed up? Granted, we have problems with USPS - any mail handling division or subcontractor needs to be audited! This is now beyond anger or ridicule... it is representative of mismanagement of grave concern.

http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=203&topic_id=466392

Subject: RE: Public Comments re Draft Criteria for Top-to-Bottom Voting Machine Review
Sent: Friday, March 30, 2007 3:49 PM
To: Voting Systems
Subject: Public Comments re Draft Criteria for Top-to-Bottom Voting Machine Review

TO: Secretary of State Debra Bowen March 30, 2007

RE: **Public Comments re Draft Criteria for Top-to-Bottom Voting Machine Review**

I am a California attorney who has also served as a technical observer of the voting process at the Los Angeles County Registrar of Voters' office in Norwalk for the Los Angeles County Democratic Party in the period surrounding the June 2006 primary election. I advised technical representatives of the Democratic and other parties and brought a brief and unsuccessful lawsuit (*Anderson et al.* v. *Conny McCormack,* Registrar of Voters of Los Angeles County) seeking a court order requiring that the Registrar remove duplicate computer equipment from the rooms in Norwalk where the primary vote would be counted. I am also active in politics and am President of the Westwood - Westside Democratic Club. I have been a poll watcher.

1. First Paragraph under Draft Criteria:

Your review should – indeed must – include the **Micro Tally System (MTS)** used by Los Angeles County. That it was allegedly developed "in house" by L.A. County doesn't mean its hardware or software is safe for use. It counts more votes than any other system, and it may or may not have ever been certified. It should meet the same criteria as the commercial systems.

2. Under SECURITY/ 1. Security Standards, paragraph a. DREs., fourth line and at all other places where the words "untraceable vote tampering or denial of service" appear (see below), the words "traceable or" need to be inserted before "untraceable." OR you should remove the term "untraceable." That a method of hacking the equipment or software is traceable doesn't make it acceptable. Recounts are expensive and time-consuming, and courts are reluctant to overturn election results. Politicians are reluctant to challenge results because they may be regarded as "sore losers." Courts might also be unwilling to issue an injunction that would delay reorganization of a legislative body for days, weeks or months or effectively deny a district of representation for that period. While untraceable vote tampering is worse than traceable tampering, we must take reasonable steps to stop all vote-tampering before it can occur.

3. **Under SECURITY/ 1. Security Standards, paragraph b. Vote Tabulating Devices:** insert "traceable or" before "untraceable vote tampering" or remove the word "traceable" for the reasons set forth in paragraph 2 above.

4. **Under SECURITY/ 1. Security Standards, paragraph c. Ballot Tally Computers and Ballot Tally Software:** insert "traceable or" before "untraceable vote tampering" or remove the word "traceable" for the reasons set forth in paragraph 2 above.

5. Under SECURITY/ 2. Security Testing. Paragraph b: Source Code Review. Add examination of the source code of the "operating system" as well as any application software even though the "operating system" is claimed to be a standard commercial or noncommercial one such as Windows or Linux. While examining that code raises copyright, trademark and/or patent issues, your technicians can at least compare files with those in genuine copies obtained from other sources. If the files' names, sizes and dates are the same as a genuine copy AND your experts can swap files between the copy provided by the vendor and copies obtained commercially, then there might not be any tampering. Perhaps you could get some help from Microsoft.

6. Under SECURITY/ 3. Security Findings: insert "traceable or" before "untraceable vote tampering" or remove the word "traceable" for the reasons set forth in paragraph 2 above.

II. ACCESS FOR VOTERS WITH DISABILITIES.

1. Disability Access Standards. ...

2. Disability Access Testing – subparagraph (e) Add "and earphones" after Privacy curtains or shields, so that it reads: (e) Privacy curtains or shields and earphones that effectively prevent others from observing or hearing the selections of a voter using such features as audio output, simultaneous, synchronized audio and visual output, [etc.]." Earphones are the only device that will effectively limit sound over short distances. Replaceable paper earphone covers could be used for sanitary reasons.

3. Disability Access Findings. Here and in each of the remaining sections (III, IV), the draft gives the Secretary of State the power but not the obligation to immediately initiate the process to withdraw certification by using "may" instead of "shall." While I can understand why one might draft it this way, this document will set a precedent. A court would be more likely to enforce these rules if the Secretary of State were required to "immediately initiate the process to withdraw certification" of non-complying voting equipment, firmware, software or system upon finding the stated preconditions.

III. ACCESS FOR MINORITY LANGUAGE VOTERS.

See II, item 3.

IV. USABILITY FOR ELECTIONS OFFICIALS AND POLL WORKERS.

See II, item 3.

WIRELESS CAPABILITY

The draft does not mention the proper role, if any, of wireless capability. The safest systems would not have it. Is it necessary? If not, it should be banned from all certified equipment and systems. In no case should a system have any more wireless capability than it needs to do its job.

ELECTRONIC SIGNATURE COMPARISON EQUIPMENT

This equipment must also be tested. Any voter who is denied anything as a result of a negative finding must be promptly notified so that he or she can re-register with a more current signature. Also, no machine or system should kick out a disproportionate number of voters of any political party or of decline-to-state voters.

Exact matching should NOT be required. People are not always consistent in using a middle initial, and it is common for people to drop "jr." after the parent dies or add "Dr." after qualifying for it. These minor changes should not deny anyone the right to vote.

Again, the Registrar could notify the voter of the difference, ask for a reply and change its records if needed.

I have read and support the suggestions of   and
Sincerely yours,

Subject: RE: Top to Bottom Review
Sent: Friday, March 30, 2007 2:50 PM
To: Voting Systems
Subject: Top to Bottom Review

To: Debra Bowen CA SOS

I voted for you because you appear to recognize that the software dependent e-voting systems are not a secure or transparent method to use for our elections in a democratic nation.

has just testified before Congress and advised them that DREs with or without a VVPAT are UNACCEPTABLE FOR USE IN A DEMOCRACY. Do you know of any one who has better credentials who can legally refute his statement? If you do please present their argument, or immediatly decertify all the software dependent machines.

The NIST declared in their recent report, Jan. 2007, that they COULD NOT DEVISE A TEST TO PROVE THE TALLIES ARE ACCURATE ON ANY SOFTWARE DEPENDENT MACHINES. They stated that the DRES should not continue to be used and that paper rolls should not be used on new machines. You should be aware of this report. THESE TWO STATEMENTS ALONE SOULD BE ADEQUATE EVIDENCE TO IMMEDIATELY DECERTIFY ALL THE SOFTWARE DEPENDENT EQUIPMENT IN CA.!!!!!!

Ciber was found by the EAC last AUG. to have failed to provide proper test records and were suspended from continuing to test. We believe this testing to be irrelevant and inconclusive to begin with, however our Sequoia machines were tested by Ciber and we therefore believe they shoud be immediately decertified.

While has determined that the software vulnerabilities he has acknowledged are unacceptable in the touch screen DREs, he has failed to heed the warning of the GAO Report of 2005 which stated that it is "unrealistic and impractical to expect mitigating security measures to protect our election system from manipulation and fraud."

I would advise that it is not only UNREALISTIC but IMPOSSIBLE and an INSULT to the American citizens to make any attempt whatsoever to attempt to provide protection for this machinery from fraud or manipulation . I would remind you that the CA CODE 19205 requires that the voting system be" free from fraud and manipulation."

The mitigating security measures devised by McPerson are a coverup for the use of equipment that is ABSOLUTEY an assult on the integrity of our election process. Please STOP THE CHARADE.

SAVElections Monterey County is an action committee sponsored by the Womens International League For Peace and Freedom. Members of SAVElections Montery County have called for the removal of all software dependent e-voting equipment. We are circulating a petition which demands that this equipment be replaced with paper ballots hand counted at the precinct level. We have the support of manyhundred of concerned individuals who share our call for a ban on all this equipment in CA.and the nation.

We are working with other citizen activist groups in CA to remove software dependent e-voting machinery throughout the state and across America.

Please hear our plea, and use your authority to return our democracy to the people. Our elections are now under control of the vendors who supply the machines and anyone who has access to the software. As you well kno, anyone who has access to the software has THE POTENTIAL TO MANIPULATE THE RESULTS OF AN ELECTION WITHOUT LEAVING A TRACE OF EVIDENCE.

Professor Appel of Princeton U. has demonstrated on the Sequoia machines he purchased on e-bay in March 2007 that these machines can easily be hacked WITHOUT LEAVING A TRACE OF EVIDENCE! Since there were at least 100 more machines offerd in that sale I would suggest that there are plenty of others who hve now had the opportunity to practice hacking these machines.

Since you must proceed with your review please engage the following experts to review the Sequoia machinery. Jeremiah Akin-Joseph Holder-Jim Soper. We believe their review will be accurate. Also please make results of all test public immediately.

Please review WinEDS/BPS Application .
We specifically request the results of this Ballot Printing Software which is being purchesed by our ROV.

Thank you for your consideration of our request. We would appreciate an acknowledgement of this letter.

Subject: RE: Comments on Voting Systems Review
Sent: Friday, March 30, 2007 12:24 PM
To: Voting Systems
Subject: Comments on Voting Systems Review

Dear Secretary Debra Bowen,

ATTN: Voting Systems Review, 6th floor

Your review of voting systems will have world wide ramifications, not just in California. Therefore it is important that the most effective review is done to ensure the integrity, dependability and reproducibility of the systems used in the voting process.

There are two major criteria, **dependability** and **reproducibility**, which are missing in the proposed "Top-To-Bottom Review of Electronic Voting Systems Certified for Use in California Elections".

"In computer science, **dependability** is defined as:

> "*[..] the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers [..]*" [1]

Dependability includes the following attributes of a computing system [2]:

- **Availability**: readiness for correct service;
- **Reliability**: continuity of correct service;
- **Safety**: absence of catastrophic consequences on the user(s) and the environment;
- **Security**: the concurrent existence of (a) availability for authorized users only, (b) confidentiality, and (c) integrity."

(http://en.wikipedia.org/wiki/Dependability)

"Reproducibility ... the ability of a test (***e.g., voting result)*** or experiment to be accurately reproduced, or *replicated* (***even in the presence of external interferences, e.g., electrical interference, cosmic rays, power outages, etc.,***), by someone else working independently."

(http://en.wikipedia.org/wiki/Reproducibility)

In particular,

1) Voters need to be assured that in case of hardware or transmission failures while casting one's vote, that his or her vote is not lost, re-allocated, misplaced, duplicated or missing in the overall tally.

a) In the case of a failure, e.g., a flipped bit in memory or logic latches caused by electrical interference (e.g., arc welder next door), energetic cosmic rays (during solar flares), etc., that could change a "yes" to a "no" or a "0" to a "1" or vice versa in any of the software or hardware decision logic or numerical values or characters stored in memory; you need to have error detection and correction logic built into the hardware, software and human factors design to mitigate the risks of these kinds of errors.

b) If necessary, in case of an internal or external failure (e.g., loss of power during startup or shutdown or transmission of results, etc.,) or detected but uncorrectable error, the voter must be allowed to complete his vote by some other process which may include moving to another voting system to cast his vote. This capability needs to be demonstrated to show that the vote is not double counted or missing or incorrectly allocated.

2) In many countries, and I assume also in California, if the vote tallies are very close or are disputed, a recount must be made. There must be assurance that an indisputable reproducible recount is possible using the same (saved) unaltered inputs provided by the voters originally, without requiring the voters to vote again.

3) To allow for a more equitable representation of the voters by their elected candidates, the design of the voting system must allow alternate vote counting methods, besides "first past the post", to be used when necessary, e.g., Single Transferable Vote, Approval Voting, etc.

Specifically,

In Section 2 Security Testing, .
"b. Source Code Review" should changed to "b. Review of Software, Firmware and Hardware Design and Implementation".
The section should be revised accordingly.
Rationale: It is not sufficient to just review the source code of the software. For example, it is possible to have a compiler which has been altered to maliciously add extra code surreptitiously into the binary output files which are then loaded into volatile memory or firmware or hardware logic (e.g., ASIC, FPGA). Nothing in the source code files would reveal that dirty deed. Similarly there can be malicious logic hidden in the hardware design.

The software must be rigorously tested with tools like Coverity, http://www.coverity.com/ to detect hazardous defects and security vulnerabilities.

Yours democratically,

Subject: A Rose for Bowen in Riverside County Editorial!
Sent: Friday, March 30, 2007 12:09 PM
To: Voting Systems
Subject: A Rose for Bowen in Riverside County Editorial!

Honorable Secretary Bowen:

Please note the following unsolicited editorial (even though I write a weekly freelance column for the paper).

We've got trouble, right here in Riverside County and I'm begging your office to launch an investigation here. This county holds concepts of open government and open bidding for government contracts in contempt.

Thank you for trying to make sure citizens are the "decision makers" in public elections.

Sincerely,

THE EDITORIAL:

Friday, March 30, 2007
Last modified Thursday, March 29, 2007 8:49 PM PDT

Roses and Razzberries

By: The Californian Opinion Staff -

A rose --- the "Better Safe Than Sorry" award --- to California Secretary of State Debra Bowen, who said last week that her office would examine electronic voting machines used throughout the state from "top to bottom." Activists here and elsewhere across the country have raised concerns about the security of the machines and the votes they hold. While Riverside County Registrar Barbara Dunmore and the county's Board of Supervisors have repeatedly expressed their faith in the machines that have been used in Riverside County for seven years without any reported tampering or related problems, critics have argued that there is the possibility that the machines could be hacked into and votes altered. Bowen's review, which is scheduled to begin next Friday, is expected to include drills where one team works to secure a voting system against hacking attempts by another team. It is possible ---- and perhaps even likely ---- that her review will underscore that the systems are secure, as local officials here have maintained for years. But it could also highlight vulnerabilities that need to be addressed. No matter the results, the move to conduct the review is a good one. While it's not as comprehensive as we would like ---- it won't focus on the comparative safety of punch-card or other paper-based systems ---- it's a step in the right direction. Any move to help reassure voters that their votes are being accurately counted is a good one.

A raspberry and a rose ---- the "Keeping the Public's Business Public (In The End)" award ---- to the city of Murrieta. A joint "get together" of the Murrieta Planning Commission and the city's Historic Preservation Commission was planned for last Saturday so the commissioners could tour historic buildings and sites in the city. However, the meeting, which was put together by the members of the city's Planning Department, was not properly publicized so that residents could attend if they wanted to. Because of that, the meeting would have been a violation of the Brown Act ---- the state's open meetings law. A city planner acknowledged that advance notice of the meeting was not posted publicly, but dismissed it as just an informal get together to tour the area. When the impending violation was called to the attention of several higher-ranking city officials ---- interim City Manager Ron Bradley, Mayor Doug McAllister and Planning Commissioner Randon Lane ---- all three expressed dismay that the meeting was not announced properly and all said they believed the meeting should be canceled. And it was ---- within the next 15 minutes. While a tour of the city may seem like a benign event that most residents may not care about, by law, the business of government is to be conducted in full view of residents. But they can't observe what they don't know is happening. The raspberry goes to the city staffers who should know that any time a quorum of any commission meets it is to be treated as a public meeting. The rose is handed to Bradley, McAllister and Lane, who realized the error ---- and the importance of the Brown Act ---- and acted quickly to remedy the situation.

A rose ---- the "Giving From the Young Heart" award ---- to Preston Root and his parents Kyle and Starline Root. When Preston celebrated his fifth birthday Saturday, he got lots of presents. But they weren't for him. Preston's parents decided that this year they would teach him the lesson of giving to others who are less fortunate and who need toys more than he does. So they asked the children who attended his party to bring an unwrapped toy for a child between the ages of 2 and 12 to be donated to Children's Hospital in San Diego. To his credit, Preston signed on. "It's nice," he said. "Everybody who is sick needs those toys." The party also served as a lesson on benevolence to some of the children who attended, their parents said. That's a lesson all kids ---- and adults ---- could stand to learn.

Subject: RE: Draft criteria for the "Top-to-bottom review of electronic voting systems..."

Sent: Friday, March 30, 2007 11:15 AM
To: Voting Systems

Subject: Draft criteria for the "Top-to-bottom review of electronic voting systems..."

March 30, 2007

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

Subject: Draft criteria for the "Top-to-bottom review of electronic voting systems..."

Dear Secretary Bowen:

We have read the 3/22/2007 draft criteria for reviewing electronic voting systems for CA certification. As security researchers and computer science graduate students at the University of California, Davis, we (the undersigned) would like to thank you for this bold initiative. We hope the final California review process will set a standard that other states will follow.

In this light, we have a short list of recommendations we feel are important to include and address in the final criteria. We list those here:

1. We recommend the "Security Findings" (I.3) include the mandate that the qualified experts who performed the Red Teaming exercise and code review shall write a report to the Secretary of State summarizing their findings and their recommendations. All proprietary information and data that cannot be made public shall be placed in appendices. This report shall be made public, although the appendices may be redacted. If the appendices are redacted, the appendices' contents and the reason for redaction will be described in the public report. As exploits and security problems are hard to interpret, this public report should not simply be a list of methods and findings, but should include recommendations and should put the findings in perspective.

We feel these public reports are incredibly important tools. They make the team of qualified experts accountable for their findings and methodology. They are beneficial to other states, who may not be able to perform a comparable review but still need data on which to base certification decisions. They put pressure on and provide feedback to the e-voting industry to improve their products (whereas the final decision to certify or not certify provides much less useful feedback). Lastly, the public reports will make the CA Secretary of State's review and certification process more transparent, and will play an enormous role in communication with and building good faith in the public. Similar public reports published by the Ohio Secretary of State (the "Compuware report") and by the State of Maryland (the "SAIC report") have been invaluable in all the aforementioned capacities.

2. We have several recommendations related to the Red Team exercise (I.2.a) and the source code review (I.2.b). From our experience, we recommend the membership of the two teams should overlap. It is not enough to share information through reports, as some innocuous code not commented

upon during review might play an important role when the system is in deployment, or combined with other systems. We hope to see this as a requirement in the final draft. It is truly the easiest way to help the two teams operate effectively with one another.

Also, while we understand the motivation for the separation of the task into various phases, we stress this is unnecessary. The qualified expert team should be able to identify in their summary findings which type of intruder corresponds to each exploit. That is, the report can reflect which exploits could be discovered by someone with access to the source code, and which might not. It is not necessary (or efficient, or convenient) to restrict the Red Team exercise and split testing into phases. We suggest the section be reworded to reflect that the testing should be done by a Red Team who shall be fully informed by the source code review. Currently, the wording suggests there could be future phases of red teaming exercises which might use knowledge of source code.

Lastly, we fear the wording of I.2 (i.e., "The security of each DRE, vote tabulating device, and ballot tally computer will be tested using two complimentary methods...") might suggest that each device will, separately, undergo each review. We stress the importance of reviewing the voting _system_, and not simply its component devices. Two devices might be found to have no problems individually, but this does not ensure their composition to be secure. The Red Team must test the complete system in the configuration in which the State of California plans to use the system. Thus, for example, ballot marking devices should not be reviewed by a Red Team who considers it isolated from, say, its ballot counting device. We recommend the Red Teaming section include that the team shall review the device in its operating environment (especially when this concerns other devices). We stress that this be added as a requirement to the review, but not imposed as a limitation.

3. We are eager to hear how the source code review section is to be interpreted for software that may not necessarily be created by the system vendor or in situations where obtaining or interpreting code is difficult or infeasible. This includes proprietary commercial off-the-shelf (COTS) software, the tool chain used by the vendor to create the election software, device drivers, embedded systems, etc. We suggest the team of qualified experts be empowered to decide which software components be exempt from review. We do not suggest the criteria itself try to specify this, as solutions may vary from instance to instance (e.g., it may be tempting to exempt COTS products from review as the EAC's VVSG has done, but it is possible the COTS product is open-source and able to be reviewed), or this issue may change over time (e.g., as inspection tools improve).

Sincerely,

Subject: RE: attn: voting systems review of March 22, 2007 draft

Sent: Friday, March 30, 2007 10:12 AM
To: Voting Systems

Subject: attn: voting systems review of March 22, 2007 draft

Hello,

I have looked at the March 22, 2007, draft "Top-to-bottom review of electronic voting systems certified for use in California elections." I am writing mainly with security in mind, since what expertise I have is closer to that than to accessibility, say.

Overall, I strongly support the intention of the review. If your intention is to make errors in favor of decertification, you have my support.

Given what I have read about flaws discovered in Diebold systems, including by Harri Hursti and Black Box Voting, and the confirmation of these problems by people at Princeton University, I would be inclined to say that any Diebold systems currently certified in California could be decertified, unless Diebold has provided you with good evidence that most of these problems are already fixed in the currently certified systems. I don't know enough about other vendors' products, in general, to say whether or not such a decision would be justified for them.

Next are a number of comments intended to be in roughly the same order as the paragraphs of the March 22 draft.

I.1.a For practical purposes I cannot imagine how to "effectively secure the DRE ... against ... attacks by any person with access to the DRE, its firmware, software and/or electronic media during ...". Given an attacker with knowledge of election procedures including security and detection policies and mechanisms and with detailed knowledge of the DRE, it seems almost impossible to prevent replacement of the correct software and firmware by corrupt software that does its corrupt deeds and yet is able to fake being the correct software. Any system that can be upgraded can also be upgraded corruptly. (And if attackers cannot corrupt the voting systems, they might be able to simply deploy their own corrupt systems as a substitute.)

If what I say in the preceding paragraph is wrong, wonderful. If I thought it were feasible, I would consider your goal in I.1.a to be wonderful. Instead, I believe that election policy must have some emphasis on measures like physically protecting and limiting access to the DRE systems, and making it hard for a single individual to have surreptitious access to DRE systems, for instance. And the DRE systems can certainly be more robust than they seem to be today, and your review should lead in that direction. So while I don't think I.1.a absolutely has to be changed, I think it could be improved. Perhaps replace "features that effectively" with "features that, when combined with reasonable security policies, effectively".

Although I believe that such security policies are needed, and that the people who do the security testing ought to have a fairly good idea what those policies ought to be, I think such details are inappropriate in the draft and am happy they are not there.

I think comments apply to I.1.b and I.1.c that are analogous to the above for I.1.a.

I.2.b For the "Source Code Review", I would specify that the reviewers are permitted (better, encouraged) to build software and test it in environments which facilitate finding out how the systems behave, such as a debug or emulation environment.
Hypothetically, a software or firmware module might be identified that makes some assumptions about the data it works with. It might be useful to create a modified version of that module that extensively checks all of the data to see if the assumptions are ever violated. Expert source code reviewers will, of course, be able to say what they think they should do. I suggest changing the name of I.2.b from "Source Code Review" to something like "Source Code Review and system testing", and adding text encouraging more activity than just review of source code.

Though it seems beyond the scope of the draft, I would say that a by-product of the review ought to be a set of recommendations or requirements on additional steps that should be taken to detect potential election problems. For instance, several paragraphs talk about preventing untraceable vote tampering or the equivalent. Perhaps state policies should require that records which might contain such evidence of tampering must be (copied and) inspected. I would think that the source code review could suggest how this might reasonably be done, if that's not already known. And it might be reasonable to demand improvements in vendor products to make such inspections easier to carry out.

I.3 "Security findings": Why wait for "completion" of either component of security testing? I would say that as soon as a sufficiently serious problem is found, the Secretary of State should be able to make written findings and initiate withdrawal of certification. Naturally, if this is done, it should be made clear that security testing is still in progress (or, as the case may be, that security testing has been suspended awhile because some other activity such as security testing of another product has become more urgent).

II.2.e Should (II.2) "Each voting system" be examined for privacy curtains or shields, or should this be a requirement imposed at the time of certification for individual counties? I find it quite plausible that a vendor might produce a voting system that has no privacy curtain or shield whatever, the vendor expecting that the customer would acquire such curtains or shields separately. I am not familiar with this aspect of the marketplace. If you expect that curtains or shields would reasonably be acquired separately, I would remove II.2.e from this document completely, making sure of course that the requirement is imposed at some appropriate stage of the certification process.

II.2.f The purpose of nonvisual confirmation is to help assure the voter's intentions were captured on the paper. Among other things, it is supposed to be a check that the software/firmware in the DRE did not corruptly change the voter's vote. If the DRE is corruptly changing the voter's vote, it can print a paper ballot that agrees with the altered vote. If, now, the same corrupt software or firmware interprets the print image or the electronic data stream, it can corruptly tell the voter that the paper is correct, even though the paper is corrupt. You might consider appending another sentence saying something like: "The method of nonvisual confirmation shall be sufficiently independent of the rest of the DRE such that the nonvisual confirmation accurately reflects what has been printed even if the DRE is attempting to conduct untraceable vote tampering."

III Access for minority language voters: Should there be any requirements that disability access testing should be performed for minority languages?

Here are a few remarks concerning my expertise and bias.

I am retired, but worked with computers including designing and programming software for about 30 years. Three of these years were on a specific computer-security-related project, which do not make me an expert on the subject of computer security, but I have some knowledge.

One bias is that I am somewhat more concerned with having substantially-more-secure elections in the long run, and am not as concerned with claiming, or trying to achieve, "perfection" in a short time. (So I was happy to read that the source code review may be performed after completion of the risk assessment.)

Another bias I have is that it is more important to try to eliminate problems that permit a single individual, or a small group of individuals, from having a large impact. For instance, one programmer responsible for some of the firmware or software in a DRE might be able to change many votes nationwide and thereby influence many close elections, without being detected. The Brennan report "The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost" emphasizes this concern. I would assume that if you assemble competent people for the source code review, this would be obvious to them. Please do not hinder them from giving this concern appropriate attention. (The report, which I'm sure you already have, is the one at http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf).

Other miscellany.

At some point, I would think that the electronic equipment used for voter registration and for verifying voters at the polling place could also be investigated for possible security and denial of service issues. This does seem outside the scope of the March 22 draft.

Also outside of the scope of this document, if paper ballots are going to be important in the long run then I think California ought to require that all ballots should be counted on two independent systems which are manufactured by distinct vendors and, insofar as possible, have no components in common that are responsible for the tabulating. That way, an attempt to corrupt a ballot tabulation would be fairly easy to detect unless both systems are corrupted in such a way as to yield the same corrupt results. This might conceivably also permit reducing the number of ballots that must be checked manually, though I don't have a strong desire for such a reduction.

--

Comments on Top-To-Bottom Review of Electronic Voting Systems

Subject: Comments on Top-To-Bottom Review of Electronic Voting Systems

Sent: Friday, March 30, 2007 7:01 AM
To: Voting Systems
Subject: Comments on Top-To-Bottom Review of Electronic Voting Systems

Dear Secretary Debra Bowen,

DEMOCRACY = PAPER BALLOTS HAND COUNTED AT THE PRECINT LEVEL

Computerized voting is not in line with our Democratic values. Election law requires open and verifiable elections. A computerized vote count is a secret vote count; it makes a public vote count impossible. Votes counted in public is key to government by the people. Certification of voting machines is paid for by the companies who own them. No official can see the software that determines the votes. There is no way to recount or prove fraud. A "paper trail" or receipt only provides a false sense of security; there is no way to know if it has been accurately tallied. When I mark or punch a paper ballot, I can physically see whether or not my vote was accurately recorded. I cannot physically see and verify that my vote was recorded as cast on a computer chip inside a DRE machine.

The accessability for the disabled canard just doesn't hold up. Many blind and disabled advocates and groups have asked for the immediate banning of DRE machines. There are other systems available for the disabled community to use such as the Vote-pad, Automark and tactile ballots.The argument that a hand counted ballot paper ballot doesn't hold up. Such a system is totally verifiable. The count must be done at each precinct, by hand, in public, overseen by citizen watch-dog groups and pollworkers, videotaped, and the results posted on the the precinct wall. The cost is one-tenth of electronic voting machines.

All electronic voting machines are susceptible to fraud.There are many documented instances of failures,irregularities, and blatant inaccuracies. Many computer scientists and voting experts agree that machines are not safe. John hopkins computer science and security professor, Avi Rubin testified recently before a House Subcommittee hearing on Elections Integrity. He stated that "Direct Recording Electronic(DRE,usually touch-screens)voting systems--with or without a paper trail--are "not reasonable" for use in a democracy. Period. "

I ask that you immediately ban all electronic voting machines and return to paper ballots hand counted at the precinct level.

Subject: RE: Recommendation for DRE machines.

Sent: Thursday, March 29, 2007 10:22 PM
To: Voting Systems
Subject: Recommendation for DRE machines.

Dear SOS Debra Bowen,
Your press release on 3-22-07 states "Every California voter has the right to have their vote counted as it was cast" and "... to ensure that California voters are being asked to cast their ballots on machines that are secure, accurate, accessible and auditable" This can never happen with DRE machines, BAN them.

There is no test or function of a DRE voting machine that can verify to the voter that their vote was counted (recorded) as cast, impossible! When you press the button to cast your vote on a DRE you can not see with the naked eye whether or not your vote was recorded as cast, you can not see inside a computer chip! A VVPAT is in no way a verification that your vote was counted (recorded) as cast, only a print out of what the DRE program tells you what was cast and it is impossible to verify this with the naked eye of the voter who cast the ballot. The only way that a voter can verify that their vote is counted as cast is if there is a paper ballot that is marked by and verified by the voter. The only secure, accurate and auditable way to count a ballot is to to record the vote on a paper ballot that is the vote of record and hand counted. I won't even go into the security issues with the DRE as this would take many pages of documented evidence, testimony by computer scientists, poll workers, poll watchers and voting integrity investigative journalists and groups, all of which I have available.

Electronic tabulators are notoriously inaccurate and susceptible to over and under counts, non-counts and brake downs. Tabulators are also programmed and a voter is unable to verify that their vote was tabulated as cast. Again, hand counting is the only accurate way to securely, accurately record the vote. A voter marked paper ballot as the vote of record can be audited at any time.

In the instance of English as a second language voter, paper ballots can be printed in any language marked by the voter and hand counted as would an English voting ballot.

In the instance of handicapped and blind voters there are "NON-DRE" touchscreen voting devices, tactile ballots, vote pad etc. are much more user friendly and accessible than any DRE on the market. In the case of the several electronic paper ballot markers for the handicapped and blind I would agree there needs to be an extensive and thorough examination of performance before certification, I would leave the particulars to those who are in the handicapped and blind communities to offer their suggestions for the certain criteria needed.

Our vote is our most sacred common and should not be compromised in the attempt to expedite a vote count or to make someones job easier. A voter marked paper ballot counted at the precinct level is the most accurate, secure and auditable way to count our vote. It is also a falsehood that manually counting of the ballots takes too long or is excessively labor intensive. To the contrary, manually counting the vote en-powers the people and gives a sense of pride and belonging to the only Democratic Republic to exist!

Please BAN DRE machines immediately! Just the costs of DRE machines and tabulators is enough to demand their ban by the taxpayers of California. Lets keep it simple and cost effective, Voter Marked Paper Ballots counted at the precinct level. KISS, Keep It Simple Secretary.

Sincerely,

RE Recommendation for DRE machines.
Member; SAVElections Montery County

I support,
Bradblog.com, votersunite.org, blackboxvoting.org, pollworkersfordemocracy.org, voteraction.org, electiondefencealliance.org and many others, you should too.

Subject: RE: Increase auditing rqmts
Sent: Thursday, March 29, 2007 9:40 PM
To: Voting Systems
Subject: Increase auditing rqmts

I hope the post election audit of randomly selected precincts can be increased from 1% (I think it is now) (plus a number to assure an audit of each ballot type). 1% is too small to sudit anything reliably. Any detection of differences can be accepted as within tolerences, and not prove anything substantively.

I would like to see an increase to 5%. If that seems too high, then increase it to 3%, but add an option for any jurisdiction to audit a numnber in excess of 'whatever' to allow jurisdictions the option to verify in greater detail. This can be opposed by vendors, but it should do nothing more than assure election administrators of the validity of vendor claims. Also if a jurisdiction wishes to audit a greater % or # at its expense, create such an option. Right now ROVs only audit up to the legally required limit, and it ends there. If such a rule can be honored in regulation or law, then jurisdictions with questions or pressures can have an option to consider.

Also require such expanded audits to be publicly observed and reported.

thank you.

Member of SAVElections here.

RE YEAHHH !!!

Subject: RE: YEAHHH !!!

Sent: Thursday, March 29, 2007 10:11 PM
To: Voting Systems
Subject: YEAHHH !!!

Wonderfull ! This is why I voted for you. Unless the machines are bulletproof and verifiable how can we the people trust the results??
If I can be of any assistance to you in your pursuit of this please don't hesitate to let me know. Yours ....

Subject: RE: amendment to comment on draft criteria...

Sent: Thursday, March 29, 2007 7:00 PM
To: Voting Systems
Subject: amendment to comment on draft criteria...

I can imagine others have said as much, but the draft criteria should explicitly include Ballot Marking Devices as well as a general definition that includes future technologies such as vote-by-phone, etc. -

Subject: RE: Attn: Voting Systems Review

Sent: Thursday, March 29, 2007 6:34 PM
To: Voting Systems
Subject: Attn: Voting Systems Review

Dear Secretary Bowen:

Attached is a composite list of suggestions from the members of the steering committee of Protect California Ballots.

Thank you for considering our requests, suggestions and questions.

March 29, 2007

Secretary of State Debra Bowen
1500 11th Street
Sacramento CA 95814
Attn: Voting Systems Review, 6th Floor

Dear Secretary of State Bowen:

Please consider the following suggestions to the TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS CERTIFIED FOR USE IN CALIFORNIA ELECTIONS:

1. include in the review the MTS system used in Los Angeles County. From our research we think the earliest version was never certified by the state or federally. Our attorney, Gregory Luke, explained that "grandfathered" has no legally binding meaning. We area concerned that the current MTS software is uncertified GEMS 2.

2. make these tests public or witnessed by outside observers.

3. publish for the public the results of all the expert reviewers' findings.

4. test for network intruder detection.

5. add "traceable" in all the places your review criteria state "untraceable." All systems must be secured against any tampering.

6. find a way to remove the wireless capacity in the Inkavote-Plus ES&S scanners now used in L.A. County. The modem is built in and there is no way to detect if it is on or off. The Umberg Bill last year outlawed wireless in DREs but not in scanners. Is wireless outlawed in tabulating software? We have screen-shot evidence of wireless on the tabulators—GEMS 1 and MTS.

7. change the word "will" to "shall" withdraw certification if review conditions are not met.

Question: How will the "additional conditions" be enforced? All the InkaVote-Plus scanners in the 5028 precincts in LA County went home with precinct inspectors days before the Nov. 06 and the Mar. 07 elections with their memory cards in them. Like San Diego in June, 06, we had "sleepovers." How can that very insecure situation continue?

Thank you for considering these suggestions. They are a composite of the steering committee of Protect California Ballots.

Yours sincerely,

Subject: RE: California Voting Systems Review: Comment
Sent: Thursday, March 29, 2007 8:32 PM
To: Voting Systems
Cc: Subject: California Voting Systems Review: Comment

Secretary of State Debra Bowen,
1500 11th Street
Sacramento, CA 95814
Attention: Voting Systems Review

First I would like to second the comments of Mr. sent to you in the last day or so.

I would also like to add several additional comments:

1. The VVPAT needs to be easily viewable in order to be reviewable. This means that there must be adequate illumination on the printed VVPAT to allow those with less than perfect vision to actually read what has been printed. As a poll worker, I have seen that many polling places have inadequate lighting, especially along the walls where voting machines are typically located.

Further, some voting machines have privacy screens that limit room light from their screens. That works well for self illuminated computer screens, but fails to provide illumination of the VVPAT.

2. Counties need to provide copies of their procedures to you as well as to the public. This means that they have to know what they plan to do in advance. Too many counties may carry out elections by solving problems as they occur. Although this may be the most expedient administrative procedure, it opens elections up to a wide variety of errors that would be better worked out in advance.

I fear this was a major source of confusion in 2006 since so many counties were using voting systems that were new to them. In addition to normal 'human errors', there was also a big opportunity for intentional error.

3. The Elections Code does not describe in anywhere near enough detail how to carry out the 1% manual recount audit.

a. Procedures describing how and when the precincts to be recounted are selected need to be expanded.

b. Counties need to be encouraged to increase the number of precincts being recounted. One way to do that would be to count ALL the races on the ballots chosen to provide a recounted precinct in every voting district. In our County, that would have increased the audit from 1.5% to almost 4% last November.

c. There is an understandable inclination for elections officials to trust their vendors and the vendor's equipment. After all, why would they buy voting systems they suspected were faulty? But this assumption is ill founded. Voting systems can, and do, fail in use. It is important that counties recognize this fact and install procedures to detect such failures.

d. It is critical that procedures spell out what will happen if discrepancies appear that can not be firmly attributable to human error. It is completely inadequate to simply substitute the hand count numbers for the machine counts. That assumes that the errors that were caught
were the only errors that occurred. When such errors are found, the manual audit must be expanded to a larger number of precincts and, if appropriate, to a full manual recount of all precincts in the county.

In general, I applaud your concentrating on expanding election transparency. That is key to improved election integrity. I find that if transparency is sufficiently widened, most of the potential areas of fraud can be mitigated. This is a big, complex area and I would be happy
to expand my thoughts at your convenience.

Many of these recommended changes could be part of your election regulations. This would be much faster than waiting for the Legislature to pass the necessary Election Code amendments.

Cheers again on the way you are addressing our CA elections.

Subject: RE: California Voting Systems Review: Comment
Sent: Thursday, March 29, 2007 2:40 PM
To: Voting Systems
Subject: California Voting Systems Review: Comment

Dear Secretary Bowen:

I applaud the long overdo intent to review all voting systems used in the State of California. In February 2004 I asked for any public records from the Secretary's office of any such review that was conducted under the provisions of the Election Code. None were forthcoming because no review had ever been done. The extent of the review you are proposing is what should have been happening at the national level before these systems were ever given the imprimatur of NASED. I applaud your efforts to make the largest market for voting systems in the country also have the highest standards and review process in the nation. California will lead the way in bringing much needed light upon a too long secretive process.

In reading over the proposed review I did notice areas of concern based upon experience and knowledge. I know personally how local election officials will parse words and attempt to circumvent both the Election Code, the Procedures for Use, and conditions for use issued by the Secretary. I am also a member of a national group of voting activist leaders and am familiar with the many problems associated with electronic voting. Those problems include reliability issues, inaccuracy because of faulty design (not because of intentional acts), and local election officials hiding problems and protecting vendors. One of the more egregious is the willingness of election officials to purposefully prevent citizen oversight.

Recommendation 1: All hardware, firmware, and software used in connection with voting or any voting systems also be reviewed.

One of the areas of concern is the increasing use of electronic methods to facilitate voter registration rolls and to compare signatures on absentee ballots. Neither the electronic poll books nor the signature comparison software have ever been subjected to testing, standards, or scrutiny of any kind. Yet those very electronic methods can just as effectively prevent a voter from voting or their ballot not being counted as can a faulty or insecure voting system.

Many of the deployed voting systems in this state use an electronic poll book (EPB) in conjunction with the voting system to enable a voter to vote. Errors or manipulation of the EPB can prevent a voter from even receiving an access card, the proper ballot choices, or even a ballot.

Many counties now use a vendor supplied software program to make signature comparisons between electronically stored registration signatures and signatures on the absentee ballots. The Diebold program allows the election official to set the threshold for kicking out a signature. Such a critical component of the voting process should also be subject to review.

Recommendation 2: That the central computers and any peripheral computers that are used in conjunction with a voting system being used in this state also have a physical review to ascertain what hardware, firmware, and software they contain. This review would also include a review of all event and audit tapes or records from the last two years.

It is known that some counties have resident on the election management computers and other peripheral computers, programs that would allow access to databases, to the Internet or intranet, and data swapping programs.

It is also known that some counties, including Los Angeles, have installed on their election related computers uncertified components, including a custom created GEMS 2.

Only by a review of event logs from central election related computers will it be determined if a county removed or disabled programs or features prior to the review.

Recommendation 3: That any review include an analysis of whether any component of a voting system at the minimum meets the reliability and accuracy standards of the 2002 VSS. Ideally the Secretary will conduct the review of the voting systems reliability and accuracy by established electronic industry standards.

The 2002 VSS already has too high of a threshold for allowable reliability and accuracy standards. Even those standards are often exceeded by actual reports from the field. The ideal would be for the Secretary to establish appropriate reliability and accuracy standards that would assure the citizens of this state that every vote is counted as cast, and every voter will be able to vote in a timely manner.

In previous elections in this state, voters have been turned away from voting because of equipment breakdowns or failure of the equipment to work properly. There have also been errors in the programming for an actual election that resulted in the wrong ballot or voters' choices being presented. Errors in programming of ballot definitions used with optical scanners, miscalibration of touchscreens or optical scanners, and the use of inappropriate scanning heads have all resulted in lost votes or votes recorded for the wrong race or measure.

Recommendation 4: To the examination standard for security of "untraceable vote tampering" should be added the "ability" to alter the recording of voters' choices, data files that contain the accumulated totals of votes, and the "ability" to alter audit logs and any other means of recording events or actions processed by the voting system.

In the real world of elections there are set timelines which would make moot any subsequent efforts to determine if there have been efforts at altering the recording, counting, or reporting of votes. The 50th Congressional District race of last year is one example of any subsequent effort to trace possible vote tampering. The candidate was sworn into Congress before it would have been possible to examine any of the records. Even if there had been a subsequent ability to "trace vote tampering" it would have been, as was, mooted by the courts.

There is also the political dynamic of elections that can thwart any effort at establishing vote tampering after the fact. In the last several election cycles there have been repeated examples of candidates either conceding based upon erroneous initial reports, or abandoning any efforts to establish the truth based upon political considerations, such as being referred to as a "sore loser".

The Soubiris v County of Riverside lawsuit by a candidate seeking to trace the event and audit logs, and electronic record of the vote is another real world example of the inadequacy of using a standard of "untraceable vote tampering". There are multiple examples of local election officials thwarting any efforts to trace the forensic evidence related to an election. In fact, many currently deployed voting systems do have the capability to have any efforts at vote tampering traced, but given that through "losing" vital evidence, resistance to allowing such tracing including the use of the slow judicial process, and the timelines which make any subsequent discoveries moot, the ability to trace is "too little, too late".

A more effective and appropriate standard would make it impossible to alter a data file created by the voter or any subsequent files containing vote totals. I am not sure any form of electronic voting system can meet that standard.

Recommendation 5: Any electronic voting system shall be capable of having the entire election generated from within the voting system, without the need for vendor supplied election specific programming such as ballot definitions, etc.

Currently some voting systems require counties to supply memory chips or other means of supplying election specific programming. In many instances such programming is sub-contracted to other subcontractors. This allows unknown source code and programming that has not been subject to any independent testing or confirmation of contents to be introduced into a voting system during every new election. Such a voting system in actual use would not have been subject to your review process. This practice is applicable to both DRE and optical scan systems. There have been multiple reports of faulty programming of such election specific programming, let alone any intentional tampering.

Recommendation 6: That 1 (c) be expanded in its description to include Election Management Systems.

Most voting systems utilize the Election Management System to create and manage the entire electronic voting process, including assigning ballot styles to a particular precinct or voter, the creation of ballot definitions and ballot designs, the accumulation of precinct totals, the reading and accumulating of central count optical scanner results, and the reporting of ongoing tabulating results to the media and the Secretary. If such a critical component of a voting system is connected to an intranet or internet connection, to external lines of communication, and subject to download of data or other electronically formatted digital information, it can be altered in such a way that a review of an electronic voting system prior to deployment in the field would not detect such vulnerabilities. Even if the system was subject to a forensic evaluation it is highly likely that any errors or tampering would be discovered too late to reverse an election result that was based upon error or tampering.

Recommendation 7: Any "red team" process be conducted not only in a neutral test environment, but also with at least one deployed voting system of each model and version.

In the past voting systems presented to the Secretary for approval were tested either at the vendor's facilities, or at the Secretary's facilities. We know from prior experience that once deployed, voting systems are connected in various configurations to other computers or communication lines, software programs have been added to the central election management system computer, and many voting systems allow the local election officials to enable or disable various portions of the voting systems capabilities. This results in deployed systems being configured or capable of performing or being exposed to internal or external access that would not be the same as in a laboratory environment.

Recommendation 8: That each voting system's VVPAT meet "readability", "usability", and "retention" requirements to conform with both the letter and intent of federal and state law.

Many currently deployed voting systems with the required VVPAT do not lend themselves to voter usability or readability. For example some models have covers that are often in a closed position by intention or by accident. There have been reports of poll workers telling voters they could not lift the cover over the VVPAT printout. In other instances the poll workers set up the equipment with the doors already closed and did not inform the voters of the need to confirm their voting choices. Some versions make it impossible to review the entire printout if it contains the choices from a ballot with many races or measures.

Any review should include a "usability" process to determine the time and ease by which any audit or recount can be conducted using the VVPAT. Such a review should include the logistics required to make effective comparisons to the electronic record and the printed record, including assigning particular precinct electronic counts to the corresponding paper record to effect an accurate audit to check the accuracy of the electronically reported results.

The VVPAT itself must be reviewed for its appropriateness for meeting the federal retention requirements of 22 months. Such review would include the industry standards for the ink, paper quality, paper type, and making sure that the paper supplied for the review was the same as what is used in the deployed systems.

Recommendation 9: The wording in II. (3) be changed in the phrase ".... fails to include ANY of the foregoing disability access features...." to ".... fails to include ONE OR MORE of the foregoing disability access features...."

Recommendation 10: The phrase ".... withdraw certification FROM THE VOTING SYSTEM..." used in II (3), III, and IV be replaced with ".... OF the voting system... "

Voting systems are tested and approved as a whole. If any one component or feature fails to meet the requirements of a law, regulation, or standard then the "voting system" is not approved.

Recommendation 11: All counties Procedures for Use of a particular voting system be reviewed to see if the county has been compliant with the adopted Procedures for Use. If it has not been compliant, to initiate corrective steps, including obtaining a judicial mandate or injunction to enforce the adopted Procedures for Use.

The voting system may be reviewed by the state, including under the adopted Procedures for Use, but if the county does not comply with those procedures the review will not reflect the real world deployment of that voting system. In that case the review would not provide assurance that the voting system as deployed has met the Secretary's high standards.

Electronic voting faces more dangers than just intentional manipulation. It has proven itself to be highly vulnerable to system errors, mistakes in programming, human error, poorly designed or less than robust hardware, and with high ongoing costs that were not initially revealed to the public or local election officials.

I once again applaud your efforts to undertake this thorough review. If it appears that the vendors have fraudulently misrepresented their products as meeting the requirements of federal and state law I trust you will make a referral to the Attorney General for compensation to the citizens of this state who are the actual owners of our electoral systems.

Regards,

RE Voter-Verifiable Printers and alternate election methods

Subject: RE: Voter-Verifiable Printers, and alternate election methods

Sent: Thursday, March 29, 2007 2:21 PM
To: Voting Systems
Subject: Voter-Verifiable Printers, and alternate election methods

I first like to note that, speaking as a poll-worker, a computer scientist, and a concerned citizen, I have found the addition of the printer to the DREs to be not particularly reassuring. The printers were highly fragile, breaking down far too easily -- in my precinct, we ended the day with six printers either broken or out of paper, and two functional. This meant that we had only two machines operational during the final-hour rush, and had a line of voters out the door. Additionally, our older, less-technically-savvy precinct captain repeatedly compromised the seals on our printers, in an effort to fix them. In the event of a recount, if many printer seals are compromised, there would be no way to prove that the paper records were untampered.

I would like to see our state shift back to using pen-on-paper wherever possible. This technology is rather less prone to failures -- we've had a few thousand years to work out the kinks.

Second, I am an advocate for shifting from the Plurality Voting system we currently use, to superior alternatives. I do _not_ favor Instant Runoff Voting (also known under many other names like "Alternative Choice" or "Single Transferable Vote"), as this system is plagued with complex flaws, gives false assurances of "majority choice", and in some realistic cases causes the addition of a voter's own honest ballot to change results against the interests of that voter.

Please note that Approval Voting, in which voters may approve as many candidates as they like (essentially voting "Yes/No" on each candidate, as with mutually-exclusive ballot propositions) would have almost zero cost to implement with any currently-used balloting system, and could later be advanced to Range Voting, in which voters "grade" or "rate" each candidate (potentially with the option to abstain from rating those they feel uninformed about).

Subject: RE: Draft plan comments
Sent: Thursday, March 29, 2007 11:49 AM
To: Voting Systems
Subject: Draft plan comments

Our biggest concern is that there really is no current safe way to use computer voting machines and insure 100% accuracy. It is possible to have a paper printout that registers differently from the final tabulated vote so that gives us no additional confidence in the honesty of election results.

We'd prefer scanners because they at least can leave an indelible paper trail. A smarter, more fool-proof punch system would be better. Even absentee ballots would be safer than computer machines.

If you do utilize machines with paper printouts, please do not use laser paper. Use only ink that will last for years without fading.

There have been way too many examples of the extreme efforts people have and will go to to manipulate elections to trust anyone anymore. Companies involved in the manufacturing of voting machines and all steps in elections must be as non-partisan as possible.

Thank you for your efforts to achieve honest elections in California's future.

Sincerely,

Subject: RE: Regarding DRE certification
Sent: Thursday, March 29, 2007 10:31 AM
To: Voting Systems
Subject: Regarding DRE certification

To whom it may concern:

I just read the article in the Contra Costa Times (http://www.contracostatimes.com/mld/cctimes/community/16986435.htm) regarding reactions to your plan to require stricter certification of DRE voting machines and the actual enforcement of the law requiring paper verified voting trails.

This is a happy day. For too long we have been inundated with reports of failures and blatant security holes while the election officials failed to react or reacted in such a way as to make one wonder if they were paying attention. As a voter in California, and a computer scientist, the situation in this country has grown increasingly frightening. I am proud that California is finally taking strides in the right direction, and hope that we can continue down this path becoming an example for the rest of the country.

I believe that electronic voting is the future and there is no reason it cannot be implemented securely. Above all, I hope you can ignore the cry that there is not enough time before the next election to implement changes. While that may well be the case, that is no excuse not to start and take the first starts. Additionally, this arguement avoids the inconvenient fact that in this country, and in this state we are never more than two years from a major election. If we don't have time to prepare before the 2008 election (18 months away) when will we ever have longer?

Subject: RE: [peoplecount] Public Comment on Draft Criteria for Review of Electronic Voting Systems
Sent: Wednesday, March 28, 2007 1:17 PM

Cc: Voting Systems
Subject: Re: [peoplecount] Public Comment on Draft Criteria for Review of Electronic Voting Systems

Well let's hope they read this six page piece!

On 3/27/07, wrote:

> Dear Secretary of State Debra Bowen, Evan Goldberg, Lowell Finley, and the Staff Member(s) Assigned to Handle These Comments:
>
> As a senior citizen, I predicted during Bowen's campaign for SOS that if elected, Bowen would not rid California of insecure, easily hacked voting machines by 2008. Even where this review finds machines not certifiable, local elections officials will plead that they cannot hold elections without them, so they will be granted waivers. I'm not a prophet, just somebody who has lived long enough to have seen all these charades many times.

<SNIP>

Subject: RE: Voting Systems Review
Sent: Wednesday, March 28, 2007 8:39 AM
To: Voting Systems
Subject: Voting Systems Review

Madame:
Having read your proposed "Top-to-BottomReview " of our voting systems, I am absolutely against your interference with the voting systems selected by each county in our state. The entire thing smacks of an elected official seeking personal gain, whether power or payback. I protest vehemently! Leave the voting systems to the voting officials of each county--they are local people that we voters know and trust.

Subject: RE: Voting Machine Review
Sent: Wednesday, March 28, 2007 12:30 AM
To: Voting Systems
Subject: Voting Machine Review

Dear Secretary Bowen:

I deeply appreciate your very able and conscientious representation of California voters.

I am concerned about the Diebold scanners used in Santa Barbara County. Last November, it took three tries for my ballot to feed into the machine. I asked about this after the election, and was told that there were some ballots with thin edges on one side, but it didn't matter. Ballots can be scanned no matter how they are fed into the machine, including upside down or back to front. This is hard to believe.

I asked about the need for making sure the counter registers the ballot as accepted. I was told that there is no need, because the counter number is checked against the ballots and the poll book, <u>after</u> the polls close. This to me is not a reassuring answer - what if they come up short? I was told four years ago the poll worker <u>does</u> need to see the ballot is accepted. What has changed?

I asked about pens we used this time instead of the markers we used before (much faster), and the pencils they used instead of pens in a different precinct from mine. I was told they never use pencils here - they must have run out of pens. But if they never use them, why would pencils be an OK substitute? Markers and pens are equally OK, as I understand it, but then why the switch?

I've complained twice about not getting my ballot stub torn off in front of me at the ballot box. I was told once that it didn't matter if anyone watched me put my ballot in because they didn't care if I voted the ballot or took it home. They did it right this time, and I was very happy about it, but the new issues make me doubt the whole process.

I have grave doubts about the tabulation of the votes, and it bothers me very much that an unaccountable consortium of media is in charge of counting votes in presidential elections.

I would like poll workers and their affiliations listed in the newspaper again. I don't think state law requires this anymore, but I think it should.

I would like there to be accountability to ensure prompt corrections to the list of voters and their particulars. I think there should be no need for any but a very few provisional ballots.

Thank you for the opportunity to comment.

Subject: RE: Draft Criteria
Sent: Tuesday, March 27, 2007 4:08 PM
To: Voting Systems
Subject: Draft Criteria

Hello again -

1.You must eliminate the word "untraceable" from your Security Standards definition. It should apply to 'any form of vote tampering' , not just that which is untraceable.

2. Red teaming ? What does the blue team do, if anything? Would there be a blue team present at any/all "real" attempts at hacking the system(s)? You know, in real life situations, not pretend?

3. Soource Code review? You refer to 'risk assessment', but you never say what or where or when this is. What is it?

Subject: RE: Public Comment on Draft Criteria for Review of Electronic Voting Systems
Sent: Tuesday, March 27, 2007 3:19 PM
To: Voting Systems
Subject: Public Comment on Draft Criteria for Review of Electronic Voting Systems

Dear Secretary of State Debra Bowen, Evan Goldberg, Lowell Finley, and the Staff Member(s) Assigned to Handle These Comments:

As a senior citizen, I predicted during Bowen's campaign for SOS that if elected, Bowen would not rid California of insecure, easily hacked voting machines by 2008. Even where this review finds machines not certifiable, local elections officials will plead that they cannot hold elections without them, so they will be granted waivers. I'm not a prophet, just somebody who has lived long enough to have seen all these charades many times.

DREs cannot be audited. But I'm in San Diego and I know how useless audits are. Brian Bilbray was sworn in on the basis of a partial machine count. In addition to thousands of votes which had not been counted, the election had not even been certified, which must be done before citizens can request a recount or audit. An audit of a partial count would be a partial audit. But once a candidate has been sworn in, only Congress can unseat them, so even if recounts were affordable, which they are not in San Diego, being priced at ten times what they cost in surrounding areas, and obtainable, which they are not since the courts will not intervene once Congress swears in a candidate and the Constitution says that only Congress has jurisdiction to allow an audit or recount once a candidate has been sworn in, they could not change the results of an election no matter how much fraud was proven. If Congress swears in a candidate on the basis of a partial machine count, and subsequently an audit proves that the machines were rigged and that candidate had received no votes at all, they would remain in Congress, voting on continuing war crimes and taxes, unless Congress itself chose to unseat them, something they are loathe to do to colleagues.

A few days ago Richard Stallman, the founder of the free software movement and someone most computer experts revere, gave a speech. Afterwards he was asked about open source code in computerized voting and in his reply he gave several examples of how open source code could be hacked and concluded his remarks by saying that computers have no place in elections and that votes must be on paper. If you want to know the truth about open source code, invite him to testify.

Many elections officials will claim that they cannot hold elections unless they send the voting machines home with elections workers ahead of time. There is no real security for these sleepovers, and as the Cuyahoga County convictions for election fraud proved, election riggers can be of either party and may have worked as elections officials for twenty or thirty years without necessarily being too honest to rig elections. Instead of trust, we need a tight chain of custody.

As for the central tabulators, we have no way of knowing if they are connected to election riggers by WiFi or modem. You do not have the technical manpower capable of examining each machine on election night to ensure that they are offline, and the public is not allowed to. Such inspections cannot take place ahead of time, as it is only a matter of seconds to open up a central tabulator and give it WiFi connectability or to plug in a cable or modem on election night, and election night is the only time that counts. Of course such connectability can be removed after the election without a trace. Here's a relevant article:

http://www.bbvforums.org/cgi-bin/forums/show.cgi?8/47056

Posted on Tuesday, March 27, 2007 - 10:45 am:

http://www.trustme.com/story.php?title=secret-White-House-comunication-system

GWB43 is the name of an internet server owned by the Republican National Committee.

The White House has its own internal email system, ending in the .gov suffix, as mandated by the Presidential Records Act. The law requires that public business be conducted on a public server.

Yet documents made public in the course of the U.S. Attorney Purge scandal reveal that key Administration figures used such email addresses ending with "gwb43.com."

As Citizens for Ethics and Responsibility in Washington (CREW) notes:

CREW has learned that to fulfill its statutory obligations under the PRA, the White House email system automatically copies all messages created by staff and sends them to the White House Office of Records Management for archiving. It appears that the White House deliberately bypassed the automatic archiving function of its own email system that was designed to ensure compliance with the PRA.

Karl Rove, we learn, does about 95% of his White House emailing from the RNC-controlled account, even though 100% of his salary is paid for by taxpayers. It is against the law for him to do partisan political work while in the White House. (During the Clinton years, allegations that Al Gore made phone calls to donors from the premises enraged Republican pundits.)

This writer makes the excellent point that the official White House communications channels are "hardened" against interception by foreign intelligence services. Can the same be said about the private RNC servers?

Did prosecutor Patrick Fitzgerald know about this bypass when he subpoenaed White House emails pursuant to the Plamegate investigation? If he had, "Scooter" Libby might not have been the only one brought to trial.

We recently learned that Susan Ralston, the former assistant to Karl Rove, used three private e-mail accounts connected to the Republican party to provide "inside White House" information to Abramoff. Would Rove have been implicated in the Abramoff scandal if investigators knew about these "hidden" communications?

After one Abramoff/Ralston communication, a follow-up email to Jack Abramoff clearly states that people in the White House use private servers to conduct business of dubious legality:

Your email to Susan was forwarded to Ruben Barrales and on to Jen Farley, who read it to me last night. I don't know what to think about this, but she said is better not to put this stuff in writing in their email system because it might actually limit what they can do to help us, especially since there could be lawsuits, etc. Who knows?

This story by Joseph Hughes and Melissa McEwan compiles statements by George Bush,

Condoleeza Rice, Donald Rumsfeld, Michael Chertoff and Alberto Gonzales, all of whom have claimed that they do not use email for business. Oddly, Rice made this claim at the same time let slip that she had used email to communicate with Richard Clarke.

Dubya's stated reasoning for not entering the computer age is both disconcerting and inarticulate:

"I tend not to e-mail - not only tend not to e-mail, I don't e-mail, uh, because of, uh, the different record requests that could happen to a president. I don't want to receive e-mails, 'cause, you know, there's no telling what somebody would e-mail me and it would show up as, uh, you know, part of some kind of a story that - and I wouldn't be able to say, 'Well, I didn't read the e-mail' - 'But I sent it your address; how can you say you didn't?' So, in other words, I'm very cautious about e-mailing."

All very amusing, but can we really believe that in the modern age these people do not use the most convenient messaging system available?

Or could it be that all these people recall how Ollie North was tripped up by the discovery of certain emails?

If the Bush White House used GWB43 to route around history, we must ask a question straight out of the Parsifal legends: What is GWB43 and who does it serve?

The answer, surprisingly enough, takes us into the dark mysteries of the 2004 election in Ohio.

A list of domains that share mailservers and nameservers with gwb43 reveals numerous sites connected to either powerful Republicans or to the Religious Right. On the mailserver list, we find domains connected to Bush, Newt Gingrich, and ohiogop.org.

Here is the WHOIS info on GWB43:

Domain Name: GWB43.COM

Administrative Contact, Technical Contact:

Republican National Committee dns@RNCHQ.ORG

310 First Street SE

Washington, DC 20003

US

999 999 9999 fax: 999 999 9999

Record expires on 16-Jan-2008.

Record created on 16-Jan-2004.

Database last updated on 21-Mar-2007 17:45:46 EDT.

Domain servers in listed order:

NS1.CHA.SMARTECHCORP.NET

A.NS.TRESPASSERS-W.NET

"Trespassers-W.net"? This odd name derives, it seems, from a passage in A.A. Milne's Winnie the Pooh stories, in which the characters try to decipher a truncated sign which once read "Trespassers will be prosecuted." The server, in this case, belongs to a web design firm called Coptix, in Chattanooga, Tennessee.

(Incidentally, it is against the law to provide a false telephone number in registration information.)

SMARTECHCORP refers to a hosting service named Smartech, also located in Chattanooga, Tennessee. Their web page is here. They offer internet hosting, streaming media and so forth.

In 2000, Smartech merged with a company called NextLec, a telecommunications firm owned by the remarkable Mercer Reynolds, President Bush's close friend and controversial campaign fundraiser. Reynolds, who raised a record amount during the 2004 campaign, has been accused of selling access to the President.

The name Smartech appeared in stories arising out of the disputed 2004 election in Ohio. From a November 7, 2006 article by luaptifer at Daily Kos:

Ohio's election results are hosted on the same servers by the partisan companies that run websites like Georgewbush.com and many of the familiar Republican group sites.

More (also see here):

SOS Blackwell also neglected to inform that he outsourced Election Night hosting services to the provider of Internet operations for the Republican National Committee, SMARTech Corp. It's clear that most of the IP address space allocated to Smartechcorp, if it has a domain name, is operated by the RNC or its functionaries and allies.

The firm handles everything Republican:

On August 22, 2004, SMARTech Corp (smartechcorp.net) announced that it would be "hosting" the Republican National Convention in New York City, providing "convention speeches, video-on-demand 'streams' and live shots of events through powerful Web servers, most of which are at Smartech's headquarters in downtown Chattanooga." The announcement stated that the "company also hosts the Bush-Cheney campaign Web site, at www.georgewbush.com, and the national committee's site, www.GOP.com ."

Smartech shows up in this interesting information technology story from 2004, which outlines a still-unsolved mystery.

During election season, web surfers from outside the United States were not able to access Bush's Web site, GeorgeWBush.com, even though surfers within U.S. borders had no

problem doing so. Why this oddity, and who was responsible? The site used network management technology from Akamai Technologies Inc. to restrict access. An Akamai spokesman referred all questions to the hosting company, Smartech. Yet Smartech's president said "All we do is host the site. I have no control over what's being done outside our servers."

Why would anyone within the party would want to restrict foreigners from looking at GeorgeWBush.com?

One possible answer: The intention was to restrict foreign intelligence services or CIA personnel (who cannot operate domestically) from learning about sensitive White House communications using the GWB43 server.

So, what does it mean that Ken Blackwell used Smartech for Ohio's election night hosting services?

One does not need to exercise much imagination to see how anyone using the net for nefarious purposes would want a "friendly" hosting company handling ultra-sensitive duties. Hosting companies keep records of who does what. If you are using computers to do something you don't want the world to know about, you don't want those records available to just anyone.

As the controversy over the 2004 elections gathered steam, Karl Rove made a joke about fixing the election returns from a computer in the White House basement. This remark struck some observers as the sort of jest that the villain in Rope might have uttered: "Yeah, sure, I strangled my friend for no good reason and hid his body in the cupboard! Now seriously, how about that drink...?"

The vote tabulators -- the "mother machines" as Teresa Kerry once put it -- had an online connection. Anyone using the internet to interfere with the data stream coming from or going to those computers would be fearful of an electronic "trail" tracking his actions.

Similarly, anyone in the White House using an RNC server to avoid incriminating emails entering the historical record would fear that the records would be subject to a subpoena served upon the hosting company.

That's why someone engaged in such activity would -- hypothetically -- want to use a company owned by the President's good friend. A private company can scrub such records whenever it wishes to do so, or it can neglect to keep them in the first place.

Now, I must stress that I have no evidence that Smartech is anything other than an honest, responsibly-run firm.

Michael Collins, a writer and "clean elections" activist, does not accuse Smartech or any other firm of wrongdoing, but he does offer this hypothetical tableau:

You're in the parallel universe in a country almost exactly like ours and you want to steal an election. How do you do it: You look at: what states are really valuable-now and in the past; your resources in those places of value; your logistical plans - can you execute in those states.

Then you take your goals and apply available technology. It's all about machines, which you can have switch votes, and networked tabulators, centralized tabulators. You get the "servicing" personnel to make sure that the pre-programmed vote switching software driven machines are put in place. Then you use a safe haven ISP as an operations base that will allow your mischief to take place without a lot of record keeping that can't be cleansed.

This is the core - the machines do their thing. You've got a safe haven ISP network provider, and you have the traditional techniques: over registering in favorable voting areas, voter suppression, voter disenfranchisement, and all around psy ops to keep the oppositions vote away.

Voila, you win the election. Who knows if this hypothetical applies? But it's fascinating isn't it?

Here in California, the intent of the voter is not taken into consideration. In San Diego's notorious mayoral election, Donna Frye was precluded from becoming mayor after being elected because the desires of Diebold, to have bubbles filled in that their machines could read, caused the votes of more than 5,000 eligible voters who had written in "Donna Frye," to be discarded. When Assemblyman Juan Vargas tried to introduce a bill in the State legislature that the intent of the voters be taken into account, he was forced to withdraw it when the Governor threatened to veto it. So if our intent does not matter legally, what good would it do if an audit proved that 90% of Californians had intended to vote for one candidate, but that the machines had recorded their votes for another candidate?

At least two complaints have been filed with your office by San Diegans regarding violations of elections laws and procedures by our former Registrar of Voters, Mikel Haas, and he was just promoted, probably to make it more difficult for your office to investigate, if you had any intentions of doing so.

If you were concerned about honest elections, you would have immediately subpoenaed everyone named in formal complaints to your office and asked them under oath if the allegations they were accused of were true. Most of the allegations are fully documented through Public Records Requests and cannot be denied. Then you would have acted to remove them from office and bar them from holding any office related to elections, as SOS Jennifer Brunner has done in Ohio. Then you would immediately decertify all voting machines which are not currently properly certified, as former SOS Kevin Shelley did. And then you could procede at your leisure to see if there were any properly certifiable machines, which, of course, there are not.

Here's another article on audits:

This was posted to http://www.bradblog.com/ on March 27, 2007, so you may have to search the March archives to find it:

Election Contest Decided by 3 Votes, Judge Refuses to Order Hand Count of Touch-Screen 'Paper Records'
'Why would you have a paper record if you don't count it?,' Asks 'Losing' Candidate
Orange County, CA Court Decision to 'Set Precent' According to Both Sets of Attorneys...

The *Los Angeles Times* underscores everything that is wrong with relying on "paper trails"

from Direct Recording Electronic (DRE) touch-screen voting systems: Nobody ever counts them. Even in incredibly close contested elections as overseen by a court of law...

A judge ruled Monday that Janet Nguyen won the February election for an Orange County Board of Supervisors seat by a slim three-vote margin, rejecting arguments by her opponent that a recount wasn't completed because the paper audit of electronically cast ballots was not counted manually.

"All the votes were counted," said Orange County Superior Court Judge Michael Brenner. "There was a full and legal recount."

...

It was, he said, "perfectly reasonable" for Janet Nguyen to ask for about 35,000 paper absentee ballots to be checked by hand to contest ones that weren't filled out properly and then ask to have about 10,000 electronic votes recounted the way they were on election night — by machine

...

Trung Nguyen, who is not related to the winner, declined to comment and left the courthouse as his attorney, Michael Schroeder, said an appeal was likely. "Why would you have a paper record if you don't count it?" Schroeder said.

...

All sides agreed that Brenner's ruling could set a precedent.

Please note that Rush Holt's Election Reform bill (HR811), which mandates the hand-count of a very small minority of paper records in most federal races (which this race was not) via an audit after Election Day, allows no audit to happen at all in the case of a an automatic state-mandated recount --- the type that occur when an election is incredibly close, and when such an audit, arguably, might be needed the most.

If your office is sincere, you will immediately decertify all voting machines which were "certified" by labs which did not test for security or that certified machines which were not certifiable, labs whose licenses were suspended, and labs which have no public oversight (all of them). None of that requires any investigation as it is all fully documented.

Your office should immediately terminate all elections officials who are on record as having violated any election codes or procedures, something which also does not require much time or effort to accomplish.

Once you have taken these steps, any other procedures you may wish to initiate will be taken seriously rather than just looked upon as methods of stalling for time to allow machines to be used to steal the 2008 election.

Respectfully,

Subject: RE: Response to Top-to-Bottom Draft Criteria
Sent: Tuesday, March 27, 2007 11:23 AM
To: Voting Systems
Subject: Response to Top-to-Bottom Draft Criteria

The following suggestions are submitted in regards to the Draft Criteria being developed by the Secretary of State's Office relative to the top-to-bottom review of voting systems currently certified for use in California elections.

1. Unless they are being developed under separate cover, the lack of measurement standards/tools as an integral part of these criteria will leave the criteria open to interpretation by the manufactures and other parties involved in the evaluation process.

2. Recommend inclusion of a requirement that the DRE's, vote tabulating devices and ballot tally computers be tested multiple times through-out Election day while polls are open and during the ballot tallying period after polls are closed. This testing should take similar form, function and purpose as the old Logic and Accuracy testing did.

3. The second paragraph under Section II.1 appears to be misplaced. This requirement is applicable to more than just the voters with disabilities. Suggest moving it to a paragraph titled I.1.d Paper Audit Trail.

4. The reference in paragraph I.2.b to "the risk assessment" is the first and only reference to such as assessment and it is not possible to directly infer from the context in which it is used what was meant.

5. In Section II.2 under Disability Access Testing, there are multiple references to "audio output". It is going to be nearly physically impossible to keep this audio from being overheard by the use of curtains or shields. It would necessarily require a voting booth being set up in a separate room from the others and this would likely be cause for some outspoken Disability advocate to cry foul. Suggest rethinking this and possibly inclusion of the use of headphones, earbuds, etc. This audio output requirement is further aggravated by the requirement in Section II.2.f that requires a non-visual method for voter verification. A disabled voter is definitely not going to want: "You have voted for candidate XYZ for President in the Republican primary race" announced to everyone.

Thanks for giving the public an opportunity to provide input on these criteria. It reflects an openness that has not always been present at the State level. It also allows those of us who have considerable years of experience in the Election process at the County level to make a meaningful contribution. My own experience includes actually coding the ballot counting program in Assembler back in the early 80's up through the negotiation for Kern County of a contract with Diebold for a touch screen system in 2002, and nearly everything in-between.

Subject: RE: Is it fraud only when the perpetrator is caught? Ballots
seem to exist when secret detectors are needed to find them! Double
standard!!

Sent: Sunday, March 25, 2007 10:53 PM
To: Voting Systems
Subject: Is it fraud only when the perpetrator is caught? Ballots seem
to exist when secret detectors are needed to find them! Double
standard!!

Does fraud only when the perpetrator is caught? Ballots seem to exist when secret propriety detectors are needed to find them! Double standard : Virtual fraud does not count when virtual ballots are counted!!! Please decertify virtual ballots! Ballots must by law be detected by equipment which most voters are born with in order for voters to trust the election process. Many eyes and ears make the election process fair.

I believe Secretary of State Deborah approach is to prevent provable fraud, while my attempt is to make fraud exceedingly difficult to implement. Because current machines use virtual ballots tracing fraud is impossible which allows all kinds of fraud to slip in. How does one prevent fraud which is impossible to view with ballots which only appear when non public secret viewer is necessary to see the "real" ballot. How does the VOTER know the ballot presented for view is the ballot which will be counted? Trusting experts is giving control to the experts!

The current DRE's system can be hacked in almost unlimited ways without showing any evidence. Their output must be considered an estimate only. A state law should require media to attach the word estimate when ever DRE numbers are presented with a penalty for not following the law. These machines must print an official ballot reject able and easily readable by humans and dedicated reading - counting machines. The dedicated ballot reading counting machine needs by law to have a microprocessor which is fast but more limited than that installed in an APPLE I in 1982 otherwise fraud is possible. This microprocessor must have an addressing capability for executing programs to less than the ROM memory in which the program is stored which will prevent alteration (viruses & other) between verifications short of chip removal attack. The high level language used must be readable by most voters so we do not have to let the computer experts vote for us. The machine would output to a printer and CD ROM on a precinct by precinct basis and be public information. I wish to remind you the computer experts are usually unable to write programs which work perfectly on the first execution; why would they find ALL fraud generated by other programers? Restricting the possessor , machine functions, and using language readable by marginally computer literate would vastly improve the ability to find fraud.

I. SECURITY.

1. Security Standards.

For purposes of these standards, "untraceable vote tampering" means preventing the accurate electronic recording of votes, or altering the record of votes, to change the result of an election in a manner that leaves no electronic record of tampering. "Denial of service attack" means disabling a voting system other than through sheer physical destruction in a manner that renders the voting system inoperable for voting. Security not possible if program runs in random access memory! Takes 7 seconds to hack!

a. DREs. Each direct recording electronic voting system ("DRE"), as defined in Elections Code Section 19251(b), must incorporate, as part of its design, hardware, firmware and/or software program features that effectively secure the DRE and all electronic media used with the DRE against untraceable vote tampering or denial of service attacks by any person with access to the DRE, its firmware, software and/or electronic media during their manufacture, transport, storage, temporary storage, programming, testing and use, including the electronic ballot definition or layout process

Ballots must be inspect able by voter without use of any computer program or any other tamper able device. Must not be tamper able after voting!

b. Vote Tabulating Devices. Each "vote tabulating device," as that term is defined in Elections Code Section 358, must incorporate, as part of its design, hardware, firmware and/or software program features that effectively secure the vote tabulating device and all electronic media used with the vote tabulating device against untraceable vote tampering or "denial of service" attacks by any person with access to the vote tabulating device, its firmware, software and/or electronic media during their manufacture, transport, storage, temporary storage, programming, testing and use. Ordinary computers with programs running in random access memory are not capable of preventing vote tampering or "denial of service" attacks unless tested between counting every vote as the program can be changed anytime. It takes only 7 seconds to compromise machine when it is capable of running programs in random access memory

C. Ballot Tally Computers and Ballot Tally Software. Each computer used to tally ballots and each "ballot tally software program," as that term is used in Elections Code Section 19103, must incorporate, as part of its design, hardware, firmware and/or software program features that effectively secure the computer, the ballot tally software program and all electronic media used with the computer and program against untraceable vote tampering or "denial of service" attacks by any person with access to ballot tally software program, the ballot tally computer, its firmware, software and/or electronic media during their manufacture, transport, storage, temporary storage, programming, testing and use. Ordinary computers with programs running in random access memory are not capable of preventing vote tampering or "denial of service" attacks unless tested between counting every vote as the program can be changed anytime. It takes only 7 seconds to compromise machine when it is capable of running programs in random access memory.

2. Security Testing.

The security of each DRE, vote tabulating device and ballot tally computer will be tested using two complementary methods, "red teaming" and source code review. The Secretary will select qualified industry and academic experts in computer and software security, including experts in electronic voting systems, to perform both types of tests.

a. Red Teaming. The "red teaming" process is analogous to military training exercises in which the members of the "red team" are adversaries trying to defeat friendly, "blue team" forces. The red team exercise will be designed to simulate conditions in which a voting system might be vulnerable to attack in the actual cycle of manufacturing, programming, delivery, testing, storage, temporary storage and use in California elections. Initially, the team will approach the system knowing nothing of its source code. Knowledge of source code may be used in subsequent attack attempts. The objective will be to determine whether and to what degree it is possible to compromise the security of the voting system to interfere with the accurate recording of votes or alter the record of votes to change the result of an election. These tests will only be valid at the moment the tests are made and can become invalid during the election time returning to normal after the election is over unless the following conditions are met:

1Only Programs installed in ROM can be executed.

2. Acomodating computer separate from counting computer.

3. Votes from accomodating computer recorded on official paper ballot which the voter is able to reject if the equipment malfunctions!

b. Source Code Review. The second component of security testing will be source code review. The objective of the source code review will be to identify anything in the code that could be used maliciously to interfere with the accurate recording of votes or alter the record of votes to change the result of an election. The source code review may be performed prior to, during or after completion of the risk assessment.

1. It is very easy to hide hooks in the source code or subroutines which are difficult to identify by experts. Most experts cannot write their own bug free computer programs on the first attempt! Who says they can find tricks in another person's program.?

2. It is the voter who should be convinced the counting is accurate & unbiased.

3. Counting programs should be written in language every voter can understand, lack proscess other than counting, outputing to CD and printer only public records!

3. Security Findings.

Upon completion of either component of the security testing, the Secretary of State may make written findings that a DRE, vote tabulation device or ballot tally computer is not reasonably secured against untraceable vote tampering and "denial of service" attacks by features included in the design of its hardware, firmware and/or software. On the basis of such written findings, the Secretary may immediately initiate the process to withdraw certification.

The machines must be rejected if every voter cannot be certain that the machines could not possibly create a denial of service attack or allow untraceable vote tampering.

II. ACCESS FOR VOTERS WITH DISABILITIES.

1. Disability Access Standards.

The federal Help America Vote Act (HAVA) requires that all polling places in elections for federal office have at least one voting system that is "accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."

Under Elections Code Section 19250(a), the Secretary of State may not certify a DRE unless the system "includes an accessible voter verified paper audit trail." Elections Code Section 19250(d) requires that all DRE voting systems "shall include a method by which a voter may electronically verify, through a nonvisual method, the information that is contained on the paper record copy of that voter's ballot." Under Elections Code Section 19251(a), "'[a]ccessible' means that the information provided on the paper record copy from the voter verified paper audit trail mechanism is provided or conveyed to voters via both a visual and a nonvisual method, such as through an audio component."

When no one is present who understands the disability features to explain how the machine can help persons with handicapped person then the machine is more of a hindrance than a help according to at least one handicapped person. If the training requirements are not present and used with each machine the machine and the vote tally should be rejected!!!!!!

2. Disability Access Testing.

Each voting system will be examined to determine whether it complies with the accessibility requirements of HAVA and the Elections Code. The examination will be conducted with the assistance of persons from the disabled community. For purposes of this review, a voting system complies only if it provides all of the following features and capabilities in at least one voting system available for use in every polling place:

(a) A dual-switch input control interface that permits use of "sip and puff" or other adaptive devices by voters with paralysis or severe manual dexterity disabilities who are unable to use touch screens or tactile key inputs.

(b) The capability for the voter to select simultaneous and synchronized audio and visual outputs, audio outputs only or visual outputs only.

(c) Voter-adjustable magnification, contrast and display color settings to improve the readability of text on the video displays.

(d) Variable audio output levels and playback speed for voters with hearing impairments.

(e) Privacy curtains or shields that effectively prevent others from observing or hearing the selections of a voter using such features as audio output, simultaneous, synchronized audio and visual output, display magnification or modified display font, contrast or color settings.

(f) In the case of a DRE, the capability to permit a voter to verify electronically, through a nonvisual method, the information that is contained on the voter verifiable paper record copy of that voter's ballot. This requirement is satisfied by a method of nonvisual confirmation that draws the information provided to the voter from either (1) the paper record copy itself or (2) the same electronic data stream used to print the voter verifiable paper record copy.

When no one is present who understands the disability features to explain how the machine can help persons with handicapped person then the machine is more of a hindrance than a help according to at least one handicapped person. If the training requirements are not present and used with each machine the machine and the vote tally should be rejected!!!!!!

3. Disability Access Findings.

The Secretary of State may make written findings, based on the results of the disability access testing described above, that a voting system fails to include any of the foregoing disability access features and capabilities, in which case the Secretary of State may immediately initiate the process to withdraw certification from the voting system for disability access use.

III. ACCESS FOR MINORITY LANGUAGE VOTERS.

HAVA requires that every voting system used in an election for federal office "shall provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a)." Every certified voting system will be tested to determine whether it provides alternative language accessibility in the federally mandated language or languages for each county that uses or intends to use the system. If the Secretary of State makes written findings, based on the results of the minority language access testing, that a voting system does not provide alternative language access as required by federal law, the Secretary of State may immediately initiate the process to withdraw certification from the voting system with respect to the affected county or counties.

Because of the possibility of creating untraceable fraud the language features should be in a machine which prints the official paper ballot so the voter can reject the ballot incase the machine malfunctions. Counting should be done only by ROM driven dedicated counting machines using a special voter language understood by every voter. Using computer languages understood only by experts allows experts to choose which candidates are elected to public office.

IV. USABILITY FOR ELECTIONS OFFICIALS AND POLL WORKERS.

Each certified voting system must be designed, configured and accompanied by sufficient documentation and training materials so that, in the absence of extraordinary circumstances, elections officials and poll workers can independently and without assistance or intervention by employees or contractors of an election system vendor, carry out all operations necessary to open the polls, set up and calibrate voting system equipment, instruct and assist voters in registering votes and casting ballots, respond to voting system error messages or temporary power failures, close the polls, print end-of-day vote totals, take down voting system equipment, transfer polling place results to central tally computers and tally final results.

The Secretary of State will conduct a review of each voting system's documentation and records regarding the use of the voting system by elections officials and poll workers in California elections. The Secretary of State may make written findings, based on the results of the review, that a voting system does not reasonably permit such independent operation. Based on such findings, the Secretary of State may immediately initiate the process to withdraw certification from the voting system.

Subject: RE: Draft Criteria
Sent: Sunday, March 25, 2007 9:58 PM
To: Voting Systems
Subject: Draft Criteria

Dear Secretary Bowen -

I have some more problems with the language in your draft. With regard to your "denial of service" definition - what about electrical source (power supply) attacks? According to your criteria, one could deliberately disengage the power source and render the machines inoperable WITHOUT destroying the machine. Is this allowable?

Also, your standards never include ACCURACY and/or EFFICIENCY qualifications. What if some of these machines just flat out don't work very well? This has been shown to be the case in many of them. They may not have been tampered with, or attacked - but they just don't function properly for other reasons - ie. bad design, poor programming, shoddy workmanship/materials etc. Where is that included in your criteria - it SHOULD be in there. Junk is junk, whether it's secure or not, and should not be acceptable.

Also, and most important is that I must assume that you are testing a limited # of machines. Well, shouldn't EVERY machine have to be tested? Particularly with volatile source code.

Also, the practice of vendors applying software "patches" (problem solvers) to these computer systems MUST NOT BE ALLOWED! These patches are rarely certified, but they are being used and can be applied (legally??) on an emergency basis without ever being examined, tested, or certified. This is unacceptable!

Subject: RE: Draft Criteria
Sent: Sunday, March 25, 2007 8:31 PM
To: Voting Systems
Cc: TheBradBlog@cville.com
Subject: Draft Criteria

Dear Secretary Bowen

At the end of Section I you say " On the basis of such written findings, the Secretary may immediately...." You should change the word 'may' to 'shall'. So it would read -

"On the basis of such written findings, the Secretary shall immediately initiate the process to withdraw certification."

The point being that if the system is NOT secure, you MUST de-certify it. NO LOOPHOLES!!!!!!!!!!!!!!!!!!! NO DISCRETIONARY ALTERNATIVES!! De-certify. Case closed!

And the same language should be used in Section II number 3. Change 'may' to 'shall'.

In Section IV there is no penalty listed for non-compliance with this section. If you regulate it, you enforce it.

Subject: RE: Optical Scanners
Sent: Saturday, March 24, 2007 8:07 PM
To: Voting Systems
Subject: Optical Scanners

Dear Secretary Bowen,

In your teleconference on March 15, you indicated that you preferred optical scanning of paper ballots to DREs. That is certainly better in the view of many computer professionals. However, optical scanning is not free from being compromised. The DFM scanners we use here in Sonoma County which are used to count all ballots centrally, have microprocessors in them for vital control functions. It would be possible, though not probable, to reprogram them during one of the frequent maintenance procedures prior to an election cycle. Some of our scanners are 20 years old and do their job at the rate of 1000 cards per minute - a tough job for any piece of machinery. Far more likely is the possibility that the Windows based computers which tally the output of the scanners could contain modified software or firmware. These machines use software produced by Hart Intercivic and are also updated frequently. This is not to say that I suspect problems here in Sonoma County, only that I can see how our scanning system could be compromised. Marin County uses a precinct based optical scanner which only has to handle one paper ballot at a time. Mechanically, it is not much more complicated than a copy machine. With ballots tallied at the precinct level, scanner results can be compared more easily with audit data and with exit polls.

As far as the need to accommodate disabled voters, the utilization so far has been minimal. See my preliminary survey report in my email of 3/22/07. There are also devices out there which can help a disabled voter produce a paper ballot: AutoMARK and the non-electronic VotePad device which your predecessor refused to certify in August 2006.

In view of the many problems reported with machine-based voting, Many computer professionals, are advocating hand-counted paper ballots. I am old enough to remember when that was how all ballots were counted. There may have been local shenanigans in some cities, but never the potential to skew the results of a National election. Unless your experts can come up with a foolproof system for monitoring the results from optical scanners, I would like to see you consider how hand-counting of paper ballots could be implemented.

Thank you for your hard work and dedication. With you at the helm, California can be a model for the rest of the country and maybe we can "**get our democracy back**".

Sincerely,

Subject: RE: Thank you

Sent: Saturday, March 24, 2007 4:44 PM
To: Voting Systems
Subject: Thank you

Dear Ms. Bowen,

Thank you for imposing strict criteria for voting machines. The process that you have proposed is exactly what we need to ensure an honest election process in California.

I further believe that election integrity in California California will create ripple effect to improve election processes nationwide.

I know that you are under intense pressure from powerful entities that oppose your reforms. Please don't back down. I trust you.

Sincerely,

Subject: RE: electronic voting
Sent: Saturday, March 24, 2007 12:01 AM
To: Voting Systems
Subject: electronic voting

I am against all electronic voting systems.

Subject: RE: Comment on needed changes/Voting Machine Review

Sent: Friday, March 23, 2007 11:35 PM
To: Voting Systems
Subject: Comment on needed changes/Voting Machine Review

Dear Secretary of State Debra Bowen,

The forcing of electronic voting machines on the voting public was a huge boondoggle. Some people made tons of money. Some people got elected who did not win the election. The machines are hackable, inaccurate, expensive to buy and expensive to maintain, cause frustration for many voters, require more time and expertise on the part of election workers, need experts dashing around town on election day to fix electronic glitches, and proprietary software stands in the way of transparency to mention a few of the problems associated with their use. Paper ballots have worked pretty well for many years and in all kinds of situations. No, they are not fraud proof but they are way cheaper than non fraud proof machines and do not have the problems listed above. Fraud can be and has been caught with paper ballots when there is/was a good and accountable chain of control.

I do not think a 1% audit is sufficient to insure accuracy and catch fraud.

How come exit polls are not more highly regarded as indicators of problems? They seem to have a good track record.

I realize that many handicapped people find electronic machines ideal for them. Seems to me other possibilities besides electronic machines exist. But perhaps one machine per precinct for special needs since we are awash with these machines anyway. But then what happens when some of those machines malfunction?

There are other problems besides inaccurate, hackable electronic voting machines. I feel very pessimistic at times thinking that we will never have a system where I can be sure my vote has been accurately counted.

Look at what happened to the votes for Dona Frye in San Diego. Look at Bilbray in San Diego being certified by Haas before all the votes had been counted. Laws need to plug loopholes and people have to be held accountable for errors and fraud.

Sincerely,

RE Let the Voters decide not the computer programers!

Subject: RE: Let the Voters decide not the computer programers!

Sent: Friday, March 23, 2007 5:19 PM
To: Voting Systems
Subject: Let the Voters decide not the computer programers!

Dear Debra Bowen;

The electronic voting machines do not provide a real ballot! The DRE virtual ballot can only be viewed through the machine with no certainty which ballot it is showing you or if the ballot you get a copy of on the screen or paper printer is the one which will be counted. Since the paper trails are not considered valid ballots they are close to irrelevant. How can the voter know that what is printed on the screen and the paper trail is actually the same data in the virtual ballot memory space? With paper ballots there is a certainty which ballot you are writing on and which ballot you are seeing and no interpretation controlled by someone else is needed. Checks can be coated in such a way that adding chemicals or using erasers will void the check and ballots should have the same properties. If some people need machines to mark ballots give them to them and provide ways of reading their ballot even if they are sightless or unable to hear. A person who has limited sight says the DRE is of limited if any help.

The counting of ballots needs to use a method which every voter can understand and believe. Who knows what is going when ballots go into black boxes and numbers come out on printers and computer screens. Trying to see fraud in the election office is an exercise in futility. Trusting these black boxes is like letting the black box makers choose the candidates for office. Testing them on one day before and the day after is insufficient because the questions is still what were they doing on Election Day. Elections with DREs or trusting computer scanners are an exercises in faith. (I thought there was supposed to be a separation between church and state.)

I am more worried about the undetectable fraud!-Florida (where DRE flipped the vote and decided a congressional or senate seat)

As a programer I can make DRE's & Card readers elect anyone who pays
the greatest amount of money. Computers use random access memory to execute programs and only experts (the ones choosing the candidates) can change the programs for seconds to hours to flip the vote without detection. Use of Read only memory in machines outputing to CD and paper limited to optically reading and counting with Voter Language understood by every voter could decrease unobserved fraud.

Subject: RE: Voting machine review criteria
Sent: Friday, March 23, 2007 4:09 PM
To: Voting Systems
Subject: Voting machine review criteria

Hello Debra -

I have some input regarding your draft criteria for voting machine review.

First of all, in your opening statement of intent, you mention "acceptable levels of security, accessibility, ballot secrecy, accuracy and usability". You must also include "transparency" and "verifiability". I believe, according to California State law, ALL aspects of elections must be transparent. This HAS TO INCLUDE all aspects of software, including source codes. This nonsense that source code is proprietary, even though it may be the law, is just that - NONSENSE and is probably unconstitutional, or at least in conflict with other law. If voting machine vendors won't reveal their code - then their machines should NOT be certified. PERIOD. As for verifiability, this must include both audits and recounts.

Under I. SECURITY, you mention "untraceable vote tampering". This language must be changed. First of all, when you say 'untraceable', you are assuming that SOMEONE is doing the tracing. Well, just who would that someone be? Is it the Voter? The poll worker? Is it the local election official? Is it the State? The Certifier? Well, NONE of these entities are capable of 'tracing' the tampering because (a) ONLY the vendor can fully understand the SECRET software codes and/or programs, and (b) just when would this 'tracing' take place? Obviously, after the election - when it's too late.

This means that ONLY the vendor could actually trace the 'alleged' tampering, and really, would they be at all motivated to do the tracing? I THINK NOT!

Secondly, you do not mention "TRACEABLE vote tampering", (as opposed to "untraceable".) So, in effect, what you are saying is that it's NOT allowed if it's "untraceable", but if it's "traceable", then it does not qualify as a criterion for your review. Or, rather that vote tampering is only unacceptable if it is "untraceable," and if it's "traceable", it is allowed. As long as you can trace it (which of course noone can do), it's okay. That's what you're saying.

Thirdly, if the vote tampering is "untraceable", HOW WILL YOU KNOW IF IT EXISTS????? You have already defined it as being - "untraceable". If it's untraceable, it's incapable of being found - therefore - IT DOES NOT EXIST. And, in fact, it may not exist. Certain programs, and/or files can be made to delete or erase themselves at a certain pre-determined time and date, or can be triggered by othere data (say, a certain plateau, or level in the tabulation process) to delete themselves and never be seen again.

You must definitely change that wording.

More to come.

Subject: RE: What Stalin said

Sent: Friday, March 23, 2007 4:08 PM
To: Voting Systems

Subject: What Stalin said

Apparently it can't be repeated often enough, because there is still advocacy of using electronic tabulators to tally the votes.

Over 92% of people have said that they do not want the votes counted by machines. Maybe because they remember what Stalin said: "He who casts a vote decide nothing. He who counts the votes decides everything." There's ample evidence that electronic tabulators can be hacked. It's been on TV, and there's even a step-by-step demonstration on how to rig an election found here:

My sparsely populated county has only 35 precincts and we really don't need expensive machines. It's just a state mandated burden placed on us, creating a possible situation for mischief. We did return a member to congress who's facing possible indictments under very questionable voting results, but the RoV has retired. Please give this matter a lot of thought before announcing a final decision.

--

Subject: RE: Comments on draft of "TOP TO BOTTOM REVIEW..."

Sent: Friday, March 23, 2007 1:46 PM
To: Voting Systems
Subject: Comments on draft of "TOP TO BOTTOM REVIEW..."

Dear Secretary of State -

As a concerned citizen, I have reviewed your draft "TOP TO BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS..." and I think it is great that you are trying to set standards for electronic voting systems. We need them. One of the first things that struck me when I looked at the draft though, was that it does not have a definition of a proper voting procedure. As a computer programmer/analyst, I know that the first thing you must do when automating a process is to produce a good description of that process.

If what we want is a fair, transparent, irreproachable and robust voting process, then we have to know what that looks like before we automate it. I think it was exactly this lack of understanding of the process both on a public and a administration level that got us into the mess we are in now. Though I have ideas about what that process might look like, my purpose here is to note its absence and to suggest that its publication, either as a separate document or in this one, would serve not only to get that definition out into the public eye, but also to motivate and underscore the demands that we must make on electronic voting systems.

Thanks again for your work;

Subject: RE: proposed review

Sent: Thursday, March 22, 2007 10:19 PM
To: Voting Systems

Subject: proposed review

Madam Secretary, thankyou for your proposal for a top to bottom review of California's voting machines- it is high time to deal with the underhanded chicanery that has been offered as high tech modernization of voting.

Subject: RE: Input for the proposed protocol

Sent: Friday, March 30, 2007 2:54 AM
To: ; Voting Systems
Subject: Input for the proposed protocol

To whom ever this may concern,

I have comments about Draft Criteria for Top-to-Bottom Voting Machine Review. As general comment, I think it is hitting the nail to the head.

However, the proposed procedure does not include hardware review. Taking into account the time constrains it would be cumbersome to build in full blown hardware review - from this perspective excluding the hardware review as separate function is reasonable approach. The natural way to deal this issue is to use Red Team to conduct the hardware review as they will inspect the hardware as part of their process.

Experiences from the voting machines have already red flagged peculiar hardware designs - from voter access-able yellow button of Sequoia to hidden battery test button of TSx, not to mention various circuit board jumpers and switches to modify the operations of the machine. For example starting the software from external media. Another examples would be hardware designs showing curious memory mapping schemes - making in the case of less than perfect documentation challenging to understand which parts on memory are physically in memory cartridge or more arcane places like service changeable "clock ship" instead of the normal on-board memory - and paper ballot scanner auto-calibration features.

Depending the quality, referencing methodology and standards the vendors have documented their source code it can be hard or even almost impossible to understand the true nature of the system within the time given without references to the hardware. For example if JP1 is reference permanent wiring jumper or voter access-able switch does makes no difference in functional programming in the source code, but can make all the difference from security perspective. This also underlines why hardware review from schematics of the circuitry alone can also be misleading without red team view. Lack of reference information can lead to situations where software review team will not be able to identify security vulnerabilities.

For these reasons, to increase the effectiveness of the software review team it would be beneficial:
1) formalize that red team will conduct light weight hardware review
2) to prioritize the process by making the red team to start their work by sweeps of all machines to be tested first
3) channelize "throw over" the observations made as soon as practically possible to the source code review team as input

I understand that with this comment the classic "working in the total isolation" of red team from other parts of the audit process can be compromised, but the time constrain alone is justifying it. Making the channel one way only will preserve the purity of red teams work against counter argumentation.

Sincerely yours,

...

RE SAIC Report - State of Maryland Diebold DRE Machines.

From: on behalf of Voting Systems
Subject: RE: SAIC Report - State of Maryland Diebold DRE Machines.

Sent: Monday, March 26, 2007 5:04 AM
To: Voting Systems
Subject: Fwd: SAIC Report - State of Maryland Diebold DRE Machines.

---------- Forwarded message ----------
Date: Mar 26, 2007 7:50 AM
Subject: SAIC Report - State of Maryland Diebold DRE Machines.
To: votingsystems@sos.ca.gov

Secretary Brown,

I am the .   I have been vocally opposed to any form of e-voting since it was first proposed in 1995.

You can not secure it.   It is not possible.   Full Stop.

My firm builds state of the art systems which attempt to defend MasterCard, AMX, Major Banks, the US Navy and Chubb Insurance.

We defend most of the systems, most of the time.

There is no way a group of retired volunteers can set up a cheap, distributed, part-time, rarely-used, uncertifiable system and have ANY assurance it works.   It is laughable.   It is a precise recipe of the field status which is the best case to ALLOW complete compromise of a system undetected.

Which I believe was the intent all along.   The systems paid for by HAVA are designed to be hacked.

HAVA was written by GOP operatives most of them now convicted felons, in order to create a system in which the GOP can move the margins of control as they see fit.

The SAIC report written at the request of the State of Maryland details over 250 ways to compromise that system.   It also makes it clear SAIC was refused access to many critical systems and software code.

I am the person who confronted the Maryland BOE with a full copy of the report (300 pages, which included 275 pages of redaction marks.)

Maryland BOE leaders, as a group, dove their head into the sand.

I will also note, in under 12 hours two FBI agents from the Baltimore field office had launched an investigation.   Not of Diebold or the BOE, but of me. And how I had gotten ahold of the report.

While the FBI matter remains open, and I have been effectively silenced from much of the public dialogue. I continue as a citizen and patriot to offer the report, software copies supporting how to hack the systems, and my expertise on the subject to any public official willing to speak out.

Please let me know if I, or any of the material I have gathered can be useful to you.

Regards.

Secretary Debra Bowen
1500 11th Street
Sacramento, CA 95814

March 28, 2007

RE: Voting Systems Review,

TOP-TO-BOTTOM REVIEW OF ELECTRONIC VOTING SYSTEMS
CERTIFIED FOR USE IN CALIFORNIA ELECTIONS

FAIL-SAFE VOTING: It's as simple as 1,2,3

1 – OPEN SOURCE SOFTWARE: All electronic voting machines and tabulation devices must use open source software.

2 – PAPER BALLOT: All election technology must allow a voter to

(a) mark (by hand or machine) an optically-scannable paper ballot,
(b) inspect their ballot to confirm their vote, and
(c) physically place their ballot in a ballot box which undergoes secure, rigorous chain-of-custody safeguards.

3 – 10% RANDOM HAND COUNT IN EACH PRECINCT:

All electronic tallies (from machines which have printed or otherwise provided ballots **AND/OR** independently-programmed tabulation devices which have optically scanned said ballots) in an election **MUST** be verified by publicly hand counting a randomly selected 10% of the ballots cast in each precinct.

See more information at www.verifygra.com

Sincerely,

Comments on California Secretary of State's Draft Criteria for TTB Review

1 Introduction

The 2007 Top-To-Bottom (TTB) voting systems review is a major step forward in ensuring the reliability and integrity of the state's voting systems. While the draft criteria provide an outline of procedures that will help to improve election integrity, the criteria need additional specificity to prevent time pressure and resource constraints from adversely affecting the quality of the evaluation.

1.1 General Comments

Given the brief period allowed for public comment on the draft criteria, some discussion of general principles may be helpful to provide the Secretary with additional context for evaluating more specific comments. We discuss these general issues before going into specific, line-by-line comments.

1.2 Under-specification

At a substantive length of about four pages, the draft criteria have little choice but to leave many aspects of this review process under-specified. High-level goals such as security, reliability and usability are systems-specific issues for which general guidelines and benchmarks are difficult to write. Under-specification of these goals can lead to charges of arbitrary treatment and can lead to confusion as to the scope and nature of specific testing. Combined with the resource and time constraints discussed below, under-specification may result in no systems being about to meet the general goals of the TTB review. We go into specific areas where items could be better specified in Section 2 below.

1.3 Constraints

Successful completion of the TTB review of all systems used in California will involve completing the review of all 16 systems from 6 vendors[2] in less than four months, an average of one week per system. Source code review, only one component of the TTB review, can easily last an entire month for a single system. To accomplish the TTB review process it will undoubtedly be necessary to run multiple evaluations in parallel. The CA SoS will need to devote the resources necessary to ensure that the TTB review

[1] Contact: ____ The authors' affiliations are provided for identification purposes only. The views expressed in this document are the authors' personal views. The authors do not purport to represent the views of their respective institutions.

[2] According to the CA SoS, for November 6, 2006, this included: Sequoia Optech 400C, Sequoia Optech Insight, Sequoia AVC Edge I, Sequoia AVC Edge II, Diebold AccuVote-OS, Diebold AccuVote-TSX, ES&S M100, ES&S Optech IV-C, ES&S Optech Eagle III-P, ES&S M650, ES&S AutoMARK, HART BallotNow, HART eSlate, DFM Mark-A-Vote, Ink-A-Vote OS and Ink-A-Vote Plus. *See:* http://ss.ca.gov/elections/voting_systems/systemsinuse_110606.pdf (last visited 26 March 2007).

for each voting system is thorough and comprehensive, and such a review must begin as soon as possible.

While we commend the Secretary for planning to conduct a comprehensive top-to-bottom review, the aggressive timeline might require setting some priorities. In particular, the Secretary should consider whether there are items that are of acute concern in the 2008 election year. Some requirements contemplated by the TTB draft criteria will clearly be met by only a few systems; to the Secretary might consider devoting resources to procedure and technology development aimed at bridging these known gaps, rather than a formal process of which some findings are a foregone conclusion.

For example, there are a number of criteria in the TTB draft criteria that are unrealistic given the state of technology available in the California voting system market. While we will go into this in more detail in Section 2, we'll briefly point out, for example, that only one voting system certified for use in California, the AutoMARK, meets the requirement that the system read back the contents of the verifiable paper record (§II(2)(f) of TTB draft criteria). This will result in counties that use other systems having to both procure and use the AutoMARK in each precinct.

1.4 Publication Requirements

Throughout the TTB draft criteria document – §I(3), §II(3) and §IV – there are references to the effect that the CA SoS "may" make written findings based on the results of testing. Just as the public has an interest in the testing criteria, it also has a substantial interest in the outcome of testing conducted to measure compliance with these criteria. All systems that do not meet one or more of the final adopted criteria should have a written report and findings issued publicly.

1.5 Blended Systems Evaluation

The draft criteria also don't contemplate the evaluation of blended systems – systems where different goals are accomplished by voting systems manufactured by different vendors. Will the red team exercise involve the blended system? Is the most accessible element of a blended system what will be tested in the accessibility evaluation?

2 Specific Comments

In this section we discuss specific comments we have on sections of the TTB draft criteria document.

2.1 Security

2.1.1 "untraceable vote tampering" is too narrow

Sections §I(1), §I(1)(a)-(c) and §I(3) should encompass all kinds of tampering, not just "untraceable vote tampering," for two reasons. First, if a voting system allows "traceable" or readily-visible "altering of the record of votes" or "chang[ing] the result of an election", there are cases in which that system could not be considered to be secure.

Second, the phrase "result of an election" can mean a variety of things and is unclear. We suggest this be clarified to involve changing "vote records" and "aggregate vote records" or "tallies" to reduce ambiguity.

In general, we would advise having a separate itemized section or glossary for definitions.

2.1.2 Denial of Service Attack

In the preamble to §I(1), the term "sheer physical destruction" is unclear. It seems to imply that any physical destruction is out of scope. However, some types of physical destruction are only possible through poor design of certain elements of the voting system. For example, DESI's AccuVote-TSx is known to have problems with the electrical cord easily falling out and exposing people to the risk of electrical shock. This could happen in the course of normal use and could render the system "inoperable" but might not directly affect vote records or tallies.

2.1.3 "effectively secure" is Too Vague

In §I(1)(a)-(c), voting systems are required to have features that "effectively secure" against tampering and denial of service attacks. Defining security in general is a difficult if not impossible task. However, it could be defined in the draft criteria as the systems robustness with respect to specific types of attacks. We would recommend an itemized robustness definition that includes common voting-system security concerns such as changes to vote records, changes to event logs, denial of service attacks, attacks against privacy and ballot secrecy, etc.

2.1.4 Qualifications of Security Testers

The preamble to §I(2) discusses "qualified industry and academic experts". This section should set forth more detailed qualifications for these experts. As written, it is unclear what qualifications industry and academic experts must possess. This groups might also be unduly exclusive; the Secretary should consider including elections officials with relevant expertise.

2.1.5 Red Teaming

In §I(2)(a) the red teaming procedure is very vague. It needs to be clear in what environment the testing will take place, how the red team will be constructed, what information they will have (not "might" have), how the "blue team" will operate and what will constitute a successful breach.

Another consideration is that red teaming might fall victim to a learning bias. That is, the first red team/blue team exercise will contribute to general knowledge that would be useful by both teams in the second such exercise. Essentially, the red and blue teams will "learn" additional techniques and information during each exercise. This means that a vendor's system will naturally be evaluated differently depending on if it is evaluated near the beginning of a series of red team exercises compared to the end of such a series of exercises. A natural way to eliminate a learning bias is to use different red teams and blue teams for each exercise, but that will inevitably increase expenses and reduce consistency from one test to another. We are unaware of a general method for conducting a large number of red team exercises. It would be next to impossible for one single red team and blue team to conduct all of these exercises in the time period available.

To maximize the amount of information that the red team exercise will generate under the top-to-bottom review's timeline, the red team will need a high level of knowledge about these systems – comparable to those available to "insiders" that might be positioned to attack these systems. This should include as much information as possible and at least all the information that the CA SoS holds in escrow for forensic analysis, including source code, operational documentation, use procedures, etc. Testers can be required to sign a standard non-disclosure agreement and reports can be produced without proprietary or confidential information.

Also, the objective of the red team exercise shouldn't be as narrow as defined in the last sentences of §I(2)(a). The objective scope should include impairment of elections equipment and software as well as attacks that compromise voter privacy and ballot secrecy.

2.1.6 Source Code Review

Source code review is a time-intensive, laborious, and highly specialized process; for example, the recent thorough source code review of the ES&S iVotronic voting system conducted by the State of Florida took a team of nationally renowned computer security experts approximately one month to complete. It will be a considerable challenge to complete source code review on all 16 current voting systems currently in use in California. Outside of these time constraints, there are other concerns with the language of the source code review. The Secretary should be aware that the top-to-bottom review's time constraints will probably not allow comprehensive source code review of any system.

The word "maliciously" in §I(2)(b) should be stricken. Requiring malicious might lead the review to overlook certain classes of vulnerabilities. Some of the most serious security vulnerabilities discovered in voting systems in recent years involved designed-in "features" that could easily have been misused. Also, if there is a possibility of an operator with innocent intentions making a given mistake, it is crucial that this class of potential vulnerability is noted and that procedures are put in place to minimize the likelihood of such a mistake. Though a malicious attacker might amplify the consequences of these vulnerabilities, an attacker's intent should not be used to define the vulnerability itself.

The word "risk assessment" at the end of this section doesn't seem to make much sense. There is no other reference to a "risk assessment" in the draft criteria document and it should be made clear what part of the process is "the risk assessment" or if such a risk assessment was left out of the details (or if that reference in this section is a mistake). Typically, a source code review can be one part of a risk assessment.

2.2 *Access for Voters with Disabilities*

2.2.1 Disability Access Testing

The preamble to §II(2), makes it clear that "assistance of persons from the disabled community" will be relied upon to help conduct disability access testing. However, it is unclear in what role this assistance will be provided. There are two possibilities (which are not mutually exclusive): persons from the disabled community might help to design tests, or they might participate in conducting the tests. In the former case, it is important that participants have backgrounds in accessible systems development, needs assessment and/or accessibility evaluation. Human factors and usability experts should play a role in the design and evaluation of the specific tests conducted; not all of these individuals will be persons from the disabled community. Thus, this section should provide that, "The examination will be conducted with the assistance *of experts in human factors and usability as well as* persons from the disabled community."

2.2.2 Dual-switch Inputs are Only One Class of Solution

The requirement in §II(2)(a) that a dual-switch input control interface be available in every polling place will eliminate voting systems that cannot provide this kind of interface or that cannot be upgraded to provide a dual-switch input. While some voting systems (such as the AutoMARK, Hart eSlate, Sequoia AVC Edge II) provide dual-switch input, some cannot (and some of these can only provide dual-switch capability in audio ballot mode). This requirement could require that some counties procure entirely new voting systems for their precincts. Note that some voters with paralysis or manual dexterity disabilities can use other means of voting, for example, using a head wand[3].

2.2.3 Voting Systems Don't Typically Allow Changing Color Settings

While most, if not all, voting systems have a high-contrast mode and magnification capabilities, the ability to change "color settings" (§II(2)(c)) outside of contrast settings is not widely supported. In many cases, the high-contrast mode removes color from the interface entirely to display a black and white interface (although some do not).

2.2.4 Audio is Useful for the Sight-Impaired *and* Hearing-Impaired

In §II(2)(d) "variable output levels and playback speed" are associated in the draft criteria with improving accessibility for hearing impairments. However, adjustments in playback speed are more often used by sight-impaired or non-sighted voters who are accustomed to using high-speed playback on other types of accessible information technologies. This should say, "sight and hearing impairments".

[3] A head wand allows an individual to use a touch screen by using a wand attached to their heads. See: "Adaptive technology." *Wikipedia, The Free Encyclopedia.* 23 Nov 2006, 06:08 UTC. Wikimedia Foundation, Inc. *available at:* http://en.wikipedia.org/w/index.php?title=Adaptive_technology&oldid=89603954. (last visited on 26 March 2007)

2.2.5 Audio Playback of Paper Records is Currently Not Possible

§II(2)(f) implements a requirement currently present in the California Election Code that has not been enforced to date. Make no mistake, this is an essential aspect of voter verification that is not being provided by the voting systems market: all voters should be able to and encouraged to verify their votes. If a certain class of voters does not or cannot verify their vote, they would be a natural target for a malicious attacker, especially if there is a high probability that the machine could algorithmically determine that a given voter would be likely not to verify her vote.

However, there is only one machine certified in California that could perform this operation currently: the AutoMARK. It is non-trivial to upgrade or adapt other voting systems to allow audio playback of the paper records. This requirement could result in all counties having to procure one AutoMARK per precinct.[4]

Another concern is that of printer malfunctions. Some voting systems with paper record attachments, such as the Hart eSlate, can detect when certain types of errors occur. However, other paper record attachments will allow electronic recording of a vote record *without* the corresponding paper record. If it is not apparent to a disabled voter that nothing is being printed, and if they are provided with audio feedback that relies on printer signals instead of scanning the paper record, they will falsely be lead to believe that they had verified their vote. Here, the criteria should specify that reading back the content of the paper record by interpreting signals sent to the printer is only valid on voting systems that can detect critical, non-printing errors with the paper trail feed.

2.3 Access for Minority Language Voters

2.3.1 Recording and Playback of Minority Language Paper Records

In §III, the criteria provided do not specify if paper records should be recorded in the voter's ballot language. If they are not, voters may have a difficult time verifying that the paper record contents correspond to the summary screen presented on the machine. Of course, paper records that are not in English might be difficult to recount or manually tally. One solution to this is to provide both the ballot language and English on the paper record, which will double the length of paper records and half the capacity of paper rolls.

Also, the criteria do not specify if the mechanism for reading back the contents of a paper record would be required to playback the voter's ballot in their ballot language. Naturally, if a disabled voter chose a non-English ballot language, their audio verification should also be required to be provided in that language. Requiring Optical Character Recognition (OCR) of non-English languages could be very difficult for vendors to support, especially in languages that are written in non-Latin (non-Roman) alphabets.

[4] Note: now that the AutoMARK is no longer exclusively licensed to Election Systems and Software, this isn't as much of a burden as it would have been in the past where an entire elections system solution would have to be procured (absentee and polling place voting and election management system).

2.4 Usability for Elections Officials and Poll Workers

2.4.1 Current Work on Training and Documentation Heuristics

We commend the focus of the final section of the draft criteria on the usability of these systems from the perspective of poll workers and election officials. As a polling inspector in Alameda County, author Hall has experienced first hand how complicated the intersection of elections and technology can be.

In addition, our research team at UC Berkeley is currently involved in a project developing heuristics for poll worker documentation and training. It has become clear, in the course of this work, that poll worker documentation is a very low priority for voting systems vendors. Often the customer jurisdiction has no choice but to develop their documentation largely from scratch. Jurisdictions have mixed success on this front. We aim to provide jurisdictions with a set of heuristics based on document design principles that they could use to improve their pollworker documentation. We hope to also extend this to poll worker training. We can provide the CA SoS with preliminary heuristics that could be used as the basis for an evaluation instrument.

3 Conclusion

These draft criteria, beyond a shadow of a doubt, constitute the single most important and forward-thinking move to increase the quality of our voting systems. The timing and resource constraints involved with the TTB review are substantial and it will be a challenge to complete the evaluation process by August. We hope that our comments were helpful in refining the criteria for the TTB evaluation process. Thank you for considering public comments and we are available to expand upon these comments in public or private.

Subject: RE: Draft Criteria
Sent: Friday, March 23, 2007 1:09 PM
To: Voting Systems
Subject: Draft Criteria

Under the security section I would recomend that a clause be in place which would prevent the DRE from being switched to manual mode. The reason for manual mode on the Sequoia System was intended for activator failure. The solution would be a paper ballot or simply require additional activators be readily available. Additional requirements for the activators would be a default to the current date in case of power and or battery failure. VVPATs must remain married to their respective DRE.
I truly believe that Secretary Bowen is taking the lead in true election integrity and reform.

Subject: RE: Review of California voting systems
Sent: Friday, March 23, 2007 8:35 AM
To: Voting Systems
Subject: Review of California voting systems

To Whom it May Concern:

Since free and fair elections are the very basis of our form of government, implementing free, fair, and accountable elections and methods is critical.

The system used by my county for many years was a paper ballot and optical reader. This allows the authenticity of a human hand marking a ballot, an authentic hard copy for recounts, and the speed and accuracy of optical reading for initial counts. This system is simple, and removes many layers of possible tampering that exist in electronic machines, even those with a paper trail.

I worked as an election judge in my precinct last year, and a number of people expressed issues with the method in which the paper trail was generated. They said it was difficult to review, and they did not feel they had ample opportunity to verify that their choices on the computer were in fact reflected on the paper ballot. One person even left not feeling convinced that the record she saw pass under the glass on the machine was actually paper - she felt it was computer generated.

Public confidence in our election methods is crucial. This is a situation where perhaps using the latest technology creates more problems than it solves. What gives people the most confidence that their vote has been fairly marked and recorded? This should be a major issue in determining the method of conducting our elections.

Please consider returning to (or initiating) a paper ballot read by an optical scanner as our primary method of counting votes. In the case of those who need special access, electronic machines may be appropriate, but should be as secure as is possible, and should be open source, to ensure that all methods of collecting, recording, and counting entered information are known, and can be seen to be accurate.

Thank you for your commitment to ensuring free, fair, and accurate elections in this state.