Voters Have Reason to Worry

California’s “Top-to-Bottom Voting System Review” Leads to
(http://www.sos.ca.gov/elections/elections_vsr.htm)

“Withdrawal of Approval/Conditional Reappraisal” of Voting Systems

A Response to Election Officials & Others Who Encourage Voters to Trust

On August 3, 2007, California’s Secretary of State decertified Diebold’ and Sequoia touch-screen digital recording electronic (DRE) voting machines and forbid their use for California elections because

“the physical and technological security mechanisms provided by the vendors for each of the voting systems analyzed were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results”

California recertified Diebold and Sequoia DRE touch-screen machines for two specific uses

1. early voting, under strict supervision; and
2. on Election Day for the purpose of meeting federal requirements for people with disabilities, but there must be no more than one DRE touch-screen voting machine per polling place.

This recertification is conditional only if jurisdictions implement

1. manual audits of 100% of DRE touch-screen voter verifiable paper roll ballot records; and
2. increased “confidence-level” manual audits of all election results; and
3. stringent new security procedures for voting system hardware, software, and memory cards.

Maryland, Florida and other jurisdictions are eliminating the use of DRE touch-screen voting machines altogether because of cost, security, audit-ability, and reliability problems. With the announcement from California, more U.S. election officials and voters are calling for immediate changes.

However, Utah appears to be strangely unconcerned. According to KCPW.org reporter Julie Rose:

“The head of elections in California last week pronounced nearly all of the state's electronic voting machines vulnerable to hackers and unsuitable for the next election. Voters in the Golden State may end up using plain old paper for February's presidential primary. It turns out that Utah uses some of the same machines that California found lacking. But election authorities in the Beehive State [Utah] aren't worried.”

For a radio segment entitled “Sizing up Election Security” Rose interviewed Thad Hall, University of Utah Assistant Professor of Political Science. Hall’s representation of the “No Worry” viewpoint is available in his interview transcript (http://utahcountvotes.org/docs/ThadHall-KCPW-interview.pdf) and provides us with the opportunity to review the flaws in the “No Worries” perspective. This response compares Hall’s statements that encourage Utahns to experience “voter confidence” with the evidence from experts in computer security science.

Contributors to This Response

Kathy Dopp kathy.dopp@gmail.com, Barbara Bellows-TerraNova bellterr825@msn.com, Richard C. Johnson dick@iwwco.com, Erik Falor ewfalor@gmail.com, Danny Swarzman danny@stowlake.com, Joseph Holder conquip@mac.com, David Webber drrwebber@acm.org; Ellen Brodsky ebrod@yahoo.com (plus remarks from Ed Felton, Steve Freeman, & Charlie Strauss)
1. Hall Describes The California Top-To-Bottom Review

- “what would happen if you could fully get access to a voting machine and the whole of the software and nobody was around, and you could just play with it for a while”; and
- “this is what would happen if you did a security test of a bank and you turned off all of the security systems and you opened the vault.”

Fact: California’s top-to-bottom review consisted of a thorough examination of all voting system documentation, procedures and the equipment used to record and tally votes. The review had four components:

- A document review to examine manufacturer documentation, prior federal and state testing reports and reports of independent examinations and testing of voting systems.
- A source code review examined the human-readable instructions that are converted into machine-readable code to run the voting systems.
- Red team penetration testing in a hands-on effort to identify and document any potential for tampering or error in any part of the voting system’s hardware, storage devices or software.
- The accessibility of the voting systems was assessed for a broad range of disabilities.

The California red team had access only to the machines and no access to any of the programming instructions for the machine. The source code review team only had access to the source code and not the machine. These two groups did not confer. Both review teams had less access than any voting machine vendor programmer and had less access than state election officials who have access to escrowed code and to the voting machines. The red team had the same amount of access as county staffers who store or maintain the voting systems.

Access to the “bank vault” (election system) has already been widely available to various insiders, programmers and technicians at Diebold and other companies involved in the manufacturing of any part of the voting machines.

It is unknown exactly how much access Utah election officials and staffers have had or will continue to have because, in contrast to California, Utah election procedures and records are secret and unavailable for public oversight.

2. Hall Believes That Election Procedures Are Already Working

- “…in the real world we engage in a variety of security checks and have chains of custody that we use to secure these machines so that nobody could do that” and
- “he [Utah Lt. Governor Herbert] put some procedures that made sure that candidates felt comfortable with how it worked” and
- “effective procedures [are] in place for maintaining the chain of custody for these machines.”

Fact: While procedures and policies are important, we don't have any empirical knowledge of how effective any procedures in Utah or California have been. The California Red Team made recommendations for making procedures more effective, but after describing their recommended changes said
“Many, but not all, of the attack scenarios contained in these reports would be mitigated by fully addressing these three topics.”

The CA Secretary of State’s experts found that Diebold voting systems:

- “contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes”, and
- “that due to these shortcomings some threats would be difficult, if not impossible, to remedy with election procedures”.

Utah keeps its security and chain-of-custody procedures secret from the public.

Any time security procedures are known only to insiders, one can bet that some insiders know all the possible security holes and have access to subvert their own secret security procedures.

Even assuming that Utah does have good security procedures, in the real world, things rarely will go as planned. Therefore, both the software and hardware should be designed to be resilient against the cleverest assault possible.

Dr. Avi Rubin, Professor of Computer Science at John Hopkins University and Director of the National Science Foundation’s ACCURATE Center (A Center for Correct, Usable, Reliable, Auditable and Transparent Elections) and other computer scientists have shown that these electronic ballot voting machines were designed to count votes first, and then maybe added something akin to security afterward.

3. Hall Touts Previous California Functionality Testing

- “testing of voting systems on Election Day to make sure there was no tampering going on and all states have benefited from that too, because they can know that these systems are working effectively”

**Fact:** “Program testing can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence.”

The idea that testing ensures performance is a fallacy unworthy of any computer scientist. The testing may provide some (but not certain) knowledge of what may be expected in the way of performance. A bad design is not improved by any amount of testing.

An important question is “What lines of the code are actually exercised by the testing being done?” Test coverage alone does not ensure performance, but the absence of coverage guarantees that the uncovered code has not been tested. A competent engineer will provide an informed risk estimate for the code not tested. Functionality testing is very limited.

Diebold has previously not allowed penetration testing or source code reviews that would reveal the kinds of problems California is reporting.

"Routine" functionality testing (called “logic and accuracy” testing by election officials) may be just banging on it, black box monkey testing, where you have no idea what is inside the box. Respectable
companies do white box testing, in which it is known what is in the box, the better to test it. And do regression testing...and do human factors testing...and so on.

According to Richard Johnson, an expert in applications security and voting architectures formerly with Oracle Corporation,

“The Voting System Testing Lab (VSTL) testers I have queried actually tell me that they do their "real" testing for DOD and NASA, while for voting machines they follow the EAC recipe and checklists. No regression testing, no white box, no coverage analysis, no risk estimation of code proven to have remained untested. The VSTL will just do what the customer wants. What is that? Oh, it is secret! This is not at all state of the art testing, on the part of the vendor or on the part of the VSTL. Rather, it is a farce, and an expensive one at that.”

Supposedly, the revealed code of the vendors--what they show of part of the total software they use to authorized parties (not the public)--could be subjected to systematic code review by experts. Is it? Well, now, that is proprietary information and is a secret, as is whatever the VSTL does.

Because electronic ballots must be programmed separately for each election, California functionality testing in a prior California election should not give Utahns any confidence that Utah’s voting machines are working properly today. Those benign results cannot be applied to what occurs on a different day, with different machines, in different circumstances, in a different state, with different officials and procedures.

There are several ways to approach security. Either you try to build a fortress against intrusion. Or you build systems which demonstrate when malfunctions, mis-operation, misalignment, program errors and intrusions occur. Utah has done neither.

4. Hall Rallies Behind Voter Confidence

- “surveys of poll workers and voters, in the last two election cycles, and one of the things we've found is that … voters here, they are confident about the machines” and says that
- “people who listen to a lot of media weren't as confident; and once they went and voted, and the process worked for them, it turned out that people tended to be very confident that their votes were counted accurately, and … people in Utah, states with voter verified paper trails, with DREs, tended to be highly confident voters.”

Fact: Security cannot be measured by uninformed citizens’ misplaced trust.

Utahns, as well as other voting citizens, busy with their jobs and families, tend to believe what they are told. And they have not been told much. The local news media has been unusually unwilling to address the important issues or to ask penetrating questions.

The State of Utah also hired Salt Lake City-based public relations and advertising agency, Richter7, to handle how the Diebold voting machines were presented to Utah voters once they were purchased. Richter7 was also the PR firm that handled the presentation (“sales pitch”) to the State of Utah on behalf of Diebold. When the Lt. Governor’s office began its “Leave your print” campaign to build voter confidence in preparation for the 2006 election, the word “Diebold” was significantly missing, since the company’s elections systems were already gaining a bad reputation nationwide.

8/28/2007

Permission to reprint in part or whole with a link to this article on “Utah Count Votes” and attribution of authorship.
Unfortunately, the little reporting that has been done on voting systems in Utah has too often been based on quotes from those who have a stake in the system rather than going directly to the work of independent voting system experts – such as readable reports of the CA Secretary of State’s office, or the report of Harri Hursti, or the report and video at Princeton University’s Center for Information Technology. (http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold.pdf http://www.sos.ca.gov/elections/voting_systems/ttbr/red_diebold.pdf http://www.blackboxvoting.org http://www.blackboxvoting.org/BBVreportIIunredacted.pdf http://itpolicy.princeton.edu/voting/)

The 2006 election audit in Utah was a prime example of an inaccurately reported story based on what officials wanted voters to hear. The flaws in Utah’s internal election audits, which never compare the voter verifiable paper records with the unofficial vote counts on the Diebold central tabulator, were pointed out by Utah Count Votes and The Desert Green Party of Utah – yet were never investigated or reported by Utah press, which ignored valid independent audits of Diebold machines which have consistently revealed the machines’ inaccuracy in recording and tabulating votes.xii

Does it matter how much confidence the public has if votes are not counted accurately and elections are possibly being manipulated by Diebold or election official staffers?

Previously Utah’s computer scientists responded to a survey study done by Thad Hall and Political Scientist Michael Alvarezxiii that claimed to show that Utahns felt confidence in electronic voting, and found that their study was flawed and its findings not based on its own survey questions.xiv

5. Hall Lauds The Paper Trail

➢ “when you vote on the DRE here in Utah, you know you vote on the screen, and then when you review your ballot electronically you're also reviewing the voter-verified paper trail.”

Fact: First, any programmer understands that it is trivially easy to show one candidate on a computer screen, record another candidate inside the computer’s memory, and print an entirely different candidate on the paper ballot records.

Additionally, studies have shown that from 70% to 100% of voters do not verify their paper ballot records when they vote on a touch-screen voting machine.

6. Hall Continues With The Paper Trail

➢ “not everybody has to check their paper trail for us to know that the machines are working effectively. As long as a certain percentage of people do, you know, we can be relatively confident.”

Fact: DRE printed paper ballot records can be manipulated in several ways so that the paper ballot records match erroneous machine counts rather than the voters’ choices; or to make DRE printed ballot records unavailable for auditing.

Utah election officials have not conducted any valid manual audits that would measure the accuracy of Utah’s unofficial vote counts against voter verifiable paper records – even if those paper ballot records were an accurate complete record of voter intent.
The Brennan Center, the California top to bottom review, computer scientist Rebecca Mercuri, New Jersey State testing, and Verified Voting have all described methods of altering printed DRE paper ballot records in different ways that would subvert manual election audits.

7. **Hall Addresses The Correction Of Problems**
   - “If problems arise, we can fix all machines at once”

**Fact:** Obviously machines must be fixed one at a time since we are assured they are not networked.

However, how can Utahns believe that such corrections have been made or will be made when, so far, there is no admission of any problems by Utah election officials?

Did they respond to the security flaws discovered in Emery County, Utah by Bruce Funk and Harri Hursti in 2006?\(^{xv}\)

Are Utah election officials going to ignore California’s new standards, such as routinely reformatting and reinstalling all voting machine software, including not just the touch-screen units, but also the central tabulators and memory cards, with known clean versions of all software before each election, using three separate isolated servers in each county?

Utah election officials, to our knowledge, claim that there are no problems with our voting machines, so are they taking actions to “fix all machines” or are they simply “trusting Diebold”?

8. **Hall Promotes Diebold Procedures As Sufficient**
   - “What you would do with the machines, the cartridges would be put in the machine, sealed, they would be tested that they were zeroed”

**Fact:** A corrupted Diebold memory cartridge (which could come already corrupted from the factory) has already been shown in Florida by Harri Hursti to easily print a zero tape showing that it had no votes, when in fact, the card was pre-set with votes for one candidate and to subtract votes from the opposing candidate.\(^{xvi}\)

The Princeton study by Professor Ed Felton showed that a virus can be spread from a single corrupt memory card to the Diebold central tabulator and back to all Diebold memory cards. Any computer program can easily print one result to a screen or paper while storing a different result.

9. **Hall Lauds Utah’s Election Audits**
   - “and you would audit the paper record to make sure the electronic tally and the paper tally add up. And that's what we're doing here in Utah”

**Fact:** Once and for all, this is the truth about Diebold and “auditing”:

The Election Science Institute and Cleveland State University showed that Diebold voting system is not auditable on the DRE machine level.\(^{xvii}\) The Diebold central tabulator which adds up all the vote counts is not capable of printing a report of all the vote counts for each race on each DRE voting machines. Therefore the individual DRE voter verifiable paper ballot records (VVPR) cannot be compared with the
individual DRE counts for each candidate on the Diebold central tabulator. The only way to audit Diebold voting machines is to count the VVPRs for entire precincts and compare the manual counts with the precinct counts on the central tabulator.

Utah’s internal election audit procedure never compares any voter verifiable paper record (VVPR) tallies with any record of unofficial vote counts; instead Utah compares the VVPRs with alleged DRE vote counts printed from the same DRE’s memory card (the DRE “vote totals tape”). There is no reason to believe that either of these counts matches the unofficial vote counts. Utah’s “audit” is easily manipulated in several ways.

Utah is one of the few states which do not print and publicly post polling place totals at the polls on election night, so that the polling place totals and the DRE totals on any of the unaudited or even the audited DRE voting machines could be entirely different in the central tabulator which tallies the votes.

The tally of absentee and military votes also affects the final announced count. How this tally is done and added into the GEMS final tabulation remains to be disclosed; are there even audit procedures for this important step?

10. Hall Addresses Attack By A Voter

- “hypothetically you could … break into a machine using a screwdriver … Of course, in a polling place… hopefully the poll workers will be paying attention, and notice that you are unscrewing the voting machine and taking it apart, much like you would hope that, in an analogous attack, if you started stuffing a paper ballot box, they would also notice.” Hall adds

- “in Utah, and in other states, we require voting machines to be set up in a way that people can see the machines, so that an observer or a poll-worker can notice if somebody is doing something that seems untoward to a voting machine.”

Fact: The California report presents scenarios of attack that include what can be done in the same time it takes to vote, with no more privacy than one is given when voting. They have also found the machines vulnerable to attacks from remote locations.

In addition, Thad Hall (and presumably the Utah Lieutenant Governor’s office as well) are primarily concerned with an attack by an outsider (voter). All of the procedures and policies that Hall touts are designed to protect against an attack by someone who is not connected with either Diebold or the state/county election office.

While we are glad that Utah officials are taking possible voter attacks into consideration, it completely misses the point that attacks against any system primarily come from within – and indeed, may already have occurred, programmed to take effect in future elections.

As long as anyone outside of Diebold Inc. cannot see the source code for the binary which will be running the DREs on Election Day, we'll never know if we're being attacked from within. If people would stop long enough to think about how secure their Windows PC is despite that source code being under Microsoft's hat, they would get a clue why computer scientists assert that "security through obscurity" does not work. The DOD, (the Navy in particular) and several other federal government
operations are moving to Linux, because it is open source. Granted, they surely make modifications, but it speaks a lot that they use open source software as their base.

Thad compares opening a DRE with a screwdriver to stuffing the ballot box. This trivializes the problem significantly. Ballot box stuffing was easily discovered and was limited. Time and time again, analysts and investigators have reported that electronic votes can be invisibly miscast, switched, miscounted – without leaving a trace of the security breach. Stuffing ballot boxes is hard work compared to automating the work with an electronic voting machine.

Electronic ballot boxes could be being stuffed right under the noses of the most honest election officials, poll workers, technicians, and voters in Utah and they would never know it. To suggest that poll workers would be able to “notice” vote theft makes Mr. Hall appear to be either uniformed or misinforming because it is humanly impossible for anyone to read the bits and bytes inside a touch-screen voting machine or a central tabulator during elections.

11. Hall Says That Diebold Voting Machines Can Be Made Physically Secure From Voters
   ➢ “whether or not the machines are sealed and secured properly so that you can't access those locations. I know that in Georgia, for instance, they had Diebold re-structure the stands that they used so that none of those openings could even be accessed.”

Fact: Studies done at Princeton and elsewhere that show that access to Diebold voting machines can be obtained without even breaking security seals.\textsuperscript{xvi} Again, voters during elections are the least likely to cause vote fraud, ballot programming errors, denial of service attacks, electronic failures, and the like.

12. Hall Says Touch-Screen DREs Reduce Under-Votes
   ➢ “there is some evidence that DREs can be more effective in making sure that people complete their ballot. For instance, it becomes harder to skip races down ballots that you wouldn't skip because you are pushed through the ballot and not flipping through some cards or things like that on a punch card. And so you do get greater ballot completion, some studies have shown,”

Fact: To the contrary, election data shows that the rate of under-votes, where voters do not cast votes in particular races, and sometimes forget to cast their entire ballots, have skyrocketed with the use of DRE voting machines. In Utah the secrecy of election records prevents us from knowing what the under-vote uncounted ballots rates are,\textsuperscript{xvii} but in states like Florida, Ohio, and New Mexico where election records and data are publicly available and analyzed, under-vote rates are soaring with the use of DRE voting machines – in clearly suspicious ways that seem to primarily favor the candidates of certain political parties.

Most recent implementations of precinct optical scanning of paper ballots present warnings of over or under voting. Mr. Hall thus presents a distinction without a difference.
13. **Hall Admits A Benefit To The California Study - Leveraging Vendors**

- the benefit of the CA Bowen studies to Utah is to “leverage the vendors to provide us with the most up-to-date and secure software based on the modifications they make to meet the California requirements.”

**Fact:** Thad Hall and Utah’s election officials put their trust into the hands of private companies to secretly cast and count Utah’s votes using trade secret software, and have ignored efforts by other states to evaluate Diebold voting machines.

So voters must blindly trust in the good intentions and infallibility of thousands of programmers and technicians who create voting systems software, firmware, and operating systems.

Here's an excerpt from Princeton University Computer Scientist Ed Felton's blog that shows that Diebold is not to be trusted to fix its voting system flaws:

> Some of these are problems that the vendors claimed to have fixed years ago. For example, Diebold claimed (p. 11) in 2003 that its use of hard-coded passwords was “resolved in subsequent versions of the software”. Yet the current version still uses at least two hard-coded passwords — one is “Diebold” (report, p. 46) and another is the eight-byte sequence 1,2,3,4,5,6,7,8 (report, p. 45).

Similarly, Diebold in 2003 ridiculed (p. 6) the idea that their software could suffer from buffer overflows: “Unlike a Web server or other Internet enabled applications, the code is not vulnerable to most ‘buffer overflow attacks’ to which the authors [Kohno et al.] refer. This form of attack is almost entirely inapplicable to our application. In the limited number of cases in which it would apply, we have taken the steps necessary to ensure correctness.” Yet the California source code study found several buffer overflow vulnerabilities in Diebold’s systems (e.g., issues 5.1.6, 5.2.3 (“multiple buffer overflows”), and 5.2.18 in the report). [http://www.freedom-to-tinker.com/?p=1184](http://www.freedom-to-tinker.com/?p=1184)

We’ve heard this same song too many times now. “Well those bugs were fixed in the latest release.” Charlie Strauss says, “I even had one person who was working for the SOS tell me that, even though the bug found in an older version was rediscovered after the latest release, [the vendor claims] that they might have fixed it in the latest release by accident despite not knowing it was present so he had no reason to believe the bug in the old release was still present. Argg!”

Many lies have been documented: Diebold and ES&S have both falsely represented code as certified when it was not and ES&S according to Dan Rather, even represented hardware as passing humidity tests that it did not pass.xxii

These voting machine companies have earned a “guilty until proven innocent” reputation. They need to open the source code and prove any claim they make is true.

As far as the public is aware, Utah has never hired any independent computer experts to verify the claims that Diebold makes about its voting systems. Worse, the Utah Lt. Governor’s office and the Utah Attorney General’s office were complicit in running former Emery County Clerk Bruce Funk out of office when, in early 2006, he allowed independent security experts to examine Diebold voting systems and discovered gaping security flaws that had been originally been uncovered in early 2003 – and not fixed by 2006xxiii. Pennsylvania took action to secure its Diebold voting machines following Funk’s discovery, but to our knowledge, Utah’s only response was to change the locks on Funk’s officexxiv.
14. Hall Says Don’t Worry

➢ “I don't think that the state needs to take the same type of actions she [CA Secretary of State Debra Bowen] did.”

**Fact:** Thad Hall seems to be a trusted advisor to Utah election officials, despite his lack of any computer science expertise or credential. He is, remember, a political scientist.

Hall’s statements, plus the lack of any formal response to the California announcement and findings on the part of Utah’s election officials, seems to indicate that Utah’s election officials plan to do nothing whatsoever to secure Utah’s voting machines from tampering or error.

Such denial cannot help but make one wonder just what Utah election officials are trying to cover up.

15. Hall Makes It Political

➢ “If you're a Democrat and you look at 2000 and 2004, and the presidential races, you know, you think "How did George Bush beat these two candidates?" and then in 2000 there was the added controversy of Florida; and in 2006 when the Democrats win, well it's hard to say that the system doesn't work when our candidates won.”

**Fact:** This is hardly a sore-loser issue. Studies of exit polls and vote patterns following the 2006 federal election are consistent with greater wins, in fact a landslide, for Democrats, if votes had been counted accurately. xxv There are 2006 federal races that are still being contested based on anomalous unverified electronic vote counts, and more elections that probably should have been contested due to anomalous vote counts.

Wouldn’t it be better to know for certain that election outcomes are correct by taking the same measures as California has, including confidence-level manual audits of paper ballots?

16. Hall Turns To Persons With Disabilities

➢ “Now, obviously, the problem … is whether paper systems are accessible, and obviously to people who are blind, or who have physical dexterity problems, they're also not accessible.”

**Fact:** Touch-screen paper ballot printers for voters with disabilities handle more types of disabilities and allow voters with disabilities to verify their own paper ballots. Although the ballot printers, which print durable individual paper ballots, are not totally adequate for voters who cannot remove their ballots themselves from the printer, the BMDs work better with wheelchairs and allow voters with disabilities to verify their own ballots and do not violate voter anonymity for all voters like the DRE paper rolls and DRE electronic ballots do. No voter in a wheelchair can inspect the paper tape easily unless it is directly next to the screen, a very uncommon approach in DREs.

Ballot printers used with blank pages put out before and after the ballot can be handled by assistants without violating privacy of the disabled voter; the assistant simply puts all three pages through the scanner by putting them in the hopper. Only the ballot will register and the three pieces of paper can be
Utah Count Votes

dropped into a ballot box without looking at the choices. Poll watchers can verify that the assistant does not peek.

Conclusion

It would behoove the Utah Lieutenant Governor's office to hire a few competent and credentialed consultants who could give guidance about critical software systems. While one may respect Mr. Hall’s good intentions, we do not feel that he is the best man for the job.

We recommend that people go directly to source -- the easy-to-read findings and decisions at the California Secretary of State's website, rather than believe the “pooh-poohing” of Hall or Utah Lt. Governor’s Chief of Staff Joe Demma. The information our voters need to know about the California Secretary of State's decision regarding Diebold are posted online here: http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold.pdf And here is where you find the report from the Computer Scientists (more apt description than the pejorative term "hackers"): http://www.sos.ca.gov/elections/voting_systems/ttbr/red_diebold.pdf.

It is worth knowing the facts. According to Computer Science Graduate Erik Falor "If I wrote code like what I saw in Dr. Rubin's original paper on the [Diebold] DREs, I would never have passed enough computer science (CS) classes to graduate. They were breaking coding conventions that I was taught about in my very first CS class."

It is the technical issues that we are sure go way over Thad Hall's head. Which is why this state should start listening to its computer scientists and national voting system experts like those financed by the National Science Foundation as part of project ACCURATE.

Election officials are telling us that we should trust their choice to subcontract elections processes to private companies and that we should be satisfied even though the process is secret. These are untenable positions if democracy is going to continue in this country.

It is time for Utah election officials to:

1. do their job and hire real independent experts in computer science rather than believing whatever voting vendor salespersons tell them; and
2. admit that they made a costly mistake in purchasing Diebold DRE voting machines; and
3. subject elections to valid independent scientific manual audits to make sure that Utah election outcomes reflect the will of voters; and
4. stop keeping election procedures, records, and data in Utah secret in order to hide the evidence of problems with our elections systems and voting machines; and
5. implement at least as stringent election security procedures as California requires.

No reasonable person expects completely problem-free elections, but we do expect our election officials to make every effort to uncover and expose and correct the problems with our election systems and invite the public to help them oversee the integrity of the electoral process. Public elections should be open to the inspection of the public, by the public, and for the public which the Utah officials supposedly serve.

11 8/28/2007
Permission to reprint in part or whole with a link to this article on “Utah Count Votes” and attribution of authorship.
Additional Information


The National Election Data Archive's Testimony on "The Ballot Integrity Act…” (S1487) (includes a list of problems that DRE voting machines cause) [http://electionarchive.org/ucvInfo/US/NEDA-S1487-Testimony.pdf](http://electionarchive.org/ucvInfo/US/NEDA-S1487-Testimony.pdf)


Utah's Computer Scientists Warned Utah's Election Officials Against Purchasing DRE Voting Machines, October 20, 2004 - [http://utahcountvotes.org/voting_system_advice.pdf](http://utahcountvotes.org/voting_system_advice.pdf)

This document is posted at: [http://utahcountvotes.org/UT/UtahCountVotes-ThadHall-Response.pdf](http://utahcountvotes.org/UT/UtahCountVotes-ThadHall-Response.pdf)


v FL’s HB 537 bans all DRE voting machines altogether by 2012. Florida will allow one DRE per polling location and DRE use for early voting for voters with disabilities in the meantime. However, in CA there will be the thermal voter verifiable paper audit trail (VVPAT) for DRE machines that will have to be 100% manually counted; whereas in FL there will be no VVPAT so votes cast on DREs will have no paper backup until 2012 unless the county decides to purchase ballot marking devices or Federal legislation such as HR811 is passed. Maryland’s legislature recently passed a bill which will replace all DRE voting machines with optical scan paper ballot systems for all voters by 2010.

vi On the list of steps CA is taking - is improved result reporting to media and transparency - see this site for participants getting started on being able to process XML for 2008. It's using the new EML 510 format from v5.0 http://www.sos.ca.gov/elections/ca_elect_results/result_example.htm Obviously this can provide media across the country with faster and more accurate details on election results in 2008 and provide analysts the ability to more easily do election result mathematical analysis to detect any suspicious vote patterns. See website downloads link for more details.

vii It should also be noted that Mr. Hall is under contract with the U.S. Election Assistance Commission (EAC) to study state vote counting laws and procedures. The EAC is a federal agency created by the Help America Vote Act. However, it is worth noting that the EAC is widely seen as a corrupt, incompetent, politicized agency that has not accomplished its Congressional mandates. The EAC recently came under fire when it was discovered that it put a gag order on Tova Wang, the co-author of a report it commissioned, when the report showed that the allegation of “voter fraud” so widely spread by the Republican National Committee, and recently noted as the reason for firing of U.S. Attorneys, is, in fact, a non-issue, rarely seen, insignificant, and a distraction from actual election vote theft and voter intimidation issues. The EAC also had to be threatened with legal action by the state of New York before it publicly released records relating to the decertification of the Independent Testing Authority which tested roughly 70% of all U.S. voting systems for federal certification.

viii See “Frequently Asked Questions About SOS Debra Bowen’s Top to Bottom Review of California’s Voting Systems” http://www.sos.ca.gov/elections/voting_systems/ttbr/ttbr_qa_final_081507.pdf The Secretary of State contracted with the University of California (UC) to assemble three review teams that relied on specialists from UC, as well as from public and private universities and private sector companies throughout the United States. Specific experience in voting system technology and security experts from other fields who had no experience with voting system technology were asked to participate. The two Principal Investigators for the project were Matthew Bishop, Professor in the Department of Computer Science and Co-Director of the Computer Security Laboratory at UC Davis, and David Wagner, Associate Professor in the Computer Science Division at UC Berkeley, with extensive experience in computer security, cryptography and electronic voting. David Wagner is a founding member of the ACCURATE center, which is funded by the National Science Foundation to research ways that technology can be used to improve voting. The accessibility of the voting systems was assessed by a single team of two accessibility experts, headed by Noel Runyan, an electrical engineer and computer scientist with over 33 years experience in designing and manufacturing access technology systems for people with disabilities. There were 42 experts involved with the teams.

ix Utah election officials clamped down on public access to election records in 2006 after implementing Diebold touchscreen voting machines. Kathy Dopp appealed the denial of public access to election records and detailed DRE vote counts and was denied in her appeal to the Utah State Records Committee. (See http://utahcountvotes.org/UT/UT-Election-Records-07-02DoppOrder.pdf and http://utahcountvotes.org/docs/Dopp-v-SummitCountyHearingBrie2.pdf ) Utah’s election statute needs to be rewritten to provide public access to election records that are necessary for the public to evaluate electoral integrity and which is customary in other states.

x The Red Team report overview is posted at: http://www.sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf


Utah election “audit” procedures are posted here: http://utahcountvotes.org/ltgov/ElectionXPolicy.pdf and an analysis of
the flaws of Utah’s audit procedures is here: http://utahcountvotes.org/ltgov/Response2LtGov-Audit-Recount.pdf
xiii Michael Alvarez’s vita http://www.hss.caltech.edu/~rma/vita.pdf
xiv September 2004, “Response to Response to: “American Attitudes about Electronic Voting” Survey By Thad Hall and
Michael Alvarez http://www.vote.caltech.edu/Reports/fall04survey.pdf And Advice for Utah’s Voting Equipment Selection
http://utahcountvotes.org/Voting_systems.pdf
xv Diebold TSx Evaluation - SECURITY ALERT: May 11, 2006 - Critical Security Issues with Diebold TSx -
system software in early 2006 in response to security flaws discovered in Emery County, Utah by Bruce Funk and Harri
Hursti.
xvi See HBO’s film “Hacking Democracy” and the report at www.blackboxvoting.org
xvii Ibid footnote xii.
xviii Hawaii is another state which, like Utah, does not publicly post polling place totals on Election Night. In addition Hawaii
sends all its DRE memory cards to a central state location and bi-passes county election officials; and conducts insufficient
election audits. Systems like Utah’s and Hawaii’s provide little, if any, confidence that vote totals are not manipulated in
transit or at a central location after leaving the polling locations, or innocently miscounted without detection.
xix During the November 2006 election in Summit County the police were called to remove Kathy Dopp from a poll closing
because Dopp took a picture of the DRE vote totals tapes; and in Salt Lake County another Utah League of Women Voters’
member who was a poll worker was threatened with eviction from the poll closing because she tried to video the poll
closing, including the vote totals tapes. These same DRE vote totals tapes are routinely publicly posted in other states
because they contain the summary vote totals for each DRE voting machine. If Utah officials are confident of the accuracy
of Diebold’s vote counts, why are they hiding the DRE vote count reports and other election records from public scrutiny?
xx See some of the reports linked under “Security Reports” at http://www.countedascast.com/issues/security.php Diebold
left a picture of its key on the Internet and keys made from this Internet picture were successfully able to open up any
Diebold voting machine. Also, the same key could be ordered on the Internet and opens hotel mini-bars and other common
items. If one does not have a key, picking the lock takes ten seconds. i.e. To build a secure voting system one would have
to throw out the Diebold voting machine case.
xxi Ibid footnote ix.
xxii Why worry about voting machine vendors? Some examples include: Sequoia intentionally mislabeled rejected,
defective paper ballots targeted to Florida counties in November 2000 -- resulting in predictable over-vote ballot spoilage
(confetti chads). ES&S knowingly shipped rejected, defective touch-screens to Sarasota Co. Florida -- where 13% of the
Congressional votes were lost in November 2006 - costing the Democratic candidate the election. Diebold has been sued for
fraud on several occasions and settled out of court, and one of Diebold’s employees put a web site on the Internet where
stories were fabricated about election integrity advocates – and Diebold sales persons told election officials that this web
site was an “independent watch-dog” site, and Diebold advertised numerous fictitious non-existent office locations in the
white pages – telling election officials that it had a large presence in their states.
xxiii See the Harri Hursti BlackBoxVoting report on Diebold TSx voting machines.
xxiv See http://utahcountvotes.org for more information.
xxv July 2007, “Landslide Denied Exit Polls vs. Vote Count 2006 Demographic Validity of the National Exit Poll and the
Corruption of the Official Vote Count” Jonathan Simon, JD, and Bruce O’Dell
http://www.electiondefensealliance.org/files/LandslideDenied_v.9_071507.pdf
xxvi Joe Demma, Chief of Staff of Lt. Governor Herbert, fabricated stories maligning local Utah election integrity advocate
Kathy Dopp and released his fabricated stories to press and to Utah election officials; and Demma has also routinely
misinformed Utah press and the Utah legislature regarding Utah’s voting systems. See Joe Demma’s press release about
Kathy Dopp: http://utahcountvotes.org/JosephDemma_email.html and Kathy Dopp’s response
http://utahcountvotes.org/JosephDemma.html