ILLINOIS BALLOT INTEGRITY PROJECT

www.ballot-integrity.org

THE CASE AGAINST DIRECT RECORDING ELECTRONIC DEVICES

January 22, 2006

For further information concerning this document, please contact:

Laurence J. Quick
Chairperson
Illinois Ballot Integrity Project
PMB 191 – 2112 Galena Blvd
Aurora IL 60506
(630) 460-0857
quickinfo@qnc.us

Robert A. Wilson
Chairperson, Suburban Cook County Chapter
Illinois Ballot Integrity Project
635 Chicago Ave – Suite 127
Evanston IL 60202
(847) 644-2654
wilson@ballot-integrity.org

THE CASE AGAINST DIRECT RECORDING ELECTRONIC VOTING DEVICES

EXECUTIVE SUMMARY

This paper has as its geneis an earlier document, "The Case Against DREs," originally published on October 15, 2005. Since that time, a number of new developments have added information and documentation to our knowledge base, including the U.S. Government Accountability Office (GAO) report released only a week later. This has been followed by the release of several other reports, including a volume testing of DRE machines in California, the first larg-scale such testing. In December, a successful "hack" was carried out against optical scan equipment and several local election jurisdictions in Florida, California, Pennsylvania and Missouri have either declined to purchase or decertified DREs.

We have divided this paper into several sections which examine in detail some of the more important aspects of DREs and why we believe that the state of development of electronic voting machines has failed to show sufficient improvement since their widespread deployment a decade ago. We will show that the serious failures in security, reliability and accuracy which were brought to the fore in the 2000 presidential election have not been corrected and that the incidence of malfunctions has escalated.

In the introduction we develop an overview of problems with touch-screen terminals (DREs) and follow with examples of 10 serious failings of touch-screen devices in recent elections. The findings of the GAO report are touched on, highlighting key findings regarding operational failures, security lapses, miscounting of votes and poor certification processes. The GAO report leads to three sections which discuss in detail key areas where DREs fail to meet even minimum standards of security, reliability and accuracy.

- In the section on security, we discuss the weaknesses inherent in the source code, the primary basis of DRE operation, vulnerability to external and internal breaches and failures in procedures and standards.

- The section on reliability shows that electronic voting machines are prone to failure and do not meet minimum standards for ensuring that millions of voters are not disenfranchised by not being able to vote on machines that fail to "boot up," jam, switch votes from one candidate to another and just plain "crash."

- When we discuss accuracy, we find the most damning evidence of all: **These machines can't count!** In an environment of consumer fraud, DREs violate even the most elementary warranty of merchantability, they don't do what they are supposed to do: count votes accurately. In fact, DREs do not even compare favorably with the punch-card systems they are designed to replace.

We also briefly discuss our conclusions that the Voter-Verified Paper Audit Trail (VVPAT) produced by the Diebold Accuview printer and the Sequoia VeriVote printer are not compliant with the Illinois Election Code.

In the penultimate section we illustrate some alternatives to DREs. Some are in the development stage like Vote-PAD, but others like the AutoMARK and Populex have already been approved for use by persons with disabilities.

Finally, we conclude by summarizing our finds that touch-screen electronic voting devices simply don't measure up and shouldn't be accepted as an adequate solution for modernizing voting systems in Illinois.

Introduction

The Illinois Ballot Integrity Project is a not-for-profit, non-partisan civic organization dedicated to ensuring fair, accurate, and completely transparent elections. The Mission of the Illinois Ballot Integrity Project is to inform and educate the public, media and government officials about important election integrity issues and to promote the adoption of legislation and policies designed to secure the democratic process. It is for that purpose that we have prepared this White Paper on Direct Recording Electronic Voting machines (DREs) often called "Touch-Screen" voting machines.

We have prepared this document because Democracy in America is under attack. This threat does not originate in far- off lands we only visit by television; nor is it being perpetrated by fanatics whose ideology we can barely comprehend. No, this attack is being mounted right here at home, by corporations that want to control our votes, aided and abetted by a compliant media and by politicians beholden to those same corporate interests. The privatizing of elections, which is nearing completion, threatens to disenfranchise millions of Americans.

Privatizing the vote does not merely open the door to potential election fraud, it is, in and of itself, an egregious abuse of power, a transfer of another precious public resource—in this case the franchise—into the hands of powerful, entirely self-interested corporations. Unfortunately, our elected representatives and election officials haven't proven to be effective guardians of voter rights. Officials like Katherine Harris of Florida and Ken Blackwell in Ohio have made whole *careers* out of purge lists, voter intimidation, and aggressive partisanship in the administration of elections.

Privatized voting is a near-perfect example of how the undermining of government regulatory mechanisms leads to one-party rule and further deregulation in a self-perpetuating cycle. We see the same thing with the highly-concentrated corporate media. No conspiracy required for corporate entities to act in concert. Combinations are in their best interests, and successful corporations are all about finding and pursuing their own best interests.

Voting machine companies and their adherents dismiss concerns about election systems and potential fraud saying, "Your can't prove elections have been stolen." Yet the debate on whether or not we can *prove* an election was stolen, is an argument that neatly stands the problem on its head: the burden of proof ought not be on voters to prove fraud, but on voting companies and election officials to provide credible evidence of the security and reliability of their machines and the accuracy of election results.

The Illinois Election Code now mandates a verified paper record of the voter's choices. Yet electronic voting companies, like Diebold and their advocates have consistently opposed voter-verified paper ballots. One reason they give is that it's too expensive. That's somewhat humorous, given the billions of taxpayer dollars being used to buy these machines. If you accept that here's no objective verification of ballots without a paper trail, then electronic voting machines begin to resemble nothing more than $3,000 pencils. If Illinois taxpayers started to view them from this perspective, they might begin to wonder about the enormous ongoing expense of buying, installing and maintaining these unreliable and insecure devices.

Given the complexity of modern-day ballots and the numbers of voters, there's nothing inherently wrong with automating parts of the election process. Yet these same issues point to the overwhelming need for security, accuracy and reliability which must not be compromised for so-called speed or "efficiency." While computerized devices may yet prove to be a valuable election component, we suggest: not *these* machines, not now and not in Illinois.

A survey of the available literature suggests that an optimal voting system would have five attributes: 1) Privacy, the ability for each voter to cast a secret ballot; 2) Anonymity, the ability of voters to protect their choices; 3) Accuracy, a direct and verifiable tracking from voter intent to final tally. 4) Scalability, the ability to adapt to small and large voter groups; and 5) Speed, for an early tabulation and announcement.

For nearly a century, election officials and private companies have tried to convince us that to improve Speed and Scalability that Privacy, we have to sacrifice Privacy, Anonymity and Accuracy. All mechanical and electrical voting technologies involve translating the voter's intent in some way, many of them multiple times. And at each translation step, errors can occur and accumulate. We have seen ample evidence of this throughout our nation: Florida in 2000 Georgia in 2002, and in 2004, Ohio, Florida and several other jurisdictions. Mechanical/electronic voting machines have proven unequal to the imperative task of accurately tallying, compiling and reporting votes.

Accuracy is not measured by how well the ballots are counted; it's how well the process translates voter intent into properly tallying, compiling and reporting votes. The majority of voting problems are a result of translation errors. For example, a punch-card system has several translation steps: from voter to ballot to punch card to card reader to vote tabulator to centralized tallying. At each step-voters can be confused by the ballot's layout or may improperly punch choices.

Tabulating machines and their software can malfunction, either by accident or design. Ballots can be lost and not counted. Ballot subtotals can be misplaced and not counted in the final total. Because electro-mechanical systems are so prone to failure, we should rather be surprised by an accurate count, rather than failures in the process. The solution is simplicity. The fewer the translation steps, the fewer errors. Paper ballots are more accurate than computerized systems because there are fewer translation steps.

Hand marked paper ballots and precinct based optical scanners provide voters with essential advantages over expensive and unverifiable electronic “Touch Screen” (DRE) technology. Ballot marking technology allows a paper ballot based system to provide accessible, private and independent voting for voters with disabilities. Optical scan systems have been used in elections around the United States for over 20 years.

The accuracy of a voting system is often assessed by what is called the “residual vote”. This is the difference between the number of voters who turn up at polling stations and the total number of votes allocated to the candidates. Though voters can choose to spoil their ballots, if one system regularly produces a higher residual vote than another its accuracy may be questioned.

If we accept this criterion, the most accurate way to record votes is to use optical scanning machines. These work in a similar way to photocopiers, and register a voter’s pencil mark on the ballot by the amount of light it absorbs. These systems produced an average residual vote of around 2.1% during presidential elections from 1988 to 2000, according to a study to appear in the Journal of Politics by Stephen Ansolabehere and Charles Stewart of the Caltech-Massachusetts Institute of Technology Voting Technology Project.

On the other hand, touch-screen voting machines have a far higher residual vote of 3.0%. These machines register a residual vote when a voter activates the machine but then fails to cast a vote. Experts attribute the high residual vote on these machines to their sometimes confusing or annoying interface, which require voters to navigate a menu and touch the screen to register their vote for their preferred candidate. Punched cards have a residual vote of 2.9%. Therefore, based on residual votes, voter-verified paper ballots, read by optical scanners show a clear advantage.

The residual vote is not the only measure of the success of a voting technology. Of equal concern is whether voting machines can allocate votes to the wrong candidate or facilitate election fraud. This is where new voting technologies have attracted most criticism. Multiple independent studies in the past two years have identified problems with voting machines that could lead to vote tallies being mistakenly altered or deliberately tampered with The flaws affect both the hardware and software of machines made

by all major companies, but especially: Diebold Election Systems, Sequoia Voting Systems and Election Systems & Software (ES&S). Concerns have also been raised about machines made by other manufacturers.

Mistrust also stems from the unsatisfactory process by which machines are certified. Machines must first be "qualified" by an Independent Test Authority (ITA) which checks that they comply with federal standards, and then certified by the state. But the ITAs are paid by the machine vendors themselves. This is a clear conflict of interest.
Public trust in electronic voting is a major issue. DREs have proven to be an unmitigated disaster for voters and election officials alike. These touch-screen voting systems have a long history of multiple failures, both mechanical and electronic. Even though DREs have been used in elections for nearly a decade, they have demonstrated a wide variety of undesirable features and performance patterns arising from a variety of malfunctions of hardware, software and communications, both at the precinct and central tabulation locations.

These extensively documented failures have led to the disenfranchisement of tens of thousands of voters in many jurisdictions throughout the U.S. and have altered the results of dozens (if not hundreds) of elections. DREs add an unnecessary layer of complexity to voting systems which contributes to breakdowns and results in unacceptable results.

Ten Common Problems with Touch-Screen Devices

While many people are advocating the use of a voter-verified paper audit trail (VVPAT) on DREs, VVPAT wouldn't have been sufficient to fix many of the problems that counties have encountered using DRE systems. This fact causes many people to question the wisdom of using DREs at all, even if they have a printer attached.

Many different types of e-voting problems have occurred in recent years. Hundreds of elections have been impacted by malfunctions which have disenfranchised voters and called the results of elections into question. In some cases, paper backup was available, and election officials were able to determine the voters' intent. In other cases, there was no paper backup, and localities have either certified the elections anyway or conducted a second election to replace the first.

Hundreds of electronic election malfunctions have been reported in newspapers in recent years, more than 125 of them from the 2004 general election alone. Here are a few examples of common problems serious enough to be reported in the news.

1) Electronic Voting Machines Lose Ballots

Carteret County, North Carolina. November, 2004. Unilect Patriot DRE A memory limitation on the DRE caused 4,438 votes to be permanently lost. *Computer loses more than 4,000 early votes in Carteret***.** Charlotte Observer. November 4, 2004. Associated Press.
www.charlotte.com/mld/observer/news/local/10099907.htm

Palm Beach County, Florida. November 2004. **Sequoia *DRE*** *Battery failure causes DREs to lose about 37 votes.* Nine voting machines ran out of battery power. *Nearly 40 Votes May Have Been Lost In Palm Beach County*. Associated Press. November 2, 2004.

2) Electronic Election Equipment Inexplicably Adds Ballots

In the first two months after the 2004 General Election, phantom votes (more votes than voters) were reported in Florida, Nebraska, New Mexico, Ohio, South Carolina, and Washington.
www.votersunite.org/info/previousmessups.asp , Reports of additional phantom votes continued to flood into the news.

Mecklenburg County, North Carolina. November, 2004. Microvote DRE Results show nearly 3,000 more votes than voters. According to election-office data downloaded by the Charlotte Observer, 102,109 people voted early or returned valid absentee ballots. But unofficial results show 106,064 people casting early and absentee votes for president. *County Retallies Early-vote Results***.** The Charlotte Observer. Nov. 4, 2004. By Richard Rubin and Carrie Levine.
http://www.charlotte.com/mld/charlotte/news/politics/10094165.htm

Lancaster County, Nebraska. November, 2004. ES&S Optical Scanner. Optical scanners double-count ballots. As the optical scanners read the election-day ballots, they occasionally added votes. While County Election Commissioner David Shively explained that the software was reading ballots twice, ES&S referred to the misread as a mechanical problem. *Problem machines spur call for recount***.** Lincoln Journal Star. November 14, 2004. By Nate Jenkins.
http://www.journalstar.com/articles/2004/11/14/election/doc4189b9c7f14bf764391458.txt

Bernalillo County, New Mexico. November, 2004 Over 8,000 phantom votes appear in the canvass report. The New Mexico certified election results reported 2,087 phantom votes (more votes than ballots cast) for president statewide. These phantom votes were concentrated in Bernalillo County. The official canvass report shows 187 precincts in Bernalillo County reporting presidential phantom votes — a total of 1,239 votes. *Bernalillo County Canvass of Returns of General Election Held on November 2, 2004***.** State of New Mexico. http://www.sos.state.nm.us/PDF/Bernalillo.pdf

3) Tabulation Software Reaches 32,767 Votes and Counts Backwards

Broward County, Florida. November 2004. ES&S DRE System - Vote tabulation software loses 70,000 votes for Amendment 4. The bug, discovered two years ago but never fixed, began subtracting votes after the absentee tally hit 32,500 -- a ceiling put in place by the software makers. "Clearly it's a concern about the integrity of the voting system," said Broward County Mayor Ilene Lieberman, a canvassing board member who was overseeing the count. "This glitch needs to be fixed immediately."
The problem, which resulted in the shocking discovery of about **70,000 votes** for Amendment 4, a measure allowing a referendum on Las Vegas-style slots at parimutuels in Miami-Dade and Broward, came to light just after midnight Wednesday when Broward's canvassing board shut down.
*Gambling vote glitch mars tally***.** Miami Herald. November 5, 2004. By Erika Bolstad And Curtis Morgan.
http://www.miami.com/mld/miamiherald/10103931.htm

Orange County, Florida. November, 2004. ES&S Optical Scan System Vote tabulating software omits counting 8,400 votes. The precinct results posted on the Orange County elections office Web site showed that Democrat John Kerry beat Republican President Bush by 9,227 votes in Orange County, but the posted results were off by 8,400 votes. The margin was actually only 827 votes. The cause of the error, Orange officials said Thursday, was a software program that could not tabulate more than 32,767 votes in a single precinct. A similar discrepancy affected vote totals posted online for the U.S. Senate race between Republican Mel Martinez and Democrat Betty Castor. *Distrust fuels doubts on votes: Orange's Web site posted wrong totals***.** Orlando Sentinel. November 12,
2004. By David Damron, Sentinel Staff Writer. http://www.votersunite.org/article.asp?id=3803

Guilford County, North Carolina. November, 2004. ES&S DRE System - Vote tabulating software changes two outcomes in Guilford County. In Guilford County, ES&S early voting machines also had capacity problems. The totals were so large, the tabulation computer threw some numbers away. Retallying changed two outcomes and gave an additional 22,000 votes to Kerry. *Winner so far: Confusion.* The Charlotte Observer. November 5, 2004. By Mark Johnson.
http://www.charlotte.com/mld/observer/news/local/10104576.htm?1c

Ken Carbullido, Vice President of ES&S Product Development, explained the problem to Guilford County. In very technical language, he wrote that when the vote totals reached 32,767 (32K), the system began subtracting from the totals. The 32,767 capacity limitation at a single precinct level is a function of the design and definition of the results database used by ERM [Election Reporting Manager]. The data storage element used to record votes at the precinct level is a two byte binary field. 32,767 is 2 to the

15th power, which is the maximum number held by a two byte word (16 bits) in memory, where the most significant bit is reserved as the sign bit (a plus or minus indicator). Additionally, ERM precinct count level data is stored in a binary computer format known as two's complement.

4) Votes Jump to the Opponent on the Screen

Maryland. November, 2004. Diebold DRE - Some voters manage to correct the vote-jumping on the screen, some don't. On election day, TrueVoteMD registered 383 reports involving 531 incidents of problems encountered by voters. Among a myriad of other problems detailed in the report, many voters reported votes switching on the screens. Here are some excerpts: *When the Right to Vote Goes Wrong***.** TrueVoteMD. November, 2004. http://www.truevotemd.org/Election_Report.pdf

Snohomish County, Washington. November, 2004. Sequoia DRE - Voters find vote-jumping difficult to correct. Voters in at least four polling precincts in Snohomish County said they encountered problems with the electronic voting machines. When they touched the screen to vote for a candidate, voters said an indicator showed they had selected the opposing candidate. Those voters told KING5 News it took at least four attempts before the indicator showed the correct candidate. *Scattered reports of voters being blocked and machine malfunctions***.** November 2, 2004. KING5 News. http://www.king5.com/topstories/stories/NW_110204ELBelectronicvotingproblemsLJ.1aac5fda.html

Bernalillo County, New Mexico. October, 2004. Sequoia DRE -
Votes for Kerry jump to Bush. When the same problem occurred in Bernalillo County, New Mexico, it took some voters as many as three times to get the machine to register their votes for Kerry instead of switching the selection to Bush. *Some Early Voters Say Machines Mark Incorrect Choices***.** ABQJournal. October 22, 2004. By Jim Ludwick, Journal Staff Writer. http://abqjournal.com/elex/246845elex10-22-04.htm

5) DREs Provide Incorrect Ballots

Maryland. March 2004. The U.S. Senate contest was omitted from ballots in three counties. Jeffrey Liss had finished making his selections on Maryland's Democratic-primary ballot and strolled out of the polling place at Chevy Chase Elementary School on the morning of March 2, Super Tuesday. On the sidewalk, he spied a campaign posted for Senator Barbara Mikulski, who is running for her fourth term. Funny, he thought, he didn't remember voting in the Senate race. Liss went back inside to talk to an election official. And another, and another. He was told he must have overlooked the Senate race on the electronic touch-screen voting machine. But Liss, a lawyer, finally persuaded a technician to check the apparatus. Sure enough, it wasn't displaying the whole ballot. According to voter complaints collected by Mikulski, who won in the primary, her race didn't appear on ballots in at least three Maryland counties***. The Vexations of Voting Machines*****.** Time Magazine. May 3, 2004. By Viveca Novak.
http://www.time.com/time/archive/preview/from_redirect/0,10987,1101040503-629410,00.html

Orange County, California. March 2004 - Incorrect access codes gave voters incorrect ballots.
Poll workers struggling with a new electronic voting system in last week's election gave thousands of Orange County voters the wrong ballots, according to a Times analysis of election records. In 21 precincts where the problem was most acute, there were more ballots cast than registered voters. At polling places where the problem was most apparent because of turnouts exceeding 100%, an estimated 1,500 voters cast the wrong ballots, according to the Times' analysis of official county election data. Tallies at an additional 55 polling places with turnouts more than double the county average of 37% suggest at least 5,500 voters had their ballots tabulated for the wrong precincts. ***7,000 Orange County Voters Were Given Bad Ballots*****.** Los Angeles Times; March 9, 2004; By Ray F. Herndon and Stuart Pfeifer. Reproduced at: http://www.votersunite.org/article.asp?id=1476

6) Election-Specific Programming Miscounts Votes

Franklin County. Indiana. November, 2004. Fidlar Optical Scan System - Democratic votes were counted as Libertarian. Optical scan equipment counted straight-party Democratic votes as Libertarian votes. County officials and Fidler technicians agree that an election programming error in the Fidlar

optical scan system caused the miscount. One outcome was overturned when the program was corrected. *Fidlar admits election blip***.** Quad City Times. November 13, 2004. By Tory Brecht. Reproduced at http://www.qctimes.com/internal.php?story_id=1039447&t=Local+News&c=2,1039447

Carroll County, North Carolina. November, 2004. ES&S Optical Scan System - Vendor mis-programming caused the miscount. The chip supplied by ES&S for the election was incorrectly programmed and miscounted the votes for the JP District 2 race between Rocky Whitely and Duane Coatney. Once ES&S supplies a new chip for the optical scanners, the county will rescan the ballots for that contest. *Computer glitch blamed for miscount in JP voting***.** Star Tribune. November 10, 2004. By Anna Mathews, CCN staff writer. http://www.greenforesttribune.com/articles/2004/11/10/news/s1.txt

Lake County, Illinois. April, 2003. ES&S Optical Scan System - Vendor mis-programmed again. The problem was caused by a programming error that failed to account for "no candidate" listings in some races on the ballot, Clerk Willard Helander said Thursday. As a result, election results were placed next to the names of the wrong candidates in four different races, including in Waukegan's 9th Ward. Helander blamed the problem on Election Systems & Software, the Omaha company in charge of operating the county's optical-scan voting machines. She said a company official told her the programmers were unaware the county would have "no candidate" listings on its ballot. *Returns are in: Software goofed — Lake County tally misled 15 hopefuls***.** (reproduced) Chicago Tribune; April 4, 2003; By Susan Kuczka, Tribune staff reporter. http://www.vote.caltech.edu/mailarchives/votingtech/Apr-2003/0096.html

7) DREs Break Down During the Election

Maryland. November, 2004. Diebold DRE - Miscellaneous break downs plague voters. Excerpts from the TrueVoteMD report show some of the malfunctions that disenfranchised voters in Maryland. Voter Lavellette White at Francis Scott Key Middle School in Montgomery County tried to vote for the school board, but when she made her selection the screen went dark and the machine spit out her ballot card. The election judge told her there was nothing he could do. *When the Right to Vote Goes Wrong***.** TrueVoteMD. November, 2004. www.truevotemd.org/Election_Report.pdf

Voters and poll watchers reported some 531 incidents to TrueVoteMD. Some 201 of these were incidents involving machine malfunctions of various types. The other 330 involved human and organizational failures, including lack of privacy, denials of provisional ballots or the right to vote at all, long lines, and insufficient help from election workers.

Mahoning County, Ohio. November, 2004. ES&S DRE - Machines broke down in 16 precincts; others needed calibration. Many problems plagued the ES&S iVotronic touch screen voting machines in 16 of the 312 Mahoning County precincts. Some of the machines malfunctioned. Others had problems with the personal electronic ballot cartridge placed into the machines before each vote to count the ballots ... Also, there were 20 to 30 machines that needed to be recalibrated during the voting process because some votes for a candidate were being counted for that candidate's opponent. About a dozen machines needed to be reset because they essentially froze. *Errors plague voting process in Ohio, Pa***.** Vindicator. November 3, 2004. Vindicator staff. http://www.vindy.com/basic/news/281829446390855.php
Back up! We need back up! Roanoke.com. November 11, 2004. By Brian Gottstein. http://www.roanoke.com/columnists/gottstein/13719.html

Broward County, Florida. October, 2004. ES&S DRE - Break downs require voters to come back the next day. Hundreds of voters showed up to vote early at Howard Forman Health Park, so many that a decision was made to keep the voting facility open until 11 p.m. Some people waited in line from early in the day until after the sun went down. Unfortunately, for a group of about 50 people, the waiting did not pay off. A mechanical problem with the voting machines caused election workers to close down polling place. The group of 50 frustrated voters will have the opportunity to be first in line to vote today. Poll workers took down their numbers and names and will move them to the head of the line. For one couple, it may not be enough. They were voting on Sunday because they planned to leave on vacation today. Now they will have to choose to cancel their trip, or give up their chance to vote. Voters Turned Away After Waiting Hours. WPLG Local 10. November 1, 2004. www.local10.com/news/3878344/detail.html

8) Electronic Voting Machines Fail to Start Up

Bexar County, Texas. October, 2004. ES&S DRE - Uncharged batteries in several ES&S touch-screen voting machines hampered early morning voting at a southeast Bexar County precinct for about two hours today, officials said. Poll workers at Sinclair Elementary School realized just before 7 a.m. that the voting machines were dead. By 9 a.m., county technicians had powered up the machines, but not before dozens of people had left, either in frustration or because they were late for work. *Voting problems minor, but frustrating***.** San Antonio Express. November 11, 2004. By Tracy Idell Hamilton, Staff Writer. http://www.mysanantonio.com/news/metro/stories/MYSA110204.online. votingproblems.1a8d060b.html; Reproduced at: http://www.votersunite.org/article.asp?id=3650

Orleans Parish, Louisiana. November, 2004. In Orleans Parish and nearby parishes, ten polling places were reported to have machines that weren't working on election-day morning *Parish by parish list of voter machine problems called in by viewers***..** WWLTV.com. 10:27 AM CST November 2, 2004. http://www.wwltv.com/local/stories/wwl110204electionmishap.18e9b314.html

9) Registration Data Transmission Fails

Many counties used "electronic poll books" during the 2004 election, so that poll workers could connect computers to the general voter registration database and look up voters online rather than in a paper poll book. But as early voting got underway, failure after failure turned this supposed convenience into long waits and possible disenfranchisement for many voters. These failures occurred in Shelby County, TN; Broward, Hillsborough and Pinellas Counties, FL; Bexar and Tarrant Counties, TX; Ramsey County, MN; two thirds of all Georgia counties, and: Orange County, Florida, where a computer crash prevented voter verification. *Few Glitches Reported in Early Fla. Voting***.** The State. October 19, 2004. By Jill Barton, Associated Press. http://www.thestate.com/mld/thestate/news/politics/9952991.htm Adams County, Colorado, where officials could not connect their laptop computers to the central voter registration database. *Early Voting Begins In Colorado***.** October 18, 2004. By Steven K. Paulson, Associated Press Writer. http://news4colorado.com/campaign2004/local_story_292161858.html

10) Memory Cards and Smart Card Encoders Fail

Collin County, Texas. November 2004. - Flawed memory cards were sent to Canadian labs to retrieve the data.Diebold touch screen voting machines locked up on election day. Election officials couldn't retrieve the results of the 63 ballots held on the memory card. County technicians couldn't retrieve the results. Diebold technicians in McKinney (home of Diebold Election Systems) couldn't retrieve the results. So the county sent the memory card to Diebold labs in Canada where technicians were able to get the totals.

As the editorial points out, "The mere fact that a piece of Collin County's election record left the country should be cause for concern." *Editorial: Put It on Paper — Election snafu points up problems for all-electronic voting***.** Dallas Morning News. November 11, 2004. http://www.dallasnews.com/sharedcontent/dws/news/city/collin/opinion/stories/111204dnccocollinvote.9eeb3.html

Volusia County, Florida. November 2004. Diebold Optical Scanner - Memory cards were inspected in the summer, failed in the fall. Memory-card breakdowns in six machines left political contests in limbo for hours. The county had the memory cards inspected by Diebold in the summer of 2004 in preparation for the busy election season. Ion Sancho, the elections supervisor in Leon County, said officials with Diebold told him that the new, higher-capacity memory cards tend to have more glitches than older cards. *Computer glitches slow Volusia results: County officials ask the machines' supplier to investigate why memory cards failed Tuesday***.** Orlando Sentinel. November 4, 2004. By Kevin P. Connolly, staff writer. Reproduced at http://www.votersunite.org/article.asp?id=3694

San Diego County, California. March 2004 Diebold Precinct Control Module - Encoders allow multiple votes ... or none. At least one voter was able to vote twice on her "smart card," and at least 250 polls opened late because poll workers were unable to start up the encoders. Hundreds, perhaps thousands, of

people were turned away – many of them disenfranchised because they were unable to return to the polls at a later time that day. *Poll workers, voters cite tied-up hotline, poor training, confusion.* Union Tribune; March 7, 2004; By Jeff McDonald and Luis Monteagudo Jr. http://www.signonsandiego.com/news/politics/20040307-9999-1n7vote.html

Later reports estimated that this problem delayed the voting at 40% of the polls and may have occurred at as many as 80% of the polling places. *Correspondence, written report regarding Touchscreen voting system used for the first time March 2, 2004 by the County of San Diego***.** From: Walter F. Ekard; Chief Administrative Officer http://www.signonsandiego.com/news/politics/county/20040310-1315-report.html While these problems were originally blamed on poll workers, a report released on April 12, 2004 by Diebold Election Systems shows that 186 of 763 encoders failed on election day because of hardware or software problems or both, with only a minority of problems attributable to poll workers. Diebold also admitted that tabulation errors during the October recall election were due to software bugs. *Diebold reports multiple problems: Registrar wants reason for e-voting***.** Tri-Valley Herald; April 13, 2004; By Ian Hoffman, Staff Writer. http://www.verifiedvoting.org/article.asp?id=1839

The above list is by no means exhaustive, but it does impart the flavor of both how widespread and serious the problems have become. Election activists have been largely dismissed as kooks, freaks, conspiracy theorists and nuts. This despite the fact that dozens of groups with differing agendas have been examining election problems with an increasing degree of success over the past five years. The debacle in 2000 planted the seed and a full-grown movement has followed. Killing the messenger is a time-worn but effective methodology. Interestingly enough, voter activists have enlisted one important segment in their criticism of electronic voting machines, the academic community, with well-known and respected computer, information technology and security experts weighing-in on the side of elctronic machine critics. We'll discuss this in greater detail, *infra*.

However, despite the furor of the attack by voting machine corporations and their allies, the controversy hasn't died away, but rather become more intense in the wake of the 2002 and 2004 elections. Concerns about election integrity are being aired in the mainstream press with increasing frequency, though the issue is still not receiving the attention it deserves. Last fall, that started to change when Congressional action came to the fore.

The GAO Report


GAO
Highlights
ELECTIONS
Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed

The U.S. Government General Accountability Office (GAO) released a report highly critical of electronic voting machines and systems on October 21, 2005. The report, entitled "Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed" (GAO-05-956) was undertaken by the GAO at the request of members of the House Government Reform Committee, House Judiciary Committee and the House Science Committee.

Ranking Member of the Government Reform Committee, Henry A. Waxman (D-CA), said, "The GAO report indicates that we need to get serious and act quickly to improve the security of electronic voting machines." Representative Waxman continued, "The report makes clear that there is a lack of transparency and accountability in electronic voting systems - from the day that contracts are signed with manufacturers to the counting of electronic votes on Election Day. State and local officials are spending a great deal of money on machines without concrete proof that they are secure and reliable. American voters deserve better."

In its key findings, the GAO listed some examples of voting system problems and vulnerabilities:

- Cast ballots, ballot definition files, and audit logs could be modified.

- Supervisor functions were protected with weak or easily-guessed passwords.

- Systems had easily picked locks and power switches that were exposed and unprotected.

- Local jurisdictions misconfigured their electronic voting systems, leading to election day problems.

- Voting systems experienced operational failures during elections.

- Vendors installed uncertified electronic voting systems.

Rep. Sherwood Boehlert (R-NY) said, "I wholeheartedly endorse the GAO recommendations, which underscore the need for the Election Assistance Commission and the National Institute of Standards and Technology to continue their work to establish standards and testing procedures for voting equipment. This work must move ahead on an ambitious schedule."

Rep. John Conyers (D-MI), ranking minority member of the House Judiciary Committee, a tireless champion for election reform and leading force behind the landmark report *"Preserving Democracy: What Went Wrong in Ohio 2004,"* has expanded comments on the report. He says the report ". . . lends important credibility to the cause of election reform generally, and more specifically to requiring that every machine have a voter verified paper ballot that is used in election day audits and, if discrepancies are found in those audits, becomes the official record for the election."

"Despite the many official assurances that the problems of the past elections were isolated and few," Conyers said, ". . . the election system is indeed riddled with problems and flaws."

The "bottom line," says Conyers, is that until these matters are seriously addressed, and "significant security and controls" are put in place with our voting machines, "American citizens have no reason to have complete confidence in our democracy."

Conyers further enumerates a list of notable and troubling security shorcomings identified by the GAO:

- Some electronic voting systems did not encrypt cast ballots or system audit logs, thus making it possible to alter them without detection.

- It is easy to alter a file defining how a ballot appears, making it possible for someone to vote for one candidate and actually be recorded as voting for an entirely different candidate.

- Falsifying election results without leaving any evidence of such an action by using altered memory cards.

- Access to the voting network was easily compromised because not all direct recording electronic voting systems (DREs) had supervisory functions password-protected, access to one machine provided access to the whole network.
- Supervisory access to the voting network was also compromised by repeated use of the same user IDs combined with easily guessed passwords.

- The locks protecting access to the system were easily picked and keys were simple to copy.

- One DRE model was shown to have been networked in such a rudimentary fashion that a power failure on one machine would cause the entire network to fail.

- GAO identified further problems with the security protocols and background screening practices for vendor personnel.

The fact that the GAO Report drew such immediate and overwhelming bi-partisan support in both its title and conclusions points up the fact that election reform is not an issue for Republicans nor Democrats, but one that all Americans should embrace. The Report covers in detail many aspects of the problem that we have brought to the attention of the Illinois State Board of Elections and election officials in Cook County and the City of Chicago. We had hoped that the GAO Report will strengthen the Illinois State Board of Election's decision to postpone certification of Sequoia Systems as IBIP proposed at their October meeting. Such was not the case and the Illinois Board has continued to approve Touch Screen machines, such as the Diebold AccuVote-TSX DRE.

GAO reported that voluntary standards for electronic voting adopted in 2002 by the Federal Election Commission contain vague and incomplete security provisions, inadequate provisions for commercial products and networks, and inadequate documentation requirements. GAO also found that tests currently performed by Independent Testing Authorities (ITAs) and state and local election officials do not adequately assess electronic voting system security and reliability

The GAO report indicated that national initiatives to improve voting system security and reliability of electronic voting systems either lack specific plans for implementation or are not expected to be completed until after the 2006 election. According to GAO, "Until these efforts are completed, there is a risk that many state and local jurisdictions will rely on voting systems that were not developed, acquired, tested, operated, or managed in accordance with rigorous security and reliability standards - potentially affecting the reliability of future elections and voter confidence in the accuracy of the vote count."

The findings of the GAO represent the first significant publication by an official government body that initiates the process of looking at the state of electronic voting systems and their shortcomings. It is not, however, the first serious report to delve into the problems of reliability and security. In the following section, we'll attempt to give the reader an overview of some of the more important documents which have come to the attention of concerned citizens in the past three years. In general, the GAO report and its predecessors examine electronic voting system flaws that fall into three broad categories: 1) Security, 2) reliability and, 3) accuracy. We will examine each of these in turn.

Security

The "Hopkins Report"

The report, "Analysis of an Electronic Voting System," was authored by Dr. Aviel Rubin of Johns Hopkins, Tadayoshi Kohno, Adam Stubblefield and Dan S. Wallach, four professors from Johns Hopkins, University of California at San Diego and Rice Universities, and is dated February 27, 2004. http://avirubin.com/vote.pdf The report was originally issued as a Johns Hopkins' document, "Johns Hopkins University Information Security Institute Technical Report TR-2003-19." The report gained general circulation after its May, 2004 publication by the IEEE when it appeared in the *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004.

The abstract of the report is worth quoting in full:

> With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts.
> We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable,

showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them.

We conclude that this voting system is unsuitable for use in a general election. Any paperless electronic voting system might suffer similar flaws, despite any "certification" it could have otherwise received. We suggest that the best solutions are voting systems having a "voter-verifiable audit trail," where a computerized voting system might print a paper ballot that can be read and verified by the voter.

While much of the report is technical in nature, it's less difficult to follow than the ordinary lay person might expect and the conclusions it draws are very clear:

- The system examined contained numerous security flaws that allow voters to cast multiple ballots with no built-in programming safeguards that log such activity.

- Administrative functions can be performed by regular voters, and the threats posed by insiders such as poll workers, software developers, and even building staff are even greater.

- The level of programming discipline was relatively low and "there appears to have been little quality control in the process."

- Because of a lack of cryptography, there is no secure authentication of the Smartcard in relation to the voting terminal.

In addition, the authors promote the concept of open source code for voting machines as a partial solution to the problem of undiscovered flaws in proprietary systems that no one can examine: "For quite some time, voting equipment vendors have maintained that their systems are secure, and that the closed-source nature makes them even more secure. Our glimpse into the code of such a system reveals that there is little difference in the way code is developed for voting machines relative to other commercial endeavors."

Their rationale is relatively straight-forward: "In fact, we believe that an open process would result in more careful development, as more scientists, software engineers, political activists, and others who value their democracy would be paying attention to the quality of the software that is used for their elections." Continuing:

"Such open design processes have proven successful in projects ranging from very focused efforts, such as specifying the Advanced Encryption Standard (AES) through very large and complex systems such as maintaining the Linux operating system. Australia is currently using an open source voting system. The model where individual vendors write proprietary code to run our elections appears to be unreliable."

The example of the Linux operating system is instructive. A few years ago, the industry "gold standard" for internet server operating software was Netscape Enterprise, a proprietary system. A decade ago, web designers and hosting companies used Enterprise almost exclusively for both internet and intranet applications. There are many of us who can remember many middle-of-the-night conversations with tech support people trying to impress on them how important it was to "get my site back up." There were extensive problems with reliability, but it was the best we had. Until Apache came along. Started by a group of developers, the Apache operating system was open source and quickly gathered adherents (and contributors) around the world. In a few short years, Enterprise had disappeared. Today, Apache is nearly bulletproof and internet developers sleep much better. This is the premier example of open source success – voting systems could be another.

On July 25, 2003, Diebold Corporation posted a rebuttal to the Hopkins Paper, posted to http://www.diebold.com/technical.htm and entitled *Diebold - Technical Response To The Johns Hopkins Study On Voting Systems*, claiming that the source code was an "old version" that had never been used, and that its machines were not vulnerable to attack through the memory card, the conclusions drawn by Rubin and his fellow authors were largely borne out in counter-rebuttals by the original authors and also

from Dr. Douglas W. Jones of the University of Iowa: http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html#answers Interestingly enough, in its response, Diebold does not dispute the factual basis for the analysis nor the conclusions reached regarding the serious security issues with respect Diebold source code. Further, the version numbers from code found on Diebold's FTP site relate to the version numbers listed as having been approved on the NASED web site. This demonstrates that the versions tested by the Hopkins group were certainly closely related to production code.

Finally, Diebold's denial that the code tested by the Hopkins group, while strident, had already been retracted by August 4, when, according to *Wired News*, “More Calls to Vet Voting Machines” - http://www.wired.com/news/politics/0,1283,59874,00.html, August 3, 2003. Mike Jacobsen, a spokesman for Diebold, "confirmed that the source code Rubin's team examined was last used in November 2002 general elections in Georgia, Maryland and in counties in California and Kansas."

Parts of the *Wired* article were rewritten at some point on or soon before August 11, and replaced by far more carefully worded quotes from John Kristoff, director of corporate communications for Diebold and presumably Mike Jacobsen's boss. The outright admission originally quoted was replaced by Kristoff saying tha the code examined by the Hopkins group "on the whole is not the same" as production code, and that Diebold cannot determine whether the lines of code that raised concern for Rubin were used in machines in the field. As Dr. Jones concludes (and we agree):

> *Wired* did not change the dateline on their on-line text when they made this change, but the carefully worded replacement still suggests that large parts of the code examined by the Hopkins group were indeed present in production systems. The phrase "on the whole is not the same" is only likely to be used if they could not honestly say "not substantially the same". That is, except for small parts, the code examined by the Hopkins group must have been substantially the same as the code used in production.

Diebold's first response was removed from the web and replaced with a collection of new material on July 29, all posted indexed under the "Diebold In The News" section of http://www2.diebold.com/default.htm.

From Dr. Jones commentary on the Diebold reports:

> On reading the Hopkins paper, I immediately called for the de-certification of Diebold's direct recording electronic voting system. I believe this is entirely justified by the magnitude of the security flaws identified in that paper, and completely independently, I believe it is justified by the fact that Diebold's predecessor, Global Election Systems, knew about that one flaw and did nothing to correct it over half a decade.

Dr. Jones also examines some of the specific claims by Diebold in their second (replacement) rebuttal, finding that many are insufficient to refute the original Hopkins conclusions. For example:

Hopkins: (p. 16):

> "Physical access to the voting results may not even be necessary to acquire the voting records if they are transmitted across the Internet."

Diebold Response:

> ... Results are not transmitted over the Internet.

Jones Comment:

> But we know that result transmission uses telephone, PPP, and a username and password, from Page 14 of the Hopkins report, quoted in Allegation #40. Therefore, it is quite possible that election central will have a LAN connected using Internet protocol, perhaps used to connect a modem bank with a single PC. This LAN may not be as vulnerable as the public Internet, but it is vulnerable to packet snooping and several other attacks, and must therefore be carefully secured. Furthermore, if an adversary can dial into the PPP host and await connections, Trojan horse applications on the

> voting system could communicate with the adversary using PPP without talking to the GEMS system at all.

And according to Dr, Jones, Diebold's defense becomes meaningless in light of changes made with the adoption of the AccuVote-TSX.

> The AccuVote TSX, apparently allows wireless transmission of precinct results to the GEMS server, but Diebold defends this, saying that the electronically transmitted results are only unofficial results, while the official canvass depends on hand-carried records. This subject was discussed in the Acron Beacon Journal on August 15, 2003. Unfortunately, the specific details of canvassing are a matter of state law, outside of Diebold's control, and in addition, the Diebold operating instructions apparently call for the connection to the server to be established prior to computing the precinct totals.
>
> This means that the memory cards holding the official results for each precinct are exposed to corruption by any network insecurity, and therefore, that the official canvass can be corrupted if someone hacks into the machine.
>
> Furthermore, it is emerging that the version of Windows CE used by Diebold is both heavily customized and full of dynamically loaded libraries. As a result, there are strong grounds for the conclusion that the operating system is not unmodified commercial off the shelf software (COTS), and that with this extensive use of dynamic linkage, we cannot even tell if the system being run on a particular voting machine resembles the system that was disclosed in the configuration documents submitted with this system when it went through the FEC/NASED approval process.

In summary, the debate surrounding the source code and the open FTP site clearly show that the Hopkins report examined operational source code that was probably used in real elections, such as Georgia in 2002, and that the flaws pointed out had been in existence for a number of years.

Three additional reports, subsequent to the publication of "Analysis of an Electronic Voting System," have come to the same conclusions and support the findings of the group which authored this paper.

The first of these, "Risk Assessment Report Diebold AccuVote-TS Voting System and Processes," September 2, 2003, was prepared by Science Applications International Corporation (SAIC) for the State of Maryland:
http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf

It states:

> In the course of this Risk Assessment, we reviewed the statements that were made by Aviel. D. Rubin, professor at Johns Hopkins University, in his report dated July 23, 2003. In general, SAIC made many of the same observations, *when considering only the source code.*
>
> This Risk Assessment has identified several high-risk vulnerabilities in the implementation of the managerial, operational, and technical controls for AccuVote-TS voting system. If these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results.

In November, 2003, Compuware completed a report for the Ohio Secretary of State, Kenneth Blackwell, "Direct Recording Electronic (DRE) Technical Security Assessment Report." (a report Blackwell suppressed for a number of months) http://www.sos.state.oh.us/sos/hava/compuware112103.pdf

Commenting on Diebold (one of several systems tested), Compuware said:

> During the course of our study, Compuware has identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question.

This was followed by the January 20, 2004 report "Trusted Agent Report Diebold AccuVote-TS Voting System," completed also for the State of Maryland by RABA Technologies. http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf In this report we find:

> The State of Maryland election system (comprising technical, operational, and procedural components), as configured at the time of this report, contains considerable security risks that can cause moderate to severe disruption in an election.
>
> A considerable amount of press has been given to the "Hopkins report." The subsequent revelation of a conflict of interest involving one of its authors with a Diebold competitor has only served to detract from the substance of the results. The single most relevant finding in this section is that the general lack of security awareness, as reflected in the Diebold code, is a valid and troubling revelation.
>
> In addition, it is not evident that widely accepted standards of software development, such as the Carnegie Mellon Software Engineering Institute's Capability Maturity Model® for Software and System Security Engineering (SW-CMM and SSE-CMM), were followed.

Diebold's sensitivity with respect to its source code has led it to refuse to even escrow such code when it might mean losing business. North Carolina has passed a tough new election law that requires among other provisions that this code is to be available to the Board of Elections and the chairs of the state political parties for review so that they could look for security vulnerabilities.

In November, 2005, Diebold filed suit against the North Carolina Board of Elections to try to avoid this state requirement that vendors place into escrow all source code "that is relevant to functionality, setup, configuration, and operation of the voting system." Opponents succeeded in convincing the judge to dismiss the case and require Diebold to comply.

Despite Diebold's open admission that it would not meet the state requirements for voting machine integrity, the Board of Elections later agreed to certify Diebold. The Electronic Frontier Foundation (EFF) filed suit against the Board of Elections in December, arguing that the Board had violated its own obligations to perform extensive security-related tests of all of the code on all certified systems prior to certification. The court denied EFF's motion, but Diebold was nonetheless forced to withdraw from the North Carolina procurement process because it did not escrow its code.

In a letter to the Board of Elections on Thursday, Diebold indicated that it is still unwilling to comply with the law. Instead, it offered to help the state "revise" the law so that "all vendors will be able to comply with the state election law."
"The purpose of election integrity law is to ensure that votes are accurately counted, not to ensure that all equipment vendors can comply," said Matt Zimmerman, EFF's Staff Attorney specializing in electronic voting issues. "The law requires voting machine transparency for good reason. All vendors must realize that the public will not and should not accept a process that forces them to simply trust, but not verify, their votes are accurately counted." By withdrawing from North Carolina's electronic voting contract, Diebold cedes the market to competitor ES&S. The rival company has stated that it will comply with all state escrow requirements.

This discussion regarding security issues with respect to Diebold touch-screen terminals has been extensive – primarily because so much of Diebold's source code and operating systems information is available and because Diebold has provided so many contradictory explanations that they have made themselves a large and easy target. But security concerns about DREs are by no means limited to Diebold.

When Diebold's source code was found on the Internet FTP (File Transfer Protocol) site, and was examined by a team of computer scientists who characterized it as "full of holes," [See the discussion of the "Hopkins Report," *supra*. Sequoia was quick to state that "while Diebold relies on a Microsoft operating system that is well known and understood by computer hackers, Sequoia's AVC Edge runs on

a proprietary operating system that is designed solely for the conduct of elections." The Sequoia website, http://www.sequoiavote.com states, "Sequoia's software is proprietary, not sold off-the-shelf and available to anyone, making it much more secure."

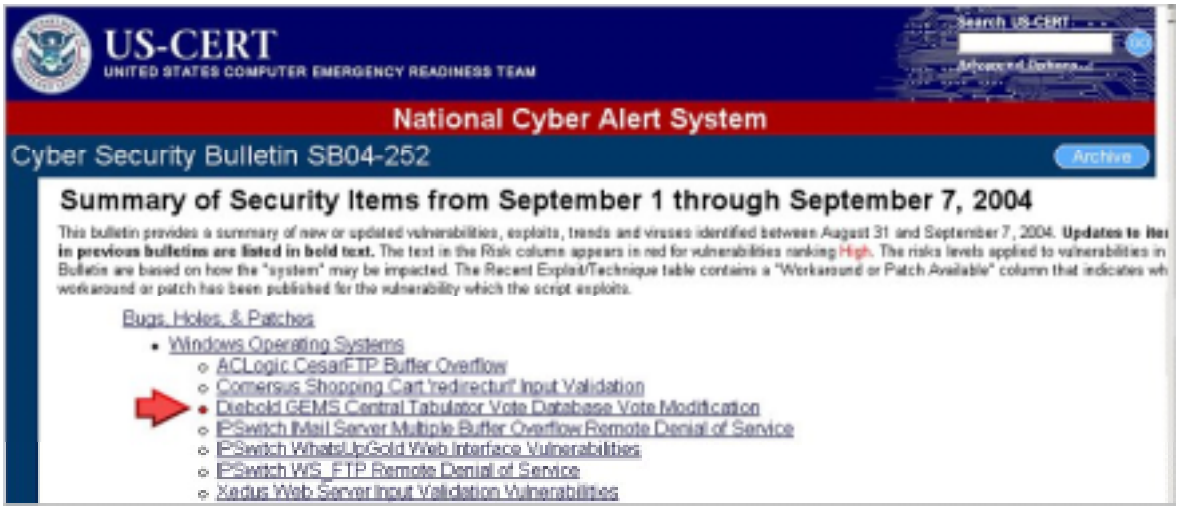
This statement ignores the fact that Sequoia's own computer code showed up on an unguarded FTP site on the Internet in 2004, and is now being studied by several experts. Jeremiah Akin, a Riverside County computer scientist, has discovered a way of writing modifications into the WinEDS ballot management software in such a way that all trace of outside intervention vanishes automatically. "You can change the code, run it, save it and then, when you close down the system and you bring the system back up, all the modifications you made will be rewritten," Akin said. "The system will set it back to the original code." http://www.lacitybeat.com/article.php?id=1013&IssueNum=55

Further, these claims are at best misleading. Sequoia's statement omits the fact that its WinEDS vote-tallying software – as opposed to the vote-gathering part of the operation – runs on a Microsoft operating system and uses a Microsoft database. WinEDS was written in a computer language called Visual Basic, which is notorious for its popularity with virus writers and hackers. Visual Basic is specifically prohibited under the Federal Electoral Commission's 2002 voting systems standards; WinEDS, like much of the software in use in computer voting machines in this country, is certified under the pre-Internet age 1990 FEC standards. This distinction is important, because it applies to all Sequoia voting system hardware and software, including the Insight Optical Scanner and the central tabulation software as well as that which runs the Sequoia AVC Edge Touch Screen system. As of September, 2005, no Sequoia systems have been certified by the National Association of State Election Directors NASED). A copy of the latest available NASED certifications regarding Sequoia is attached as Appendix C and is available online at http://www.nased.org/ITA%20Information/NASEDQualifiedVotingSystems12-03-9-05.pdf

It does not appear to be correct that the software used to run the touch screen machines is "proprietary" and "not sold off-the-shelf." According to a 2001 report by Wyle, an independent testing lab that analyzes voting software as part of the federal certification process, the AVC Edge machine has, "at its core," a commercially available operating system called pSOS. Note: Wyle labs only qualifies the hardware. Either Ciber, Inc. or their counterpart, SysTest Labs, Inc. are the proper entities to qualify the election software. http://www.nased.org/ITA%20Information/NASEDITAProcess.pdf

The Diebold "GEMS Defect"

Note the National Cyber Alert from the Department of Homeland Security:



Reported by Bev Harris and Dr. Herbert Thompson, and independently confirmed by the security consultant firm Compuware on commission from the state of Ohio, the GEMS Defect concerns the central vote tabulating database that accumulates all the precinct and absentee votes for all Diebold optical scan

and touch-screen voting systems. The GEMS Defect allows VBA (visual basic script) to rewrite the access database containing the vote count without a trace

Despite assurances by Diebold, records obtained by Black Box Voting show that this issue has not been resolved in either California or Ohio, or apparently any of the other 1,200 jurisdictions that use Diebold. A critical set of Compuware documents confirming this was suppressed by Ohio Secretary of State Ken Blackwell.

Votergate the Movie**,** previously furnished to the Board and available for free download at (http://www.votergate.tv) contains footage from a national TV broadcast of Bev Harris instructing Howard Dean how to hack GEMS and untraceably alter vote tallies in under two minutes. Additional vulnerabilities have since been found and publicized at http://www.blackboxvoting.org.

Subsequently, Diebold has published a "rebuttal" to certain types of security breach protocols that had been previously outlined. (http://www.diebold.com/dieboldes/pdf/rebuttal.pdf). This rebuttal relies primarily on the so-called "perimeter defense" which requires that election officials maintain perfect control of all passwords and access to GEMS. Unfortunately, this is not always possible and Diebold itself has admitted to several instances, one specifically in Volusa County Florida, in which security may well have been breached with "a second memory card." **[Tulare] County votes for machines.** By Roger Phelps, The Porterville Recorder; June 10, 2004.
http://myopr.com/articles/2004/06/10/news/local_state/news01.txt

For something that doesn't exist (according to Diebold) there's certainly a lot of attention being paid to this alleged problem. One can only wonder how Diebold can be rightand so many scientists and government agencies so wrong.

David Jefferson, a computer scientist at Lawrence Livermore National Laboratory and a member of the California secretary of state's voting systems panel, agreed with Diebold that election procedures could help prevent or detect changes in votes, but said that election officials and poll workers do not always follow procedures. Therefore, election observers need to know about the vulnerabilities so they can help reduce the risk that someone could use them to rig an election.

Jefferson added that he doesn't believe that the vulnerabilities show deliberate malice on Diebold's part to aid fraud, as Harris has sometimes contended in public statements. But the vulnerabilities do show incompetence and indicate that Diebold programmers simply don't know how to design a secure system.

On Oct. 17 2005, an ordinary citizen in Cleveland, Mr. Wright, asked what may turn out be the most important question of the year. What is Diebold's explanation, he wanted to know, for the VBA Script hack of the GEMS central tabulator performed by Dr. Herbert Thompson?

This leads to the crucial question: If Diebold knew, and if Ken Blackwell knew, why wasn't the U.S. Election Assistance Commission told, why were no other secretaries of state told, why didn't Blackwell tell the Ohio election officials using GEMS, and why weren't the fixes deemed necessary by CompuWare ever implemented?

The GEMS defect has been proven. The risks are significant. Mail-in votes are at exceptional risk because they are counted on a system that lacks protective features found on polling place machines. While the precinct-based optical scan machines made by Diebold produce a results tape, the same machines, when counting mail-in ballots, use a different program and do not store vote tallies on a memory card, nor do they produce an independent results tape. Therefore the defective GEMS program holds the only record for absentee vote totals.

The GEMS program is run on an ordinary PC, using the Windows operating system. Vote totals from each precinct, along with mail-in votes, are uploaded to the GEMS computer. GEMS tallies all votes and produces final election results.

According to the Aug. 18, 2004 report by CompuWare Corp., an independent evaluation commissioned by the Ohio secretary of state: “... an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results."

The ability to selectively change ballot definition files with mail-in votes can achieve vote swapping from one candidate to another. In GEMS, each candidate is assigned a number.

Sims: #413
Irons: #200
Lange: #522

In GEMS, you can selectively change the candidate identifier number for mail-in votes, like this:

Sims: #200
Irons: #413
Lange: #522

This will cause the mail-in results to give Sims votes to Irons, and vice versa, a very dangerous vulnerability for close elections. (You can also change the votes themselves in GEMS, but that requires adjustments in several GEMS database tables.)

Changing the candidate identifier number in GEMS provides one-step adjustment that takes only seconds, and can be implemented any time during the absentee vote-counting process to flip results. As demonstrated in the Leon County, Florida elections office on May 2, 2005 by Dr. Herbert Thompson and Black Box Voting, this kind of GEMS manipulation does not require opening the GEMS program, does not require a GEMS password, and does not show up in any audit log.

The standard safeguard for this known risk is to compare results reports from voting machines with GEMS results reports. However, Black Box Voting has learned that Diebold's mail-in vote-counting system does not produce a voting machine report. In November, 2005, Jim March of Black Box Voting examined the Diebold voting system in San Joaquin County, Calif. and learned that the voting machine results tape -- the telltale sign and the key safeguard for GEMS tabulator hacking -- *does not exist for mail-in votes.*

You don't need to be a computer scientist to understand plain English: Both the 1990 and 2002 Federal Election Commission (FEC) standards prohibit "interpreted code." The Diebold memory card architecture relies on interpreted code, executing logic on the memory card by passing memory card code through the interpreter.

You also don't need to be a computer expert to understand that another item forbidden in the FEC standards, "nonstandard computer language" is being used. Diebold decided to make up its own language, calling it "AccuBasic." Only Diebold uses it, no one else in the world. Apologists for the ITAs explain that the AccuBasic language is similar but different to the C++ computer language. That's like saying German is English because the languages are "similar."

But the FEC standards are deficient in some areas. Here's something that doesn't take a statistician to figure out: The FEC standards set a failure tolerance so low that 8 percent of the voting machines are allowed to fail on the first day of use. Would you buy a TV set if you knew there was an 8 percent chance it would stop working the first day? Would you consider this a good use of taxpayer money?

Further, the State of California has decertified all touch-screen systems for use in elections, essentially beginning all over at the start of the process. In a letter sent to Diebold on December 20, 2005, the Secretary of State’s office made these observations:

> Unresolved significant security concerns exist with respect to the memory card used to program and configure the AccuVote-OS and the AccuVote-TSX components of this system because this component was not subjected to federal source code review and evaluation by the Independent Testing Authorities (ITA) who examined your system for federal qualification. It is the Secretary of

State's position that the source code for the AccuBasic code on these cards, as well as for the AccuBasic interpreter that interprets this code, should have been federally reviewed.

Furthermore, we strongly believe it is the duty and responsibility of the Secretary of State and you to make certain that the ultimate users of your products – the voters of California – have a voting system that has been thoroughly and rigorously evaluated. Therefore, we are requesting that you submit the source code relating to the AccuBasic code on the memory cards and the AccuBasic interpreter to the ITA for immediate evaluation.

We require this additional review before proceeding with further consideration of your application for certification in California. Once we have received a report from the federal ITA adequately analyzing this source code, in addition to the technical and operational specifications relating to the memory card and interpreter, we will expeditiously proceed with our comprehensive review of your application.

Ironically, December 20, 2005 was the same day that the Illinois State Board of Elections certified the Diebold AccuVote-TSX ouch-screen DRE!

Reliability

No matter how secure or accurate an electronic voting machine may be, if it breaks down, it can't do the task for which it was intended. And breakdown they do – early and often. Here is a sampling:

March 2000, Shelby County, Tennessee: Computer problems halted the voting at all 19 of Shelby County's early-voting sites during the 2000 Republican presidential primary, forcing officials to use paper ballots (which were supposed to be provided by the voting machine company as a backup but were unavailable when needed). Election officials had to make voters wait in line or tell them to come back later. Because early voting turnout in this election was six times normal,
this snafu affected about 13,000 voters. *The Commercial Appeal,* 5 March 2000; "Computer Glitch Hampers Voting ... "

November 2000, Allegheny County, Pennsylvania: City Councilwoman Valerie McDonald reported that machines in Pittsburgh's 12th and 13th wards and other predominantly black neighborhoods malfunctioned on Election Day. They began smoking and spitting out jammed and crumpled paper. Poll workers felt the machines had been intentionally programmed incorrectly and had been sabotaged. Whether or not there was sabotage, the spit-and-polish image so carefully crafted in election company press releases didn't seem to apply to the African-American precincts that day. Poll workers in the 12th and 13th wards waited hours for repairs, and voters who couldn't spend the day at the polling place were rendered politically voiceless. *Pittsburgh Post-Gazette*, 4 May 2001, "Hearing Gets Landslide of Voting Problems"

February 2000, Passaic, New Jersey: About 75 percent of the voting machines in the city of Passaic failed to work when the polls opened on Election Day, forcing an undetermined number of voters to use paper ballots during the morning. Independent consultant V. Thomas Mattia, a Philadelphia voting machine supervisor who later examined the machines, concluded the problem was due to sabotage, which led a Democratic candidate to refer the matter to the FBI. For no discernable reason, Mattia later reversed himself. "I believe that it was an oversight, and there was no fraud involved," Mattia stated in a letter. Freeholder James Gallagher, who had referred the matter to the FBI based on Mattia's previous suspicions, said that he was surprised by the reversal and needed more information about why the expert had changed his mind. *The Record*, 23 February 2000; "Expert Finds No Sabotage in Election, Reverses Stance ... "

November 2002, Tangipahoa Parish, Louisiana: "I can't say every precinct had a problem, but the vast majority did," Tangipahoa Parish Clerk of Court John Dahmer said. He reported that at least 20 percent of the machines in his parish malfunctioned. "One percent might be acceptable, but we're not even close to that," Dahmersaid. He said 15 employees worked to combat the malfunctions. *The Baton Rouge Advocate*, 7 November 2002; "Voting machine glitches worrisome ... "

November 2002, Ascension Parish, Louisiana: An elections official gnashed his teeth as more than 200 machine malfunctions were called in. The Parish Clerk said his staff was on the road repairing machines from 5 a.m. to 9 p.m. In one case, a machine wasn't repaired until 12:30 a.m. Wednesday. *The Baton Rouge Advocate*, 7 November 2002; Voting machine glitches worrisome ... "

November 2002, Ohio: A voting machine malfunctioned with 12 of Crawford County's 67 precincts left to count. A backup machine was found, but it also could not read the vote. Election workers piled into a car and headed to another county to tally their votes. *Telegraph-Forum*, 6 November 2002; "Glitch sends vote count to Richland"

November 2002, Pickens County, South Carolina: Pickens County couldn't get totals from two precincts due to computer problems. Associated Press*,* 6 November 2002; *"*Equipment causes voting problems in several counties"

Prince George's County, Maryland - The Board of Elections had technical difficulties last night [September 14, 2004] compiling results. Election workers said the main modem to receive results from the polls had malfunctioned.

Election officials said there were no major problems at polls throughout the day. The only known glitch was at Mount Rainier Elementary School. When polls opened yesterday, nearly a dozen voters were told the machines were not pulling up the Democratic slate. Linda Couch, a Mount Rainier resident, said poll workers told the voters that because the machines weren't operating properly, they could write down their choice on a piece of paper. Couch said some voters left, saying they would try to come back. Others, like her, wrote their selections down on the paper. *Johnson Aide Wins Democratic Primary - Newcomer Nets a Third of the Vote*. By Ovetta WigginsWashington Post Staff Writer, Wednesday, September 15, 2004; Page B04 - http://www.washingtonpost.com/wp-dyn/articles/A22014-2004Sep14.html

However, there are also some reports of problems in the November, 2004 election: Voters and poll watchers reported some 531 incidents to TrueVoteMD. Some 201 of these were incidents involving machine malfunctions of various types. The other 330 involved human and organizational failures, including lack of privacy, denials of provisional ballots or the right to vote at all, long lines, and insufficient help from election workers.

TrueVoteMD only covered 6% of Maryland's precincts. Among the 201 machine failures reported were:

Battery/Electrical Problem -3
Late Opening due to Machine Problem -4
Machine Crash - 42
Replacement Machine - 11
Review Screen Incorrect -2
Technician Accessing Machine -8
Write-in Vote Problem -9
Voter Access Card/Encoder Problem - 37
Vote Switching -17
Screen Malfunction -30

Exxtrapolating only the 163 listed malfunctions from 108 precincts (the other 38 may have been human error) over all of Maryland's 1,787 precincts would indicate that there may have been as many as 2,700 machine failures statewide.

March, 2004 - San Diego County, California. Multiple problems occurred,18 among them: Poll workers saw unfamiliar Windows screens, frozen screens, strange error messages and login boxes none of which they'd been trained to expect. A report released Monday by Diebold Election Systems shows that 186 of 763 devices known as votercard encoders failed on election day because of hardware or software problems or both, with only a minority of problems attributable to poll worker training. Diebold's post-mortem of the March 2 election said it was "disappointed" in the encoder failures and that it values its ties to local elections officials. But the McKinney, Texas-based firm offered no fundamental explanation of how and why the company delivered faulty voting equipment to Alameda and San Diego counties its two largest West Coast customers on the eve of the 2004 presidential primary.
"Diebold reports multiple problems: Registrar wants reason for e-voting" *TriValley Herald*. April 13, 2004. By Ian Hoffman, Staff Writer. http://www.votersunite.org/article.asp?id=2390

July, 2004 - DeKalb County, Georgia. Over 150 Georgia citizens volunteered as poll watchers in the primary. They observed machine malfunctions and irregularities. Excerpts from one observer's report.30 When the polls opened we had a poll watcher in every precinct, informed and trained with the things to look for and how to address the problems the moment they cropped up. We insured the law was followed to the letter. The calls from the poll watchers began promptly at 7:00 AM with every irregularity, improper behavior and machine malfunction they saw reported to the attorneys. One precinct reported almost upon opening of the polls that all machines (10) were failing. Voters inserted the access card and the card **was** immediately ejected. The pollwatcher reported that voters were offered provisional paper ballots, but they were prepared with only 25 of these ballots and ran out within 10 minutes. It took almost 2 hours to rectify the situation even though our HQ personnel reported it to the County office immediately. *Wish us luck! Poll Watching in Georgia* - National Ballot Integrity Project Discussion Forum. Posts by Roxanne Jekot. July 20-22, 2004. http://www.ballotintegrity.org/cgi-bin/dcforum/dcboard.cgi?az=show_thread&om=61&forum=DCForumID1&omm=0&viewmode=threaded

March, 2005 - Montgomery County, Maryland. The IT report to the County Elections Board reveals widespread problems with the electronic voting machines on election day. Here are some excerpts: *Information Technology – Election Day Review Election Day Equipment Review For Election Day*, "IT Report to the Montgomery County Election Board**" -** Page 11.
http://www.truevotemd.org/Resources/Lessons_Learned.pdf 2,597 voting units were deployed. An additional 80 voting units were sent to about 65 polling places on Election Day to replace malfunctioning units. A few were sent out to accommodate long lines at polling places.
From Help Desk tickets and GEMS reports, 189 voting units (7%) of units deployed failed on Election Day. An additional 122 voting units (or 5%) were suspect based on number of votes captured. Of the 189 voting units that failed:
1. On Election morning, 58 voting units failed to boot up, showing a Ballot Exception Error. These units were unusable and were immediately taken out of service. No votes were captured on these units.
2. 106 voting units experienced screen freezes. In staff opinion this is the most serious of errors. Election judges and technical staff reported that many of these units froze when the voter pressed the Cast Ballot button. This leads to great confusion for judges and voters. The voter leaves the polling place with little or no confidence that their vote was counted. In many cases, the election judges are unable to provide substantial confirmation that the vote was, in fact, counted.
3. 25 voting units failed due to a variety of problems including card readers, printers, and power problems.
4. The additional 122 suspect voting units were identified because few votes were captured compared to other units in the same polling place. A unit was considered suspect if it had 25-50 votes captured when all other units in the polling place had over 150 votes.
5. Of the 1,245 encoders deployed, approximately 30 failed and were replaced on Election Day. Preliminary tests indicate that the failures are a result of little or no battery power.
6. Prior election day, we prepared approximately 95 voting units using new touch screen units and new PC memory cards. Of these, 5 failed; 4 with screen freezes and 1 with a ballot exception error. Another 4 units were in the suspect category.
As of February 16, 2005, Diebold in Maryland was unable to diagnose the problems and was shipping the systems out of state for testing.
*Diebold Memo***.** http://www.truevotemd.org/Resources/DieboldMemo2-16-05.jpg

July 20, 2005 -California. After testing 96 touch screen machines and finding a high error rate, Secretary of State Bruce McPherson rejected Diebold's application to certify the AccuVote TSx touch screen with AccuView printer module. After possibly the most extensive testing ever on a voting system, California has rejected Diebold's flagship electronic voting machine because of printer jams and screen freezes, sending local elections officials scrambling for other means of voting. "There was a failure rate of about 10 percent, and that's not good enough for the voters of California and not good enough for me," Secretary of State Bruce McPherson said. If the machines had been used in an election, the result could have been frustration for poll workers and long lines for thousands of voters, elections officials and voter advocates said Thursday. "We certainly can't take any kind of risk like that with this kind of device on California voters," McPherson said. The report, "Analysis of Volume Testing of the AccuVote

TSx/AccuView" was prepared by the California Voting Systems Technology Assessment Advisory Board on behalf of the California Secretary of State

A total of 96 AccuVote TSX machines were tested. A minimum of 34 incidents of failure were recorded by the 96 machines during 5.33 hours, a failure rate of 35.4% in terms of total failures A total of 20 software errors and 14 printer jams were recorded. These failures involved 29 distinct machines, which means that 30.2% of the machines tested incurred one or more failures during a relatively short testing period.

The report calculated two different metrics of failure, the mean *time* between failure (MTBF) and the mean *votes* between failure (MVBF) The Report found:

> When considering only software failures, the estimated MTBF is approximately 25.6 hours. This means we expect a typical TSx machine to experience a software failure about once every 25.6 hours, under the conditions experienced during the volume testing. The estimated MVBF, when considering software failures only, is approximately 536 votes, meaning that one might expect a software failure about once every 536 votes.
>
> And further: During the volume test, approximately 20% of machines experienced a software failure, so one might expect roughly 20% of machines to experience a software failure and need to be taken out of service during an election of comparable scale. Under these assumptions, some polling places would be left without any working machine by the end of the day.

The Report concluded that the Diebold AccuVote TSx does not meet EAC standards: "The observed failure rate appears to be far larger than the MTBF called for in the relevant federal standards. Both the 1990 and 2002 FEC standards require a MTBF of at least 163 hours. On the surface, then, the aggregate failure rate observed during the volume test would appear to be more than 10 times higher than permitted."

We suggest that this failure rate, when translated into actual election day experience has the potential to cause more than a "few errors." In addition, there is an issue of lost votes from the standpoint of audit and/or recount. In examining the 13 of 14 paper jams, the testing results showed:

> For 6 of these 13 cases where counts were available, the number of VVPAT records matched the number of electronic ballot images, and so we assume no VVPAT records were lost. However, for the other 7 jams, some number of VVPAT records were lost. These involved 6 distinct machines; machine numbers #8, #10, #33, #45, #55, and #60 were associated with 1, 5, 4, 2, 1, and 8 lost VVPAT records, respectively. Machine #10 experienced two printer jams. In total there were 21 lost VVPAT records, out of a total of 1535 ballots cast on those particular machines.

The Report describes the results of the paper jams as being consistent with those found by Dianne Felts during her evaluation: "In every case where a printer failure occurred, the loss of VVPAT records would be evident upon inspection of the paper trail. In every such case, the paper stopped advancing and the printer overprinted multiple lines of text to the same place on the paper."

This type of failure is particularly relevant when considering the 5% audit contemplated under the revisions to the Illinois State Election Code embodied in HB 1968. The concludes that : "The loss of VVPAT records would be problematic during any recount of the VVPAT records. If the VVPAT were to govern in the event of any discrepancy between the electronic and paper records . . . then lost VVPAT records might constitute lost votes."

During the test, a total of 21 VVPAT records were lost out of 1,535 votes cast, a failure rate of 1.37%. Projected against the two million votes cast in Cook County during the last presidential election, for example, this would be approximately 4,100 lost votes, rendering any audit or recount virtually meaningless. For this reason, it would appear that the Diebold AccuView printer does not meet Illinois standards.

We concur with this statement of the Report: ***"These calculations provide evidence that the failures observed during the July 20th test are serious. It is hard to escape the conclusion that any system with failure rates this high is not ready for use in an election."***

Accuracy

One of the enduring myths that voting machine companies foster is that their machines and vote-counting systems are far more accurate than hand-counting of ballots. However, upon closer examination, this turns out to be just that . . . a myth.

The California Institute of Technology and the Massachusetts Institute of Technology mobilized a team of computer scientists, human-factors engineers, mechanical engineers and social scientists to examine voting technology. Touch-screens did not get high marks. Here are voting system error rates, as estimated by the Caltech/MIT Voting Technology Project report, issued in July 2001: Caltech/MIT Voting Technology Project, www.vote.caltech.edu

Most lost votes — Congressional and gubernatorial races

1. Lever machines **7.6%** — 1.5% for presidential races
2. Touch-screen machines **5.9%** — 2.3% for presidential races
3. Punch card **4.7%** — 2.5% for presidential races
4. Optical scan **3.5%** — 1.5% for presidential races
5. Hand-counting **3.3%** — 1.8% for presidential races

Both the Sequoia Insight Optical Scanner and the Sequoia AVC Edge DRE have many documented failures. In Palm Beach County, Florida, AVC EdgeTouch Screens froze up, registered incorrect votes. In Hillsborough County, Florida vote data could not be transferred from 24 of the 26 data cartridges to the readers that would transmit the totals to the central office to be tallied. Precinct totals were faxed over and entered by hand.

Ten days after the November 2002 election, Richard Romero, a **Bernalillo County, New Mexico**, Democrat, noticed that 48,000 people had voted early on unauditable Sequoia touch-screen computers, but only 36,000 votes had been tallied — a 25 percent error. Sequoia vice president Howard Cramer apologized for not mentioning that the same problem had happened before in **Clark County, Nevada**. A "software patch" was installed (more on that risky procedure later) and Sequoia technicians in Denver *e-mailed* the "correct" results. *Albuquerque Journal*, 19 November 2002; "County Certifies Vote Tally"

Not only did Cramer fail to mention to Bernalillo County that the problem had happened before in Nevada just four months later, Sequoia salespersons also failed to mention it while making a sales presentation to Santa Clara County, California. A Santa Clara official tried to jog their memory. According to the minutes of this meeting, Notes on "Workshop" on Voting Machine Security for Santa Clara County Supervisors, 11 February 2003; see http://verify.stanford.edu/dill/EVOTE/sc-2-11-2003.html "

Supervisor McHugh asked one of the vendors about a statistic saying there was a 25 percent error rate. No one knew where this number came from and Sequoia said it was incorrect." That meeting was held Feb. 11, 2003. Just 20 days before, in **Snohomish County, Washington**, at a meeting called because Sequoia optical-scan machines had failed to record 21 percent of the absentee votes, *The Everett Herald,* 20 January 2003; "County to Discuss Ballot-Counting Foul-up" When asked about the 25 percent error in Bernalillo County. The Sequoia representative was well aware of the problem, replying quickly that ***that*** 25 percent error was caused by something quite different from ***this*** 21 percent problem. (see below)

January 2003, Everett, Washington: If there was any doubt that Republicans were right to ask for a recount of some Snohomish County absentee ballots from November's general election, it was erased by one sobering number: 21.5 percent of the ballots cast in 28 selected precincts were not counted. The Snohomish County Auditor's Office recounted 116,837 absentee ballots after county officials discovered that the optical-scan ballot-counting machines had miscounted. The problem was attributed to a faulty

“read head” on each of two optical scanners; the heads failed to read ballots with blue ink. The machines had passed the test on blue ink before the election.

The Sequoia representative could not recall that the “read head problem” had ever happened before. When asked by a citizen how many machines of the same make and model number Sequoia has in the United States, she said, “About 1,500.” When asked how many years they’d been in use, she said about six years. “Why, then,” asked a citizen, “would this unheard-of problem happen at exactly the same time in exactly the same place on two different machines at once?” The Sequoia rep said she had “no idea.” Citizen meeting in Snohomish County, 23 January 2003, reported at Black Box Voting http://www.blackboxvoting.org

And the list goes on and on:

In the ***Alabama 2002 general election***, machines made by Election Systems and Software (ES&S) flipped the governor’s race. Six thousand three hundred Baldwin County electronic votes mysteriously disappeared after the polls had closed and everyone had gone home. Democrat Don Siegelman’s victory was handed to Republican Bob Riley, and the recount Siegelman requested was denied. Six months after the election, the vendor shrugged. “Something happened. I don’t have enough intelligence to say exactly what,” said Mark Kelley of ES&S. – *Mobile Register,* 28 January 2003; “Voting Snafu Answers Elusive”

March, 2004 - San Diego County, California. Ten votes were inexplicably lost at one polling place. John Pilch, a retired insurance agent who worked as a polling place inspector in San Carlos, said that when polls closed at 8 p.m. Tuesday, the number of people who signed the voter log differed from the number of ballots counted by computers. "We lost 10 votes, and the Diebold technician who was there had no explanation," said Pilch, who registered complaints with elections officials, his county supervisor and several others. "She kept looking at the tapes." “Poll workers, voters cite tied-up hotline, poor training, confusion.” *Union Tribune*; March 7, 2004; By Jeff McDonald and Luis Monteagudo Jr. http://www.signonsandiego.com/news/politics/20040307-9999-1n7vote.html

November, 2004 -San Juan County, New Mexico. 1,843 election-day phantom votes were reported in Precinct 51. With only 318 people casting election day ballots on the Danaher Shouptronic electronic voting machines in the Precinct 51, Fran J. Hanhardt, Republican incumbent running for County Clerk, received 2,079 votes, while Democratic challenger Glojean B. Todacheene received 82. However, Ms. Hanhardt didn't need the 1,843 phantom votes to win. She won by a strong margin of 16,484 votes. Since New Mexico Secretary of State Rebecca Vigil-Giron says phantom votes are not possible, you may want to check thecertified canvass report for yourself. Look on page two of the San Juan Canvass Report to find the County Clerk totals in Precinct 51 on election day. Then look at the far right side of page three for the number of voters who signed in at the polls. **Vote Recount Fight 'Is Not Over'.** *Albuquerque Journal*. December 24, 2004. By Andy Lenderman, Journal Politics Writer. http://www.abqjournal.com/elex/278376elex12-24-04.htm and http://www.sos.state.nm.us/PDF/San_Juan.pdf

November, 2004 - Franklin County, Ohio. Phantom votes appear in the presidential totals. Bush received 4,258 votes and Kerry received 260 in a precinct with only 638 voters. Matthew Damschroder [director of the Franklin County Board of Elections] said he received some calls Thursday from people who saw the error when reading the list of poll results on the election board's Web site. He said the error would have been discovered when the official canvass for the election is performed later this month. Damschroder said after Precinct 1B closed, a cartridge from one of three voting machines at the polling place generated a faulty number at a computerized reading station. The reader also recorded zero votes in a county commissioner race. Damschroder said the cartridge was retested Thursday and there were no problems. He couldn't explain why the computer reader malfunctioned. “Computer error at voting machine gives Bush 3,893 extra votes.” *Akron Beacon Journal*. November 5, 2004. Associated Press. http://www.ohio.com/mld/beaconjournal/news/state/10103910.htm?1c

November 2000, San Francisco, California: In polling place 2214, machines counted 416 ballots, but there were only 362 signatures in the roster and the secretary of state found only 357 paper ballots. *The San Francisco Chronicle*, 11 February 2002; “2000 election finds work was sloppy”

November 2000, Albuquerque, New Mexico: A software programming error in New Mexico led officials to withhold about 60,000 ballots from their vote count. According to an AP wire service report: "Their (voting) machines have a problem in the database," elections bureau director Denise Lamb said, "and they can't count any of the straight-party ballots." *AP Online*, 8 November 2000; "Ballots Withheld in New Mexico"

November, 2003, Indiana. Computer voting machines in Boone County, Ind. — not manufactured by Diebold or Sequoia — somehow recorded 144,000 votes cast in a country where only 19,000 registered voters live. When corrected, it turned out a mere 5,352 ballots had actually been cast. "Computer Glitch Changes Indiana County Election Result" *Associated Press*, November 12th, 2004, archived: http://www.verifiedvotingfoundation.org/article.php?id=5251

Officials in **Broward County, Florida**, had said that all the precincts were included in the Nov. 5, 2002, election and that the new, unauditable ES&S touch-screen machines had counted the vote without a major hitch. The next day, the County Elections Office discovered 103,222 votes had not been counted. Here's perspective on this: Remember the flap about a missing ballot box found in a **Dade County, Florida**, church daycare center in the 2000 presidential election? ." *CNN: Breaking News,* 8 November 2000; "Election 2000: Strange Events Plague Florida Polls." One hundred and three thousand uncounted votes represents about 1,000 ballot boxes. Broward Deputy Elections Supervisor Joe Cotter called the mistake "a minor software thing ." *The Post-Standard,* 5 December 2002; "More Florida Blunders; Precious Votes Should Be Counted"

"I knew something was wrong when I looked up the results in my own precinct and it showed zero votes," said Illinois Democrat Rafael Rivera, according to the *Chicago Tribune*. "I said, 'Wait a minute. I know I voted for myself.'" The problem cropped up during **the Lake County, Illinois**, election held April 1, 2003. Clerk Willard Helander blamed the problem on ES&S, the Omaha company in charge of operating Waukegan's optical-scan voting machines. Rivera said he felt as if he were living an episode of *The Twilight Zone*. No votes showed up for him, not even his own. "It felt like a nightmare," he said. *Chicago Tribune*, 6 November 1993; "Kane Election Results Just Didn't Compute"

***November 2002, Georgia*: Fulton County** election officials said that memory cards from 67 electronic voting machines had been misplaced, so ballots cast on those machines were left out of previously announced vote totals. Fifty-six cards, containing 2,180 ballots, were located, but 11 memory cards still were missing two days after the election. Bibb County and Glynn County each had one card missing after the initial vote count. When DeKalb County election officials went home, they were missing 10 cards. Memory carda are the ballot box. The electronic ballot boxes for the Diebold machines used in Georgia are about the size of a credit card. With the new electronic voting systems, you can pocket a dozen ballot boxes at once or carry 67 ballot boxes around in your purse. *Atlanta Journal-Constitution*, 8 November 2002; "2002 Election: 2,180 Fulton ballots located after tally 67 memory cards misplaced ... "

April 2002, Johnson County, Kansas: Johnson County's new Diebold touch-screen machines, proclaimed a success on election night, did not work as well as originally believed. Incorrect vote totals were discovered in six races, three of them contested, leaving county election officials scrambling to make sure the unofficial results were accurate. Johnson County Election Commissioner Connie Schmidt said that internal checks revealed that the system had under- and over-reported hundreds of votes. Schmidt said the voting machines worked fine, they just tabulated wrong. "The machines performed terrifically," said Robert J. Urosevich, president of Diebold Election Systems. "The anomaly showed up on the reporting part." The problem, however, was so perplexing that Schmidt asked the Board of Canvassers to order a hand recount to make sure the results were accurate. Unfortunately, the touch-screen machines did away with the ballots, so the only way to do a hand recount was to have the machine print simulations of ballots from its internal data. Diebold tried to recreate the error in hopes of correcting it. "I wish I had an answer," Urosevich said. In some cases, vote totals changed dramatically. *The Kansas City Star*, 5 April 2002; "Election errors unnerve Johnson County official"

November 2002, North Carolina: Elections officials tried to find 300 voters so they could vote again. In Wake County, North Carolina, one out of four new touch-screen voting machines failed in early voting,

losing 294 votes. Election workers looked for the 294 voters to ask them to vote again. *The News & Observer* Raleigh, NC, 31 October 2002; "Machines lose 294 early votes"

This is just a sampling of a dozen or so items among the hundreds that have appeared in the mainstream press. After every election, we hear this happy refrain: "The election went smoothly." More recently, as election activists have brought concerns to light, this has become: "Though some people expressed concerns about the voting machines, the election went without a hitch." Here's the hitch: You don't discover miscounts until you do an audit, which does not take place on election night, and errors sometimes aren't identified until several days later, if at all.

Most errors are detected only when voter sign-in sheets are compared with vote tallies. Many of the errors listed in this chapter were found *only* because the number of votes cast did not match the number of voters who had signed in. But suppose 100 votes are cast, 55 for Mary and 45 for John, but the computer says you have 100 votes, 48 for Mary and 52 for John. John wins, and no one's the wiser.

But they are tested and tested and tested again. This is the official rebuttal when you ask whether machines can miscount. More on this testing later, but for now, suffice it to say that the ultimate invalidation of the testing a voting machine endures would be ***a machine that can't count!***

How do voting-machine companies respond to these reports? With shrugs and very little concern. They say that their miscounts are nothing to be concerned about. One of their favorite phrases is: "It didn't change the result." Except, of course, when it did: In the 2002 general election, a computer miscount overturned the House District 11 result in **Wayne County, North Carolina**. Incorrect programming caused machines to skip several thousand partyline votes, both Republican and Democratic. Fixing the error turned up 5,500 more votes and reversed the election for state representative. *The News & Observer* , 9 November 2002; "'Winners' may be losers"

Voting machines failed to tally "yes" votes on the 2002 school bond issue in **Gretna, Nebraska**. This error gave the false impression that the measure had failed miserably, but it actually passed by a 2 to 1 margin. Responsibility for the errors was attributed to ES&S, the Omaha company that had provided the ballots and the machines. *Omaha World-Herald*, 6 November 2002; " A late night in Sarpy; glitches delay results"

According to the *Chicago Tribune*, "It was like being queen for a day — but only for 12 hours," said Richard Miholic, a losing Republican candidate for alderman who was told that he had won a **Lake County, Illinois**, primary election. He was among 15 people in four races affected by an ES&S vote-counting foul-up *Chicago Tribune*, 4 April 2003; "Returns are in: Software goofed Lake County tally misled candidates, officials."

Putting aside for a moment (admittedly a difficult thing to do) issues of security and reliability, isn't it the ultimate testimonial to the incompetence of the manufacturers of electronic voting machines that **their machines just plain can't count?**

VVPATs Are Not Compliant With The Illinois Election Code

Diebold AccuView and Sequoia VeriVote Printer

The Illinois Election Code requires a conveniently verifiable paper record of the voter's choice(s), and this is required of all ballots so that they can be "easily reviewed by the voter for completeness and accuracy." The paper record that is printed by the Dielbold AccuVote-TSX touch-screen system with Accuview printer and the Sequoia AVC Edge VeriVote printer includes a barcode which theoretically represents the voter's choices.

However, the barcode cannot be "easily reviewed by the voter for completeness and accuracy," thus the current Dielbold AccuVote-TSX and Sequoia AVC Edge configurations fail to comply with the Illinois Election Code (10 ILCS 24/C-2) as a barcode cannot be "easily reviewed by the voter for completeness and accuracy." In fact, it is extremely difficult, and impractical, for the voter to review a barcode for completeness and accuracy.

Further, as neither system printer produces a distinct individual paper ballot or record, but rather relies on continuous-roll thermal paper that is retained within the touch-screen unit, this record cannot be "easily reviewed by the voter for completeness and accuracy," nor does it produce a “permanent record” for audit and recount.

Because the set of software modules that produces the barcode is not identical to that which produces the voter-verifiable data, the accuracy of one does not ensure the accuracy of the other. Further, the data which is transmitted to the central tabulation system (either WinEDS or GEMS) is generated by yet a third module. While the voting machine companies attempt to sell this as redundancy which ensures accuracy, it is more on the order of divide and conquer – no one knows for sure that all the vote totals are the same, nor which one is used in the final certified tally.

Voters With Disabilies

A significant marketing talk point used by manufacturers of touch screen voting devices is their supposed ability to provide election officials with an easily implemented means of complying with HAVA requirements. However, as we have noted previously, Title III of HAVA, entitled “Uniform and Nondiscriminatory Technology and Administration Requirements” [Section 301(a)] sets forth the standards that voting systems must meet after January 1, 2006. While certain touch screen (DRE) devices may indeed meet such standards, they are by no means the only way that local election jurisdictions may choose to comply.

Diebold is no exception. When extolling the virtues of the AccuVote-TSX, they state on their web site (http://www.diebold.com/dieboldes/accuvote_tsx.htm):

“Every AccuVote-TSX voting station offers voice guidance capability enabling blind voters to navigate through the entire ballot without assistance and in complete privacy. A voter makes candidate selections and casts their ballot all on one unit, providing an increased voting process integrity.” As we have previously noted, U.S. Election Assistance Commission Advisory 2005-004 states: “This advisory should not be read to preclude the innovation and use of accessible voting systems other than DREs for purposes of meeting this requirement.”

“The ten pound voting tablet, with 15 inch screen, can be easily used to facilitate curbside and nursing home voting, eliminating the need for a paper ballot for these applications.” However, it seems unlikely that this feature could be implemented in Illinois as removing the “tablet” disconnects the unit from the AccuView printer, thus failing to provide the VVPAT required by the Illinois Election Code.

Just how well the AccuVote-TSX works for voters with disabilities compared to other devices might be inferred from this article, “Spencer Lane Report on Voting Technology Accessibility,” posted online at (http://www.verifiedvotingfoundation.org/article.php?id=6135). On June 7, 2005, Lane visited the Annual Conference of the Florida State Association of Supervisors of Elections at which voting machines were on display. The only three being represented as handicapped-friendly models were the Diebold Accuvote TSX system, The ES&S Automark and the AccuPoll AVS1000.

Lane says, “The first machine we evaluated was the Diebold Accuvote TSX assisted by Wes Krivanek who, most generously, gave us several hours of his time, and later Mark Earley. Two machines were used. S/N 202010, contained Georgia software and a disabled voter interface. After several unsuccessful attempts to boot the system, the disabled interface was moved to the 2nd machine, S/N 201267 which we were told was programmed with Florida Certified Software.” (Does this sound suspiciously like a 50% failure rate?)

“My wife and I then “voted” on 202010 (sans interface) while Paton, voted on the disabled configured machine, 201267. With the screen blanked off, a synthesized voice led her through the ballot. My wife had a problem that it took 5-7 screen “pushes” before any of her actions registered. Wes observed that and postulated that perhaps her nails (which were slightly longer than mine) may be causing the problem. Even with her repeated pushes, her vote took just over three minutes. I had no problems and my fat fingers got a response on each touch, completing my ballot in just under three (3) minutes.”

"Paton[1]s vote using the handicapped audio interface to outline the ballot through headphones took 31 minutes, much longer than I had thought it would.. The handicap interface was a "telephone keypad" style with 12 keys to be selected than pressed. To select the appropriate key number required sightless touch-counting of the keys to locate the correct one before it could be pressed. (Think of placing a call on a telephone in the dark)"

Another disadvantage pointed out was: "In the audio review of her ballot after it was cast on the Diebold TSX Touchscreen unit with Florida approved software, the synthesized voice says, "Your choice has been selected" without specifying just what that choice was. Without audible verification in her headset she had no way of knowing if the votes she cast were recorded correctly."

"Paton Axelrod also tested the ES&S Automark system for handicapped voters, S/N ENG 023) as our seriously sight-impaired voter. With the screen darkened (as was the Diebold) and going through a similar audio interface, Paton listened to the complete ballot and voted on all the choices. The voting took only 9 minutes, less than one third the 31 minutes the Diebold required. The through-put of 6 sight-impaired voters per hour on the AutoMark vs only 2 per hour on the Diebold seems extremely advantageous."

"The sight-impaired AutoMark interface consisted of a large round central button surrounded by four large triangular arrow shaped buttons at the 12:00, 3:00, 6:00 and 9:00 positions. The points of the triangles pointed Up, Right, Down and Left respectively in a manner similar to many TV remote controls. Paton reported she found the AutoMark Control interface easier to use and more intuitive than the Diebold as it had larger and fewer buttons and did not require searching the keypad for specific numbers."

"The AutoMark is also an optical scan unit. In contrast with the Diebold unit, It produces a voter-verifiable ballot identical to the present ballot now in use. After voter verification of the ballot, it is placed in the existing optical scanner for tabulation."

While the "testing" of a few persons in a marketing environment is hardly definitive (as Lane himself points out) the concerns voiced ought to give the Board reason to carefully consider whether-or-not to offer interim certification to a device that even in the highly-controlled vendor environment performs significantly less effectively than a the type of device already approved by the Board last September. It would appear that the ballot-marking device is both easier to use and more cost-effective than the Dielbold AccuVote-TSX, an important consideration when considering that the AccuVote-TSX is being considered primarily for providing Section 301(a) access for disabled voters.

When confronted with the extensive list of DRE malfunctions, vendors routinely assure election officials that the problems are being fixed, that the "glitches" are being taken care of and that all will be well in the next election. That, however, has not proven to be the case as the malfunctions experienced in 2000 and 2002 were present in even greater numbers in the 2004 election.

With the approval of available of reliable and cost-effective tactile ballot technology and ballot marking devices, no bona fide reason exits to introduce expensive, unreliable and insecure touch-screen computerized-voting equipment in Illinois. HAVA doesn't require DREs, and Illinois voters don't need them!

Alternative Systems and Devices

Braille Templates

Braille templates have been in use for more than two decades in more than 30 states. This low-end technology has provided visually impaired voters who use standard Braille with the ability to cast their votes in privacy with little need for intervention from poll workers. A long-time supplier of re-useable plastic templates is MEMCO. Their site http://www.memco.net/ballot.htm explains the technology and indicates that the cost is extremely low compared to DRE technology, averaging about $100 per precinct for relatively complex ballots.

The State of Rhode Island has developed a convenient, reliable and cost effective technology which permits private voting for visually disabled voters. The technology is called “tactile ballot templates.” Tactile ballot template technology does not require the use of computers. Instead, tactile technology requires an audio tape, a set of headphones, paper ballots and ballot marking equipment.

The cost of the equipment (including printed ballots) is approximately $800 per polling place. Here is an informative descriptions of tactile ballot technology prepared by the International Foundation for Election Systems which has implemented systems in Albania, Macedonia, Armenia, Nicaragua, Bangladesh, Peru, Canada, Sierra Leone, Cambodia, Sri Lanka, El Salvador, Ukraine, Ghana, Kosovo, Zambia and the United States. http://www.electionaccess.org/Bp/Ballot_Templates.htm. This site documents the technology and explains its use.

The tactile ballot template points the way to possible improved low-end technology, but does have drawbacks, including adapting the system for multiple languages. Certain technical issues will have to be resolved before it is fully HAVA compliant.

Vote-PAD

Touch-screen ballot machines billed as the ideal solution for disabled voters are facing unexpected competition from a newly designed system using inexpensive plastic sleeves and paper. Called the Voting-on-Paper Assistive Device, or http://www.vote-pad.us/, the device has won high marks from some advocates for the disabled, and has already been selected for use in California's Yolo County in order to meet federal voting-accessibility requirements.

With Vote-PAD, poll workers fit specially designed sleeves over paper ballots. Audio instructions guide visually impaired voters to bumps on the plastic next to each race. Holes in the sleeve corresponding to ovals on the ballot allow voters to mark the ballot with a pencil or pen without going outside the oval. Afterward, voters can run a specially designed LED wand over the ovals to verify their choices. "This is a very generic, very simple solution," said Freddie Oakley, Yolo County's registrar of voters. "We don't have to train poll workers to do anything complicated."

The Voting-on-Paper Assistive Device (Vote-PAD) is an inexpensive, non-electronic, voter-assist alternative that helps most people with visual or dexterity impairments to vote independently. The Vote-PAD can be used in any jurisdiction. It is customized to provide access to each precinct’s hand-counted or optically-scanned paper ballot. All jurisdictions must offer provisional ballots during federal elections, and many also provide paper ballot backups in case voting machines break down. It is particularly suited for jurisdictions that use hand-counted paper ballots.

The heart of the Vote-PAD is the transparent “ballot sleeve,” which encloses the ballot on both sides and reveals the content of the ballot that slips into it. The Vote-PAD is composed of one custom ballot sleeve for each sheet of a ballot. The sleeves are bound together between front and back opaque covers for privacy. Holes are cut out of the sleeve at locations where a voter can mark choices. The sleeve protects the ballot from stray marks. A page-turning aid is attached to the outside of each sleeve and each cover to assist voters with dexterity impairments in turning the pages.

Yolo County, for example, was looking at spending $250,000 just to design storage space to house the accessible optical-scan machines it was considering purchasing for each precinct, on top of the thousands it would have cost for each machine. Vote-PAD, by comparison, costs $2,000 per polling precinct, which includes software to create audio instructions and enough sleeves to last a precinct five years.

Vote-PAD works for both hand-counted ballots and optical-scan paper ballots that pass through an electronic reader. One drawback is that the system is better for small counties than large populations that speak multiple languages.

AJ Devies, a member of Handicapped Adults of Volusia County in Florida, tested Vote-PAD and found it fully accessible. "People who have a closed fist, which is what happens with cerebral palsy or arthritis or after a stroke, often overlap onto another area when they go to touch a place on a touch screen," she said. The machine either records their vote incorrectly or fails to record a vote at all. "What we found (with Vote-PAD) is that it allows them to darken the circle without going outside the lines because of the thickness of the ballot sleeve," Devies said.

Vote-PAD shares some of the shortcomings of tactile ballots in terms of multiple languages but still holds promise as an alternative to the relatively more expensive DREs. In addition to these potential low-end technology solutions, Illinois voters also have the opportunity to use two additional devices.

AutoMARK

In addition, on September 13, 2005, the Board certified the AutoMARK The AutoMARK is a ballot marking system provides privacy and accessibility to voters who are blind, vision-impaired, or have a disability or condition that would make it difficult or impossible to mark a ballot in the usual way. In addition, it provides language assistance to voters who are more comfortable speaking an alternative language or who have reading difficulties. The AutoMARK voter assist terminal has been developed with input from election authorities and disability organizations, and meets all the requirements of HAVA.

Voters insert their standard optically scanned ballot-punch-card width or standard page width-into the slot, and the AutoMARK reads the ballot style. There's no need for a special ballot. Voters can use the touch screen to scroll through the options and make their selections. Then the AutoMARK prints the selections onto the ballot, and the ballot is returned to the voter to be cast in the regular fashion. These features of the AutoMARK device make it ideal to integrate with the current plans to purchase optical scan equipment for each precinct:

Disabilities which might prevent a voter from marking a ballot range from blindness or impaired vision, to an age-related condition such as arthritis or Parkinson's disease. In addition, a temporary condition such as a broken arm could make it difficult for a person to mark his or her vote. The terminal displays each race on screen in a variety of magnifications, and the voter uses the touch screen to make a selection. Blind voters or those with impaired vision can choose to listen to the choices through headphones.

The AutoMARK provides Alternative Language Accessibility: Assuring that all citizens in a diverse population can exercise their privilege to vote, visual and audible ballots in multiple languages can be stored on a single machine.

The AutoMARK does not tally or store votes; it simply marks a conventional paper ballot which is then cast by the voter. The paper ballot can be audited in the same manner as hand marked ballots. This means that ballots produced by the AutoMARK can be used both in hand-count audits and full election recounts.

The AutoMARK works with and enhances all major optical scan/mark sense voting systems currently in use. It is expected that the vast majority of voters will continue to manually mark paper ballots during the election process. Voters with disabilities or a personal preference will be able to use the AutoMARK by inserting the same paper ballot used by other voters. After all decisions have been made by the voter, the AutoMARK prints those selections on the paper ballot which is then cast by the voter in a manner identical to all other voters, using existing optical scanner hardware/software solutions.

The AutoMARK also allows for write-in candidates where appropriate. Voters can spell their candidate's name using a touch-screen keyboard. Blind voters can use audio prompts to navigate through and select letters one at a time. After all selections are made and the answers have been confirmed by the voter, the AutoMARK prints the name of the designated write-in candidates in the appropriate locations on the ballot.

The AutoMARK does not require a special ballot. Voters with disabilities and those requiring language assistance use the same ballot as any other voter. The AutoMARK scans the ballot to determine the appropriate ballot style, and presents the choices for each race in sequence. Once the voter has made his or her selections, the AutoMARK fills in the ovals or squares and prints the write-ins as entered by the voter. The voter then takes the marked ballot to the tabulation equipment, just like any other voter. There is no need to print special ballots, and voters with disabilities get the same privacy and confidentiality as other voters.

Over-voting cannot occur when a voter uses the AutoMARK to mark his or her ballot. The AutoMARK software has been developed to ensure that no more than the proper number of candidates can be chosen for each race. The AutoMARK minimizes under-voting by providing voters with a summary page of their selections. Voters will be able to notice any skipped races and are free to change their selections prior to printing.

Populex

On January 9, 2006, the SBOE approved the Polulex Digital Paper Ballot system. The Populex Digital Paper Ballot™ is created with an easy-to-use computer-based touch screen system. In contrast to most other touch screen voting systems that collect and store votes electronically inside the computer, the Populex voting system prints a tangible voter-verifiable paper ballot card.

This ballot card is the official ballot. Each voter receives one card. The final ballot contains a bar code that is scanned to record and count the votes on election day. The same ballot card is the paper audit trail that must be available for manual audits and recounts as required by the Help America Vote Act of 2002.

The voter can be highly confident that his or her votes will be counted because the voter sees and verifies the paper ballot contents.

The system is interactive, so the voter is guided through each ballot question, warned of potential errors and given a chance to make changes immediately in the privacy of the voting booth.

Those who are blind or visually impaired can vote privately using text-to-speech technology, fulfilling another requirement of the new Act. The Populex voting system also supports voting in multiple languages.

We like the idea of the combination of touch screen technology coupled with a paper ballot that is the official ballot. However, as we have highlighted above, the The Populex Digital Paper Ballot™ falls short of meeting the requirements of the Illinois Election Code, to wit:

The Code provides that a conveniently verifiable paper record of the voter's choice(s) be made available for review prior to the casting of the ballot. 10 ILCS/ 24C-2. "This permanent paper record shall be printed in a clear, readily readable format that can be easily reviewed by the voter for completeness and accuracy." This requirement is intended to apply to all of the vote data that is printed on the paper record.

However, the paper record that is printed by the Populex Digital Paper Ballot™ touch-screen ballot-printing system relies on a barcode which represents the voter's choice(s) and is used for tallying those choices. A barcode cannot be "easily reviewed by the voter for completeness and accuracy." In fact, it is both difficult, and impractical for the voter, absent specialized equipment, to review a barcode for completeness and accuracy.

While the Populex Digital Paper Ballot™ is highly preferable to touch-screen DREs, the barcode feature, which we believe violates the provisions of the Illinois Election Code should prevent certification. If the Polulex system could be modified to accept the standard digital scan ballot, it would become a viable alternative (along with the AutoMARK) to the Sequoia AVC Edge, Diebold AccuVote-TSX and Hart Inter Civic eSlate.

Advantages of Paper Ballots with Optical Scanners

- **All voters use an identical ballot and the same system.** Absentee, disabled, military, and provisional voters use the same ballot; and the voter can immediately verify that the right ballot has been issued.

- **Paper ballots are easily understood by voters and are inherently voter verified.** All of us have had experience with pencils & paper; most of us have taken tests or filled out lottery tickets to be read by an optical scanner.

- **Paper ballots allow each voter to vote only once.** Each voter is given a single ballot when signing in at the polling place. Some DREs require “smart cards” to be inserted in the computer to allow voting. These could be compromised and used to vote several times.

- **Precinct-based optical scanners allow voters to correct mistakes and detect over-votes and under-votes**. Incorrectly completed ballots (e.g., over-voted ballots, smudged ballots, etc.) will be rejected by the scanner. Voters can then exchange the spoiled ballot for a new blank ballot and correct their mistakes. In the case of under-votes, they have the option of completing the same ballot or having the scanner accept it as is.

- **The paper ballot is the official record of the vote.** Since the vote is recorded by the voter on the paper rather than electronically, the scanner only counts the votes into memory and then deposits the ballot into a locked ballot box. The paper ballot marked by each voter is the official record of the vote and is used in recounts.

- **Paper ballots for optical scanners are easy to recount by hand.** Lay-out is clear and on quality paper, whereas DRE paper records are light, quickly-fading print on thermal, ATM-type paper; recounts are difficult.

- **Paper ballot systems easily accommodate additional voters at low cost.** If a precinct has an unexpectedly large turn-out, only additional privacy booths must be provided, since a single scanner can handle voters from multiple privacy booths and election districts.

- **Voters can continue to vote on paper ballots in the event of equipment failure.** Both DREs and optical scanners have back-up batteries; but in the event of a prolonged power failure or other type of equipment failure, voting can continue on paper ballots that later are either fed into the scanner or handcounted.

- **Voting will take less time and lines will move fast with paper ballots.** Some people, particularly the elderly, find computers unfamiliar and will find the marking of a paper ballot more comfortable than using DREs. Separate ballot marking devices will enable other voters to continue voting even when it takes longer for a disabled person, an elderly person, or someone needing to use the multi-lingual features of the marking device to vote. Optical scanners take just seconds to read and verify a ballot, and no problems with lines are experienced in states using precinct based scanners**.**

- **Only one optical scanner and one small marking-device per precinct will require less storage between elections.** Optical scanners and ballot markers are much smaller than DREs and can be stacked in storage, requiring far less storage space and cost during the year than DRE systems. They are also small, and easy to transport to and from polling places during elections and do not require professional movers to handle them.

- **The scanner only counts votes;** therefore, it is much less complex and will require much less maintenance and upgrading over the years than DREs which are a newer, unproven technology. Although the data is not yet complete, preliminary surveys indicate that DREs increase the per voter cost of elections by more than 50 percent.

- **Optical scanners are a reliable, mature technology that has been used successfully in U.S. elections for 20 years.** About 30% of precincts in the United States use paper ballots and precinct based optical scan systems. Many states are now adopting PBOS systems to meet HAVA compliance.

The Illinois State Board of Elections has already given interim certification to two ballot marking devices which can be used in conjunction with optical scan devices. An appropriate and feasible system for accommodating voters with disabilities currently exits obviating the need for additional complex, expensive, fragile, unreliable and insecure electronic devices such as touch-screen terminals. The people of Illinois expect and deserve voting systems which inspire confidence that every vote counts and that every vote will be counted. The Illinois Ballot Integrity Project urges the Illinois State Board of Elections to adopt this more reasonable approach to guaranteeing the integrity of the vote for Illinois citizens.

When confronted with the extensive list of DRE malfunctions, vendors routinely assure election officials that the problems are being fixed, that the "glitches" are being taken care of and that all will be well in the next election. That, however, has not proven to be the case as the malfunctions experienced in 2000 and 2002 were present in even greater numbers in the 2004 election.

With the approval of available of reliable and cost-effective tactile ballot technology and ballot marking devices, no bona fide reason exits to introduce expensive, unreliable and insecure touch-screen computerized-voting equipment in Illinois. HAVA doesn't require DREs, and Illinois voters don't need them!

Conclusion

In the foregoing, we have attempted to set forth the primary reasons why privatizing elections in America is fraught with peril. It's no coincidence that the companies that manufacture and distribute electronic voting systems are frantically competing for a share of the multi-billion dollar pie that Congress has baked for them. Wally O'Dell tried to convince Diebold shareholders that his company could derive nearly $2 billion from this enlarged market. Voting machine companies, largely until now, a cottage industry, intend to grow fat at the public trough. Profits not democracy are their *raison d'être.* And if control over who gets elected by letting private companies count our votes is one result – so much the better.

To put the industry in perspective, Sequoia Voting Systems received a contract for more than $50 million to supply voting systems for Cook County and the City of Chicago – the same Sequoia that changed hands in March, 2005 for a mere $17.6 million. Chicago and Cook County might have been better off to buy the whole company and cut out the middleman!

It's just this aspect of the industry that largely accounts for the unholy mess they've made of electronic voting. Few, if any, companies in the industry have the financial or human resources to produce a product that satisfactorily meets the needs of state and local election officials. Is it any wonder that electronic voting machines breakdown so often, or that votes disappear, or phantom precincts arise from the vapor? With undisciplined and unsophisticated programmers, should it be a surprise that source code is poorly documented, written in obsolete languages and full of security holes? That one professor who

looked at the source code of one system said that if a student of his had submitted this code as a project he'd get an "F?" Unfortunately, the answer to all of these is: "No."

We have examined in turn three major areas of performance: Security, Reliability and Accuracy. In each discussion we've shown that the products being offered in today's marketplace just don't measure up. Would you go to the hardware store and buy a lock with a combination that's published in every newspaper? Or, a car that only starts one time in ten? Or a scale that weighs heavy one time and light the next, and does it differently every time? Of course you wouldn't. But election officials all around the country are buying machines just like those locks, cars and scales . . . with ***our*** tax dollars.

In the foregoing we've given you dozens of examples the documented failures of electronic voting machines, our list is by no means exhaustive. We've quoted from well-known and respected computer scientists, consulting companies and elected officials. Problems with voting machines aren't a figment of our imagination – they're very real and they imperil our right to free, honest, fair and accurate elections. This isn't about partisan politics, it's about our fundamental right as Americans to have our voted counted – and counted correctly. Paper ballots are a known quantity, the easiest, most transparent and reliable system yet devised. It's more than obvious that touch-screen voting devices can't do the job . . . but paper ballots have and can. "High-tech" implementation can wait until electronic voting technology is proven to be secure, reliable and accurate. American voters deserve better than what's currently being offered by private voting machine companies.

Notes and Acknowledgements

This paper would not have been possible without the untiring research of many people from many different organizations like Voters Unite, www.votersunite.org; Black Box Voting, www.blackboxvoting.org; True Vote Maryland, www.truevoteMD.org; from whom I have borrowed liberally, especially in developing the documented examples quoted herein. I am also grateful for the support of members of the Illinois Ballot Integrity Project www.ballot-integrity.org who have also contributed to the completion of this document.

Academics like Dr. Avriel Rubin, Dr, David Dill, Dr. Douglas Jones and many others have provided election activists with the seminal research into the more arcane features of computer languages and the world of encryption. Their work has contributed much to our understanding of some of the underlying issues addressed herein.

We are also indebted to those public officials, like Ion Sancho of Leon County, Florida and California Secretary of State Bruce McPherson who have taken the lead in efforts to provide citizens with honest elections.

My role has been much less author than editor as I have attempted to develop a cohesive blend of fact and advocacy. Please thank those both named above and others unnamed who have worked so diligently in the pursuit of American democratic ideals – they have done the tough work in the trenches. For any shortcomings you may find in the foregoing, the responsibility is mine alone.

Robert A. Wilson
Evanston, Illinois
January 22, 2006

Additional copies of this document may be downloaded at www.ballot-integrity.org/DRE_22-Jan-06.pdf