Black Box Voting

History of the Controversy

- Before the 2000 election, a private company wrongfully purged over 50,000 voters from the Florida voting rolls.
- The Florida election was plagued by ballots that were undecipherable or otherwise faulty .
- After the 2000 election debacle, Congress passed HAVA, the "Help America Vote Act."
- Using HAVA funds, many states are rushing to buy the newest electronic "touch screen" voting machines.
- The private companies that create these machines assert that their software is a trade secret.

So What's the Big Deal?

- What was always intended as a transparent and public process—counting our votes—is now subject to the veil of corporate secrecy.
- Computer systems are inherently vulnerable to glitches, software errors, and tampering.
- No voter, no citizens' group, no academic experts are permitted to verify the integrity of these machines, either before or after the election.
- No paper trail exists to verify our votes.
- Wireless communications can help make wholesale and widespread vote-rigging virtually undetectable.

Are we in danger of losing our democracy?

3/14/04

Who creates these Machines?

Voting-machine companies are not required to reveal their ownership. Several of the companies are as secretive about their ownership as they are about their voting systems.

However, three of the top six voting machine companies are known to have owners and/or directors who represent special vested interests:

Election Systems & Software

A key owner of ESS, the largest company, is Michael McCarthy, the campaign finance director for Sen. Chuck Hagel (R-NE). Hagel was CEO of the company when the machines that counted his votes were built.

Diebold

Diebold's CEO is Wally O'Dell, one of an elite group of George W. Bush fundraisers. Following a meeting at Bush's ranch in August of 2003, O'Dell wrote a memo promising to "deliver the votes" in Ohio to Bush.

VoteHere

VoteHere manufactures the cryptography software used in other companies' machines. VoteHere's chairman, Admiral Bill Owens, is a close Cheney supporter and a member of the Defense Policy Board.

What can I do to ensure that our elections remain free and fair?

- Demand that a paper ballot be used for all vote counts, not merely for recounts.
- Demand legislation guaranteeing integrity and openness in our electoral system.
- Get more ideas at http://ballot-integrity.org

Diebold Election Systems and Common Ties to ES&S

Diebold Elections Systems is run by **Bob Urosevich,** who has been working in the election systems industry since 1976 and is a active Republican which has led to questions of conflict of interest. **In 1979, Mr. Urosevich founded American Information Systems.** He served as the President of AIS from 1979 through 1992, and **that company, now known as Election Systems & Software, Inc. (ES&S),** counted over 100 million ballots in the U.S. 2000 General Election. **Bob's brother, Todd Urosevich,** is Vice President, Aftermarket Sales with ES&S.

In 1995, Bob Urosevich started I-Mark Systems, whose product was a touch screen voting system utilizing a smart card and biometric encryption authorization technology. **Global Election Systems, Inc. acquired I-Mark in 1997**, and on July 31, 2000 Mr. Urosevich was promoted from Vice President of Sales and Marketing and New Business Development to President and Chief Operating Officer. **On January 22, 2002, Diebold announced the acquisition of GES,** then a manufacturer and supplier of electronic voting terminals and solutions. The total purchase price, in stock and cash, was $24.7 million. **Global Election Systems subsequently changed its name to Diebold Election Systems, Inc.**

Together, ES&S and Diebold Election Systems are (as of 2004) responsible for tallying approximately 80% of the votes cast in the United States. The software architecture common to both is a creation of Mr. Urosevich's company I-Mark. Some experts claim that this structure is easily compromised, in part due to its reliance on Microsoft Access databases. Britain J. Williams, responsible for certification of voting machines for the state of Georgia and a consultant to Diebold, has provided an assessment based on his accounting of potential exploits.

In August 2003, Walden O'Dell, chief executive of Diebold, announced that he had been a top fund-raiser for President George W. Bush and had sent a get-out-the-funds letter to Ohio Republicans. When assailed by critics for the conflict of interest, he pointed out that the company's election machines division is run out of Texas by a registered Democrat. Nonetheless, he vowed to lower his political profile lest his personal actions harm the company.

DES claims its systems provide strong immunity to ballot tampering and other vote rigging attempts. These claims have been challenged, notably by Bev Harris on her website, Blackboxvoting.org (http://www.blackboxvoting.org), and book by the same name. Harris and C. D. Sludge, an Internet journalist, both claim there is also evidence that the Diebold systems have been exploited to tamper with American elections —a claim Harris expands in her book Black Box Voting. Sludge further cites Votewatch for evidence that suggests a pattern of compromised voting machine exploits throughout the 1990s, and specifically involving the Diebold machines in the 2002 election. **DES also has come under fire for the recent discovery that the Diebold voting machines do not and did not in 2004 meet the Help America Vote Act (HAVA) error standard.**

Teresa Hommel
www.wheresthepaper.org

Statement Against the Use of Money
Allocated under the Help America Vote Act
for the Purchase of Electronic Voting Systems for New York

Before the Governmental Operations Committee
of the New York City Council
October 18, 2004

Thank you for the opportunity to speak before you today. My name is Teresa Hommel. I have been working as a citizen activist on the issue of electronic voting for the last 16 months. My professional credentials are that I have worked with computers since 1967 as a programmer, technical writer, corporate trainer, and consultant.

I am here today to caution New York City against urging our state to move forward with the purchase and use of electronic voting systems.

There are two alternative approaches: One is for New York State to keep our old lever machines, and add one accessible ballot-marking device per polling place. The other is to switch to paper ballots and precinct-count optical scanners, with one accessible ballot-marking device per polling place.

What's wrong with electronic voting systems?

(1) They don't work reliably.

Attached to my testimony is a packet of materials. The first item is 63-page list of failures of electronic voting systems. Only six vendors are represented. There are 13 pages for Sequoia, and I put these pages first because many people think Sequoia will be the vendor selected in New York, if we go to electronic voting.

For every failure on this list, I would assume that there were many others that went undetected -- errors that you need an audit to find: votes recorded incorrectly, and wrong final tallies. Since no electronic voting system has ever been audited, we can't know how many errors of that kind have been made.

(2) Federal certification does NOT mean that a voting system works. "It has to have [certain] functions. But it doesn't have to work."

The second item in your packet is the I-Team interview with MicroVote Executives. MicroVote makes electronic voting systems. This quote comes from page 2, the candid remarks about certification made by Bill Carson.

We've had hundreds of failures of certified voting systems in this country, but some people need to read an interview like this to bring it home -- certification does not mean the systems work.

(3) Even if electronic voting systems worked perfectly today, they may not work tomorrow because they are so easy to hack.

A person with moderate computer skills can read information that has been on the internet for over a year, and then hack these systems to give falsified election results. The hack takes less than a minute. You don't need direct physical access, because it can be done over a phone line and modem, a wireless communication device in the voting system, or over the internet.

Last month in Washington D.C., Bev Harris of BlackBoxVoting.org held a press conference where she demonstrated how to change the votes in a Diebold GEMS central tabulator and in a Sequoia system. She was dismissed by the major media, but in fact the "Trusted Agent Report" commissioned by the Maryland General Assembly said the same thing last January about the Diebold GEMS central tabulator (they used more technical language, and didn't publicize the exact methods like Bev Harris did).

"Given either physical or remote access ... it is possible to modify the GEMS database ... without detection. Furthermore, system auditing is not configured to detect access to the database."

(4) The security of these systems cannot be monitored or enforced by the people responsible for them.

The vast majority of elections professionals are not computer experts. Once they convert to electronic voting, they become dependent on vendor technicians to handle the computers. And they can't monitor what's going on because they don't know the technology.

For example: A technician walks over to the computer and says, "I better check the files." Who's going to question that? Or understand the answer if they do ask? Yet that brief access to the computer is a large-enough window of opportunity for someone to falsify an election.

(5) Computers conceal the process of ballot recording and vote counting, which is contrary to democracy.

The 2500-year history of elections tells us that whenever some part of an election procedure is concealed from public view, errors and fraud will occur. Electronic voting systems convert the heart of our elections to an invisible process, and we shouldn't do that.

(6) Computers give you speed. Audits give you accuracy.

In Albany we had two one-house bills on voting system standards that passed in February, 2004. Both bills required a voter-verified paper audit trail (VVPAT). One bill required a 2% surprise random recount, the other required 3%.

The VVPAT is essential with electronic voting, but it's only the first of two requirements. To detect all errors and fraud, we have to use the VVPAT to perform a complete audit on every election.

If a surprise random check of a small percentage of transactions could ensure the accuracy of a computer system, no bank or other company would ever spend the time and money to perform a complete audit. Companies do complete audits of their computer systems on a continuous basis, because that's the only way to find and correct errors which, if your customers see them, you'll lose your customers.

An audit performed by counting the voter-verified paper ballots in public would restore public oversight. If the tallies of paper ballots and electronic ballots differ, however, this requires an investigation into the conduct of the election (to determine whether there were irregularities by people) AND a computer audit (to determine whether the computer made an error).

Does any Board of Elections have the staff, expertise, or resources to perform a computer audit? One obstacle is that a computer audit requires thorough knowledge of the software used, and to my knowledge, all major vendors claim that their software must remain a trade secret.

At any rate, a complete audit of an election run with electronic voting systems would be far more complex, costly, and time-consuming than the effort required to securely guard paper ballots that were marked by hand, and to recount them before an audience of observers.

(7) The Help America Vote Act requires voters with disabilities to have a "private and independent vote."

This requirement should mean more than a private and independent experience in a voting booth, fiddling with a touchscreen or some assistive devices.

But in fact, electronic voting systems don't give anybody a private and independent VOTE.

Every vote cast is handed over to a large number of anonymous technical people who have been responsible for the system from its initial design, programming, testing, maintenance, storage, programming for the ballot, transportation, and installation in the polling site. And another cast of characters after the election.

A computer is only an instrument created and managed by people. Every voter using the computer is being assisted by these people, so the vote is not unassisted, private or independent. Without the complete audit I discussed before, we can't know if these assistants are recording our ballot choices, or counting our votes, honestly and without mistakes.

Voters who are blind, or have visual impairments, would get accessibility, privacy, and security if they mark paper ballots by using ballot templates like they have in Rhode Island and in other countries. There are data-to-voice scanners that can read the paper ballot back to the voter through headphones. There are

accessible ballot-printing and ballot-marking machines, such as Populex or Automark, that can assist voters with a wide variety of disabilities.

(8) Elections are not about "my vote," they are about the will of the people.

In states with electronic voting, some people have suggested that if any voter doesn't want to cast his or her vote on a computer, they should request a paper absentee ballot. But elections are not just about "my vote," they are about the will of the people--all votes. If computers are the wrong technology for elections, as I believe they are, they are wrong for all voters.

(9) You can't fix a broken democracy by throwing a computer at it.

If democracy is government "of the people, by the people, for the people," I think it is time we ask, "Where are the people?" We need to put people back into the center of our elections, and not replace citizen participation by computers.

If people knew how desperately their participation was needed, more would respond.

(10) States and big cities that use paper ballots and optical scanners.

Illinois, Chicago. 83% of the population of Illinois (10 million) votes using such systems, including Chicago. One Illinois County's rationale:
http://www.willclrk.com/votingsystem.htm#Why%20was%20the%20optical%20scan%20system%20sele

80% of Arizona, including Phoenix.
http://www.azsos.gov/election/voter_outreach/info.htm

Michigan Secretary of State's recommendation:
http://www.michigan.gov/sos/0,1607,7-127-1640_9150-43906--M_2001_5,00.html

States that use mostly precinct-count optical scan systems also include
South Dakota http://www.sdsos.gov/2000/00pripre.htm
Minnesota http://www.sos.state.mn.us/election/Interactive%20Election%20Guides/HTML/15.htm

Seattle:
http://www.metrokc.gov/exec/news/1998/vote421d.htm

(11) The CalTech/MIT study of voting systems found that precinct-count optical scan systems outperformed DRE voting systems in terms of residual voting errors and cost per voter.

CalTech/MIT Voting Project, http://www.vote.caltech.edu/Reports/

Five Myths of invulnerability in touch screen voting systems

http://homepage.mac.com/cems/voter/myths.html

Even though fraud is not the issue we want to rely on, it's worth countering myths about voting system invulnerability.

1. Touch screen proponents will tell you the scale of conspiracy required to achieve an intrusion or software backdoor is huge.

This is not true. Most backdoors are not deliberate but simple coding errors. And most exploits are found and viruses written by a single person. Witness for example yesterday's discovery of an unintentional backdoor in Windows arising from a single line of source code missing a single word. Even if this had been deliberate, it passed all code reviews and lurked for years; it did not require any conspiracy, and was discovered by a lone hacker.

2. Touch screen proponents will tell you that source code certification and escrow is enough to protect us.

This is not true. All of the documented mistakes to-date were on systems that fully passed all testing and certification, exceeded all state federal standards, and many had escrowed source.

Source code escrow has proven useless since although the code is escrowed the so far states are not allowed to look. Worse, the public has no access and the most trained eyes are prohibited by non-disclosure agreements.

3. Touch screen proponent will tell you that their voting kiosks are invulnerable because they are never connected to an insecure Internet connection.

This is not true. An equivalent statement has been be made for the much more tightly regulated Automatic Teller Systems used by banks. These are never connected to the Internet, in theory. In fact, the internet worm Blaster infiltrated the ATM systems of two major banking institutions. How? Because even though it was against policy, someone somewhere did connected a computer directly to the Internet, if only for a moment.

Moreover, though any given computer might never be connected to the Internet, the software on it was almost certainly written on a computer that was connected. Indeed it was probably written in another country.

4. Touch screen proponents will tell you that since future ballots may not be known at the time the vendor programs the machine they can't put anything bad in the software.

This is not true. For example, a machine could be rigged such that when a malicious voter touches the screen in a certain combination of places then whatever ballot is cast next will become the "desired" outcome for the machine. This is exactly how slot machine software has been rigged (to change the payoff schedule following a combination of coins and button presses). Other successful slot machine hacks include using the daily "testing software" to secretly re-program the systems en-mass through a backdoor. It should be noted that the security controls for successfully attacked Nevada slot machine software obey much tighter regulation than voting machine software yet hundreds of millions are stolen.

5. Touch screen proponents will tell you systems can't be corrupted because Election Officials only enter data, not programs.

This is not true, and in fact is the single most common attack. Election officials work at a deliberately simplified level normally only entering ballot description file. In principle this is just data not a program in exactly the same sense that an e-mail message is just data, a word processor document is just data, and a web page is just data; the underlying program is unchanged by the data, in theory. But all of these similar cases have been compromised when bugs allowed the data to contain executable instructions.

Indeed, a newly-found Windows backdoor is entered by opening a photograph in the web browser. Theoretically, an image is pure data, but a bug placed executable instructions on the command stack. One would be truly naive to believe that elections software won't contain analogous exploitable bugs that allow program alteration via innocuous ballot description files.

Five Myths of invulnerability in touch screen voting systems

http://homepage.mac.com/cems/voter/myths.html

Even though fraud is not the issue we want to rely on, it's worth countering myths about voting system invulnerability.

1. Touch screen proponents will tell you the scale of conspiracy required to achieve an intrusion or software backdoor is huge.

This is not true. Most backdoors are not deliberate but simple coding errors. And most exploits are found and viruses written by a single person. Witness for example yesterday's discovery of an unintentional backdoor in Windows arising from a single line of source code missing a single word. Even if this had been deliberate, it passed all code reviews and lurked for years; it did not require any conspiracy, and was discovered by a lone hacker.

2. Touch screen proponents will tell you that source code certification and escrow is enough to protect us.

This is not true. All of the documented mistakes to-date were on systems that fully passed all testing and certification, exceeded all state federal standards, and many had escrowed source.

Source code escrow has proven useless since although the code is escrowed the so far states are not allowed to look. Worse, the public has no access and the most trained eyes are prohibited by non-disclosure agreements.

3. Touch screen proponent will tell you that their voting kiosks are invulnerable because they are never connected to an insecure Internet connection.

This is not true. An equivalent statement has been be made for the much more tightly regulated Automatic Teller Systems used by banks. These are never connected to the Internet, in theory. In fact, the internet worm Blaster infiltrated the ATM systems of two major banking institutions. How? Because even though it was against policy, someone somewhere did connected a computer directly to the Internet, if only for a moment.

Moreover, though any given computer might never be connected to the Internet, the software on it was almost certainly written on a computer that was connected. Indeed it was probably written in another country.

4. Touch screen proponents will tell you that since future ballots may not be known at the time the vendor programs the machine they can't put anything bad in the software.

This is not true. For example, a machine could be rigged such that when a malicious voter touches the screen in a certain combination of places then whatever ballot is cast next will become the "desired" outcome for the machine. This is exactly how slot machine software has been rigged (to change the payoff schedule following a combination of coins and button presses). Other successful slot machine hacks include using the daily "testing software" to secretly re-program the systems en-mass through a backdoor. It should be noted that the security controls for successfully attacked Nevada slot machine software obey much tighter regulation than voting machine software yet hundreds of millions are stolen.

5. Touch screen proponents will tell you systems can't be corrupted because Election Officials only enter data, not programs.

This is not true, and in fact is the single most common attack. Election officials work at a deliberately simplified level normally only entering ballot description file. In principle this is just data not a program in exactly the same sense that an e-mail message is just data, a word processor document is just data, and a web page is just data; the underlying program is unchanged by the data, in theory. But all of these similar cases have been compromised when bugs allowed the data to contain executable instructions.

Indeed, a newly-found Windows backdoor is entered by opening a photograph in the web browser. Theoretically, an image is pure data, but a bug placed executable instructions on the command stack. One would be truly naive to believe that elections software won't contain analogous exploitable bugs that allow program alteration via innocuous ballot description files.

Six Ways to Attack a Touch Screen Computer

http://homepage.mac.com/cems/voter/hacks.html

Easter eggs and code bombs

At Microsoft it's a firing offense to insert "Easter eggs" (secret backdoors) in software, and code is given multiple layers of security reviews. Despite this thousands of MS Easter eggs have been documented, some of staggering proportions (A flight simulator appeared in Excel when the right spreadsheet rows were clicked in the right order.) Recently discovered security holes that let viruses propagate have been in place for almost a decade.

Maryland's SAIC commission on touch screen voting has said in regard to voting system software that its 99.9% certain that maliciously inserted back doors would never be detected via code review.

Physical access hacks

Virtually all computer experts agree that if you can get unattended physical access to a computer you "own" it.

The Albuquerque Tribune reported that 47 polling machines were destroyed when the truck carrying them crashed. Only because of this serendipity was it learned that the drivers escorting these machines to the polls were 1) drunk, 2) had no driver's licenses, 3) had left the machine unattended in the parking lot of Hooters for hours, and 4) were caught in a part of Albuquerque not on the path to the polls. Despite laws, policies and good intentions our own election officials cannot guard these machines from physical access. Nationally, machines are commonly left protected only by simple locks. Last month it was demonstrated that amateurs could pick the locks on the Diebold system in under ten seconds. The Ohio Secretary of state noted that the same Sequoia systems kiosks New Mexico has approved will go into supervisor mode if an unsecured yellow button on the back is pressed - no lock picking needed.

Binary Code hacks

Of course source code is not what runs on the machines. The complied binary is what is actually loaded. So how do you know that the binary that was loaded corresponds to the human-readeable source that you reviewed? This is a very very tricky technical problem. Source escrow does not address this at all.

Data Transport hacks.

Voter data has to be stored and transported somehow; memory cards, disks, or Internet. And it has to be collated on some computer. It has already been proven that the encrypted "tamper-proof" Diebold memory cards are anything but tamper-proof and the votes can be undetectably altered. Not only can vote collation systems modify vote totals, already have they been hacked in actual elections.

In King County (Seattle, Redmond), the election officials found it cumbersome to use Diebold's GEMS database access software due to its security features and limited capabilities. Instead they used an unauthorized tool to directly access the database, bypassing the security system. They had the capability to alter the system logs to erase any record of a change made to vote totals done by this backdoor. Did they make illegal changes and erase the logs? One hopes not, but no one can actually prove it did not happen.

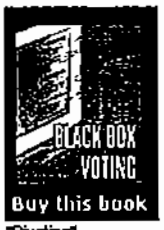
Access Card hacks

Commonly, a single-use activation card is given to the voter that allows him to go into the "booth" unattended and cast only a single vote. It's been shown already on Diebold systems that these cards can be forged. Worse yet, similar, forgable, cards are commonly used by Election Supervisors to program the machines.

Embedded Processor hacks

Most "computers" actually contain several embedded slave computers you rarely think about. For example, the graphics card and CD ROMs can contain reprogrammable firmware and would be an excellent place to unobtrusively attack a touch screen system.

Another approach is $50 device, about the size of an olive, that can inserted into any keyboard cable; its called a "key logger" and it's actually an embedded computer that can record and alter any keystrokes or screen presses.



"Riveting"
— *Vanity Fair*
"The gospel of the movement"
— *Time Magazine*

black box voting
CONSUMER PROTECTION FOR ELECTIONS
www.BlackBoxVoting.Org

6/12/05: Request to the California Secretary of State Under Election Code 19202

Jim March, Member of Board of Directors, Black Box Voting 916-370-0347 / jmarch@prodigy.net
Bev Harris, Executive Director, Black Box Voting 206-335-7747 / bev@blackboxvoting.org

EC19202 reads as follows:

> Any person or corporation owning or being interested in any voting system or part of a voting system may apply to the Secretary of State to examine it and report on its accuracy and efficiency to fulfill its purpose. The Secretary of State shall complete his or her examination without undue delay.

Black Box Voting, Inc., a nonpartisan, nonprofit, 501c(3) consumer protection organization for elections, requests a formal examination under this statute of a specific Diebold Election Systems component: the programmed "electronic ballot box" memory cards used in optical scan and touch-screen voting systems.

As your office may be aware by now, Black Box Voting, Inc. was allowed to test the Leon County, Florida Diebold optical scan system (firmware 1.94w). During this testing, we proved that Diebold memory cards contain executable code, that the firmware in the optical scan places a "call" to the executable code on the memory card, and that the operation of the election system can be changed in various malicious ways without detection. We succeeded in loading altered code onto the optical scan via the memory card, which altered votes undetectably. We also succeeded in pre-stuffing the ballot box in a way that does not alter the overall number of votes, but flips a predetermined number of votes to another candidate.

We specifically request that the Secretary of State's office evaluate the following:

1. Whether or not executable code is present on these cards;
2. Whether or not the firmware of the touch-screen and/or the optical scan (either precinct count or central count) ever places a call to executable code on the memory card;
3. Under what specific conditions any executable code on the memory card is checked by the firmware for accuracy (via checksums, hashes, file size);
4. Whether or not it is possible to load manipulated code on the memory card so as to perform malicious functions such as vote shaving, vote "skimming," vote changing, altered reports, altered audit log, pre-stuffing of the ballot box, over-writing results of other precincts, or any other substituted code;
5. Whether or not it is possible to override and invalidate the California certified version of the firmware or software by executing program "updates" via the memory card.

We make this request for:

1. The latest optical scan systems (firmware 1.96.4);
2. The paperless touch-screens as used in Alameda County on Nov. 2, 2004;
3. The new TSx system proposed for certification;
4. Any older optical scan models still in use in California.

Note that on touch-screen precinct terminals, the exact filenames involved on the memory card and the type of executable may be different than those on the optical scan systems. The call to the executable may be obscured in Dynamic Link Library (".dll") files. We have found references to this under the name "abc." All files under the name "abc," AboBasic," "AccuBasic," and "ABasic" should be examined to determine exactly where they are invoked in system designs for all Diebold voting equipment.

We also have evidence that altered code can be centrally loaded on ALL cards from GEMS by altering files at the **C:\PROGRAM FILES\GEMS\ABASIC** directory, propagating the "hack" either county-wide or to hand-selected precincts as a batch. We believe the altered code can be linked to a specific day, can be loaded months or even years prior to elections, and can be constructed so as not to appear during pre-election and post-election Logic and Accuracy tests.

Both of us have personally witnessed Diebold employees, other contractors, and even local volunteers handling Diebold memory cards, unsupervised by county officials.

We are convinced that a design which invokes executable code on a memory card is unsupportable in a certified software environment where security is of critical importance. This code is allegedly "certified," but if a standard feature exists within the design allowing alteration of code on removable modules, long after certification and even during the middle of elections, the intent appears to be to provide a vote-tampering mechanism. This Diebold design clearly sacrifices security for "flexibility" – and in the election environment, that translates to "quick and easy tampering."

We ask for a timely response on this matter. Regardless of what you find, we request that a formal report be issued to address these issues as soon as possible.

Jim March
Member of the Board of Directors
Black Box Voting, Inc.

Bev Harris
Executive Director
Black Box Voting, Inc.

Could one hacker alter an entire election?

Last Revised November 21, 2004
http://www.mutanteggplant.com/singleagent.htm

The failure of the media to take seriously any potential major and global problem with the 2004 election is due in part to a failure of imagination. **Most media people assume that to steal the entire election would require a huge conspiracy involving thousands of people operating in thousands of locations.** The problem with a huge conspiracy is that something is going to get royally messed up in the process giving away the game. It's just too complicated to pull off. Nixon couldn't pull off a simple break in without getting caught and giving us the nightmare of Watergate.

Thus the media reports the occasional "glitch" as if it were an isolated incident and not a part of a bigger picture. Yet, serious observers are very concerned that just such a theft may have occurred. http://www.ecotalk.org/Recounts.htm

The purpose here is to suggest a simple hypothetical method by which a single person (the agent) acting alone could have stolen the election. We are not arguing that this in fact happened but are merely describing a potential method that could have been used. **The first requirement for this single agent hypothesis is the existence of a computer communications network interconnection most if not all of the nation's machines doing the actual counting. Two companies Diebold and ES&S produce the systems that counted 80% of all votes from both computerized ballot scanners and touchscreen machines.** Perhaps a network interconnecting these tally machines would be sufficient to throw an election. http://www.ecotalk.org/UrosevichBrothers.htm There has been conjecture that the National Election Pool (NEP) used to disseminate vote counts to the news media uses just such a network. http://www.ecotalk.org/VNS.htm

A reporter observed an NEP employee attach a laptop computer to the ES&S vote tally machine in Chicago. Don't even try to contemplate the many nefarious things this laptop can do. http://www.ecotalk.org/APvotes.htm

A simple way to dismiss this agent conjecture is for the NEP to explain how they collect the vote counts without using such a network and to prove that such a nationwide network does not exist during voting. We will assume for purposes of this conjecture that the network exists and, for example, is a private IP network (using Internet protocols but not an actual part of the Internet).

The agent needs access to this voting network. Bev Harris on her web site http://www.blackboxvoting.org, in her book **Black Box Voting** and in her video http://www.votergate.tv/ describes how **many tally computers are equipped with modems, and that these modems are often functional during voting, and that modem numbers are sometimes disclosed to outsiders inadvertently.**

Diebold systems are also deployed with wireless networks, probably Wi-Fi. The agent need only be with a few hundred yards of the Wi-Fi hub to secretly obtain a high bandwidth link to the network. The agent can be in their car outside a voting center with a laptop computer and have free access to the whole network. The Johns Hopkins study (see below) mentions that **Diebold's AccuVote-TS DRE can be connected to the Internet** (page 12). Please tell us this has never been done!

All our agent needs is access to a single functional modem or Wi-Fi hub during voting to access the entire voting network of vote tally machines. The agent dials into the machine or attaches to the Wi-Fi network or Internet and hacks his way onto the tally machine. The agent finds the networks to which this PC is connected, the network type and the network address. The use can use simple techniques such as ping to quickly uncover the IP address of every tally machine on the network and thus the typology of the network. The agent would hack the password to gain access to each machine. Need help? How about http://www.openwall.com/john/

The agent can then determine the type of software in use and the type of database involved in the voting for each tally machine. The agent would then hack each machine voter database. Bev Harris again describes how easy it has been to hack the passwords from the Diebold voting systems. Software is available to recover passwords from a windows system. We know that Microsoft Access is used by Diebold so the agent might simple buy the program to "recover" the passwords. http://www.openwall.com/passwords/office.shtml

Bev Harris also describes how easy it is to change the election count databases and how the log files can be modified to cover up the changes. In other words it seems plausible to change an election result, at least in the Diebold systems without leaving a trace. The agent now has all the information they need to modify the election results, not on a single tally machine, but on the entire network of tally machines. A detailed demonstration of hacking the tally machine without leaving a trace is now available http://www.chuckherrin.com/hackthevote.htm

You still don't believe the voting system is this vulnerable? **Try reading the current definitive Johns Hopkins study of the Diebold system at http://avirubin.com/vote.pdf**

Weren't these systems certified? Bev Harris received one certification report that is 75% redacted (blacked out) including all references to the version number. She recently received another certification that is not redacted. It reads like pure boilerplate and she has found no one connected with the certification who actually looked at any source code. How do you certify something you haven't studied?

Certifications are useless anyway since Diebold simply fixes bugs and patches the software without any regard for version control. California just settled its lawsuit against Diebold Nov 10 for $2.6 million. The settlement seals the information gathered for trial and stops further legal research but maybe some experts and lawyers involved can use what they have learned to fight elsewhere. https://verifiedvoting.org/article.php?id=5236

Want more horrors? Try this collection of information for voting officials trying to meet the new HAVA standards. This is a 63 page document.
http://www.votersunite.org/takeaction/mythbreakers.pdf

A teenage hacker agent might be tempted to just go wild with this power and put in crazy numbers like negative vote totals (possible) or far more votes than voters. **The more cunning agent who wants to throw the election surreptitiously will modify the votes more subtly in order to avoid tipping his game. It is important not to raise undo suspicion and not to trigger a recount.** In order not to trigger a recount or attract a challenge, the changed vote totals must result in an overwhelming victory. The agent can not chance a close election.

And while the agent is at it, why not go for a big popular vote margin countrywide. This is best done by narrowing the margins in overwhelmingly blue states and increasing the margins in overwhelmingly red states. For example the difference in NY between actual results and exit poll data is close to 600,000 votes. A few modifications like that and you quickly win a big margin of the popular vote as well as secure the Electoral College.

With the sole exception of Nevada, **the nation's e-vote machines have no voter verifiable paper so recounts are thought to be meaningless.**** If the agent has modified results in the tally database, an e-vote recount may not be meaningless. But the cunning agent can modify votes in tally machines counting optical scan ballots safely so long as a recount is never done. Thus those five counties in Florida where all the registered Democrats like to vote Republican using optical scan ballots needn't worry about discovery during a recount because there will never be a recount for those counties. **The agent would thus map out ahead of time the changes they want to make to the vote counts in each machine.**

The window of time to modify votes during the actual count is relatively narrow. The agent

would prepare an automated script containing all instructions to log into each system, make the required changes, log out, modify the logs and erase event log to cover all tracks and move on. This script would perform the changes to thousands of machines within the time window required.

Who might such an agent be? Any hacker is a potential candidate but would require a lot of study, care, and diligence. An agent working for a county or state dealing with the tally machines directly is a better candidate since he/she already knows a lot about the systems and has automatic access to the network and some passwords. **The best candidate is a technical employee of the vote system manufacturer** who has the most information, the best access, knows the most passwords, and is most knowledgeable.

Could our agent steal the election using modified software installed in each tally machine? Yes, but this possibility poses a higher risk of exposure is too complicated for anyone not intimate with the software currently running in each machine. In other words, use of illegal software narrows the field of suspects to those few people familiar enough with all the software to be able to create such illegal modifications. The modified software would have to be very sophisticated to make sure the modified vote counts don't trigger a recount or otherwise attract undue scrutiny for each individual tally machine.

Then the software must not only be distributed; it must be retrieved without discovery. **The best candidate software would be a Dynamic Linked Library (DLL) which Diebold personnel insist incorrectly is part of the windows operating system and not a part of the tabulating software. There are no controls whatever on the DLLs running of the tally machines.** DLL hell is a notorious Microsoft problem and source of error in windows applications. DLLs should always be hard linked to the application for critical and certified application such as counting the nations votes. The lack of software control in the voting tally machines is notorious but pulling off such a massive fraud without eventually leaving behind illegal software in a machine somewhere would be tough. This is not impossible but tough. **Database hacking is simpler and safer** for the amateur hacker.

None of the above is to suggest that any of this actually happened or to accuse any organization (NEP, Diebold or ES&S) of any wrongdoing. It is purely an exercise to examine a possibility. Is it possible even feasible that something like this might have happened?

Send your comments to Dennis Hall

Creeping Vaporization of the American Vote

A compilation of related observations on electronic voting and the ease of rigging elections

In NOV of **2000, about 12% of the ballots in America were invisible - created with secret software.**
In **2002, it was about 18%**
In **2004 over 30%.**
That's more than **30 million invisible ballots created with secret software in the most recent and controversial election!**

Election Fraud and Irregularities:

Voting machines are relatively easy to rig and almost impossible to monitor. There are several ways the mechanical lever machines can be rigged. Whoever controls access to the machines could, one-by-one, rig the machines. Thus the opportunity for election fraud exists, but it is also somewhat limited.

Computerized voting opens the door for a single individual to manipulate votes in elections across the country. Voting system firmware and software is proprietary (i.e, a trade secret) which can be hacked by outsiders or "updated" at any time by company technicians, much like Microsoft sends automatic upgrades to a home computer. **In the same way, electronic manipulation of votes could take place before, during, and after an election. It can be done offsite and remotely.**

There is a long history of election irregularities that suggests that vote fraud using voting machines has been occurring. Republicans appear to be the main beneficiaries. In the 2002 election 74% of upset elections went to Republicans by as much as 9-14% outside of the margin of error of the pre-election polls, according to reporter Alastair Thompson of Scoop.

Dan Wallach, for example, is a co-author of the Johns Hopkins study that ripped apart the security practices of Diebold, the largest maker of e-voting machines.

"I think you've missed one of the best technologies we've got for voting," he wrote. "It's called **precinct-based optical scanning.** The voter fills in a bubble with a pen on a printed paper ballot, then inserts it into the scanner above the ballot box. This sort of system satisfies what computer scientists have been grumbling about **(it's voter-verifiable -- voters see the ballot when they mark it up) and it has a low error rate. And, oh by the way, op-scan is much, much cheaper."**

But don't let your guard down yet.

Hacking Optical Scan Machines:

I can think of a pretty simple way to do it - if it is known that the test run will be, say, 100 ballots, set the software to flip every x vote (5th, 10th, 100th) a certain way after the number exceeds 200 or 300 or 1000. Vendors know the procedures, y'all. There's nothing magical about optical scanners - it's just software, too.

This is similar to a gas pump exploit used by the Mafia in Texas a while back. They knew that the accuracy testing for gas pumps was performed by taking a container measuring exactly 8 gallons from station to station and filling it up to exactly 8 gallons, then checking the gauge. They set the pump software to be right for the first 8 gallons, then started padding the price for gas pumped above that. They only got caught when somebody driving an RV noticed that the numbers didn't add up to what they should have - sort of a "gas pump exit poll".

Why Optical Scan Equipment?
Observations on rigging potential

Most fraud concerns prior to the election focused on the new touchscreen voting systems (DRE) which lack voter verifiable paper. These machines can be hacked in such a way that the results are altered without possibility of recounts (the perfect crime). DRE machines are popular with voters and may have been placed in locations where the voters are heavily conservative or where unusual results might have attracted immediate attention. We have also learned that Ohio did not deploy 200 DRE machines at all contributing to heavy voting lines so maybe there were not enough DRE machines to adequately change the results.

What is now clear is that optical scan voter equipment seem implicated in some statistical anomalies across several states. The Berkeley study now indicates that DRE e-voting machines may be implicated as well in Florida. Illegal software in DRE machines without voter verifiable paper will forever destroy all evidence of the voter's intent. The search for fraud must initially focus on those machines with paper evidence, the optical scan equipment. It may be possible to prove that illegal software was used in DREs but the true vote counts will never be known.

Lets look at optical scan models from three suppliers; Diebold, ES&S, and Sequoia Pacific.

There are two primary types; precinct and central.

With **precinct tabulators,** the voter inserts ballot and receives immediate overvote/undervote notification. These model are located at the actual voting place and are unlikely to be networked though they may be equipped with modems, either wired or wireless (Wi-Fi). Illegal software would likely be loaded into these models prior to their move to the precinct.

With **central tabulators,** ballots are counted centrally, away from the voters. Therefore the voter receives no overvote/undervote notification. This model is more likely to be networked and are certainly modem accessible with the possibility that illegal software can be loaded remotely just prior to counting. Further, these models are all PC based.

ES&S has two primary optical scan types. **The ES&S Model 100 precinct tabulator appears to be PC based and has two PCMCIA slots and RS232 ports for insertion or attachment of wired or wireless (Wi-Fi) modems.**

The second is the PC based ES&S Model **150, 550 and 650 centrál tabulator.**

The Sequoia Pacific Eagle Precinct Optical Scan has an optional modem. The Sequoia Pacific 400C also known as the IV_C Central Optical Scan is a PC based unit that also serves as the vote tabulator machine and can be networked.

The Diebold AccuVote OS is a precinct optical scan unit and is not networked or modem equipped.

Diebold's central tabulating unit is the GEMS which is PC based and **does not include centralized optical scanning.**

GEMS is also used to tabulate counts from the Diebold AccuVote TS DRE.

Does the official Ohio State site show real time (updated automatically) counting going on in Ohio?

Ohio Election Real Time Counts:
http://election.sos.state.oh.us/results/RaceDetail.aspx?race=PP

This is first evidence I have seen of a statewide network of vote tabulation machines.

"More than one year after submitting the TSx to the federal ITAs, more than six months after submitting its application for approval, more than five months after assuring the VSPP that completion of federal testing was imminent and more than four months after the vendor told the Secretary of State's Office that it had started a "new day" relating to the way it handled compliance with certification requirements, there is not a single version of the TSx firmware that has completed federal qualification testing for use in the November 2004 General Election."

STAFF REPORT
ON THE
INVESTIGATION OF
DIEBOLD ELECTION SYSTEMS, INC.
April 20, 2004

Presented to
Secretary of State Kevin Shelley
and the
Voting Systems and Procedures Panel

REMEDY?

Debarment of Vendors for Violation of Election Laws, Standards and Regulations

Source: CA Election Code Section 19214-19215

See Reverse

Debarment of Vendors
for Violation of Election Laws, Standards and Regulations

Source: CA Election Code
http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=elec&codebody=&hits=20

19214. The Secretary of State may seek injunctive and administrative relief when a voting system has been compromised by the addition or deletion of hardware, software, or firmware without prior approval.

19214.5. (a) The Secretary of State may seek all of the following relief for an unauthorized change in hardware, software, or firmware to any voting system certified or conditionally certified in California:

(1) Monetary damages from the offending party or parties, not to exceed ten thousand dollars ($10,000) per violation. For purposes of this subdivision, each voting machine found to contain the unauthorized hardware, software, or firmware shall be considered a separate violation. Damages imposed pursuant to this subdivision shall be apportioned 50 percent to the county in which the violation occurred, if applicable, and 50 percent to the Office of the Secretary of State for purposes of bolstering voting systems security efforts.

(2) Immediate commencement of decertification proceedings for the voting system in question.

(3) Prohibiting the manufacturer or vendor of a voting system from doing any elections-related business in the state for one, two, or three years.

(4) Refund of all moneys paid by a locality for a compromised voting system, whether or not the voting system has been used in an election.

(5) Any other remedial actions authorized by law to prevent unjust enrichment of the offending party.

(b) Prior to seeking any measure of relief under this section, the Secretary of State shall hold a public hearing. The Secretary of State shall give notice of the hearing in the manner prescribed by Section 6064 of the Government Code in a newspaper of general circulation published in Sacramento County. The Secretary of State also shall transmit written notice of the hearing, at least 30 days prior to the hearing, to each county elections official, the offending party or parties, any person that the Secretary of State believes will be interested in the hearing, and any person who requests, in writing, notice of the hearing.

(c) The decision of the Secretary of State, to seek any relief under this section, shall be in writing and state the findings of the secretary. The decision shall be open to public inspection.

19215. (a) The Secretary of State may seek injunctive relief requiring an elections official, or any vendor or manufacturer of a voting machine, voting system, or vote tabulating device, to comply with the requirements of this code, the regulations of the Secretary of State, and the specifications for voting machines, voting devices, vote tabulating devices, and any software used for each, including the programs and procedures for vote tabulating and testing.

(b) Venue for a proceeding under this section shall be exclusively for Sacramento

Clarification of Decertification/Recertification Orders from Secretary of State Kevin Shelley

Below is the clarification of the 23 security measures California Secretary of State Kevin Shelley is requiring California counties to meet in order to have their paperless, touchscreen voting systems recertified (not including the AccuVote-TSx system, which cannot be re-certified prior to the November election.)

Clarification of Conditions for Using Electronic Voting Machines at the November 2004 Statewide General Election

Many county elections officials have requested clarification of the 23 conditions for using DREs at the November election. Based on numerous conversations with elections officials, vendors and other interested parties, we are providing the following information.

1. Provide Option of Voting on Paper at Polling Places Should there be an unexpected failure of a voting system or any of its components, we want to ensure that voters are not disenfranchised. Therefore, paper ballots must be available at all polling places as a backup. A voter must have the option of voting on paper if he or she wishes. Provisional ballots may be used for this purpose. The Secretary of State's Office is committed to ensuring that any cost of making paper ballots available is not borne by counties.

2. Creating a Permanent Record of Each Ballot Cast We believe that creating a permanent record of each ballot cast is useful for purposes of subsequent auditing of the system even though the record created lacks the benefits of a voter verified paper audit trail. Therefore, as we directed at theMarch election, at least four original CD-Rs, DVD-Rs or DVD+Rs (**but not CD-RWs, DVD-RWs or DVD+RWs**) containing images of the voted ballots cast on each touch screen (DRE) voting machine used in the election must be created. Two of the disks should immediately be sent to the Secretary of State. Two of the disks should be retained by the county elections official. The Secretary of State's Office is committed to ensuring that any cost of creating the disks is not borne by counties.

3. Parallel Monitoring Following the procedures implemented at the March election, we will conduct parallel monitoring of voting systems at the November election. The monitoring will not involve taking any units out of service on Election Day. We will work with you to ensure that the monitoring does not interfere with the conduct of the election. Any costs will be borne by the Secretary of State's Office.

4. Provide a Technical Security Plan

We want to ensure that all reasonable steps are being taken to secure the voting system from tampering. Therefore, a Technical Security Plan must be submitted to the Secretary of State by September 17, 2004. The Plan should be consistent with the recommendations contained in the *RABA Report* (*Trusted Agent Report to the Maryland Department of Legislative Services by RABA Innovative Solution Cell (RiSC)* dated January 20, 2004 (http://www.raba.com/press.html?id=9), to the extent applicable, to the voting system being used. At a minimum, the Plan must, to the extent applicable to the voting system being used, provide for creating security key cards with computer-

generated passwords by precinct. By obtaining the plans, we anticipate being a resource for the counties by serving as a clearinghouse for "best practices" in this regard. However, in order to avoid compromising security, the details of the plans will be kept confidential by the Secretary of State. The Secretary of State's Office is committed to ensuring that any additional cost of preparing the Technical Security Plan is not borne by counties.

5. Federal Testing and Qualification Federal testing and qualification are essential to help ensure that all components of a voting system function accurately, reliably and securely. To the extent that federal testing and qualification apply, we believe that all components of a voting system must pass federal testing and qualification procedures. We are working with the vendors with respect to federal testing and qualification. This should not involve any county costs.

6. State Testing and Certification
Full state testing and certification is essential with respect to all components of a voting system to help ensure that the voting system functions accurately, reliably and securely. Therefore, these are requirements with respect to all components, including peripheral components such as precinct control modules or similar devices. We are working with vendors with respect to state testing and certification. This should not involve any county costs.

7. Late Modifications
We are concerned that in the past we were often presented with requests for approval of proposed last-minute changes in software, firmware or hardware. These requests often were made so close to the election that adequate federal or state testing could not be performed. Therefore, to allow time for adequate testing, proposed changes in software, firmware or hardware, with respect to the November election, must, except in the most extraordinary circumstances, be submitted by September 17, 2004. This should not involve any county costs.

8. No Official Results Received by Component Modem
Our security experts advise us that receiving official results through a public telephone system increases risks of tampering with electronic voting systems. Therefore, official results must not be received through a public telephone. This should not involve any county costs.

9. No Wireless Connection
Our security experts advise us that wireless telephone connections to voting system components increase risks of tampering with electronic voting systems. Therefore, wireless connections cannot be part of any voting system. This should not involve any county costs.

10. No Internet Connection Modem
Our security experts advise us that Internet connections increase risks of tampering with electronic voting systems. Therefore, Internet connections with any part of a voting system are not permitted, directly or indirectly, at any time. This should not involve any county costs.

11. Physical Security Plan
We want to ensure that all reasonable steps are being takento secure the voting system from tampering. Therefore, a Physical Security Plan must be submitted to the Secretary of State by August 4, 2004. The Plan should be consistent with the recommendations contained in the *RABA*

Report (*Trusted Agent Report to the Maryland Department of Legislative Services by RABA Innovative Solution Cell (RiSC)* dated January 20, 2004 (http://www.raba.com/press.html?id=9), to the extent applicable.
At a minimum, the Plan must, to the extent applicable to the voting system being used, provide for applying tamper resistant tape to terminals to prevent non-authorized entry of security key cards into the terminals and instituting strict procedures to prevent the use of unauthorized supervisor cards. By obtaining the plans, we anticipate being a resource forthe counties by serving as a clearinghouse for "best practices" in this regard. However, in order to avoid compromising security, the details of the plans will be kept confidential bythe Secretary of State. The Secretary of State's Office is committed to ensuring that any additional cost of preparing the Physical Security Plan is not borne by counties.

12. Compliance with Security Enhancements We want to ensure that all reasonable steps are being taken to secure the voting system from tampering and to ensure its accuracy, reliability, security and accessibility. Therefore, counties will be subject to poll monitoring such as that conducted at the March Statewide Primary Election and there must be compliance with all of the procedures set forth in the approved procedures for the particular voting system being used. In addition, as provided for in Elections Code section 15001, a copy of each election computer vote count program must be provided to the Secretary of State for escrow no later than 5 p.m. on the seventh day before the election.

13. Poll Worker Training
The success of the election depends, in large part, on poll worker training. Therefore, a Poll Worker Training Plan must be sent to the Secretary of State by September 17, 2004. By obtaining the plans, we anticipate being a resource for the counties by serving as a clearinghouse for "best practices" in this regard. The Secretary of State's Office is committed to ensuring that any additional cost of preparing the Poll Worker Training Plan is not borne by counties.

14. Communication Plan
One of the problems that was identified in some counties at the March election was difficulty in communicating between the polling places and the central elections offices. Therefore, a Communication Plan must be sent to the Secretary of State by September 17, 2004. By obtaining the plans, we anticipate being a resource for the counties by serving as a clearinghouse for "best practices" in this regard. The Secretary of State's Office is committed to ensuring that any additional cost of preparing the Communication Plan is not borne by counties.

15. Provisional Ballots on Paper There were problems at the March election with respect to processing electronic provisional ballots under Elections Code section 14310(c)(3)(A). Therefore, provisional ballots, except at early voting sites, must be on paper. The Secretary of State's Office is committed to ensuring that any additional cost of making provisional paper ballots available is not borne by counties.

16. Disability Access Devices
At the March election, we received complaints from some individuals with disabilities that some disability access devices attached to DREs did not work properly resulting in possible

disenfranchisement. We believe that it is appropriate to identify any problems with the disability access devices before the polls open so that the problems can be fixed before voting begins. Therefore, the devices must be tested before the polls open. This should not involve any county costs.

17. Posting of Results We believe that the Elections Code requires that after the polls have closed, results should be posted at the polling place for each electronic voting machine if the machine is capable of printing out results. The results should be posted for 48 hours but elections officials are not required to monitor the polling place after the polls have closed to ensure that the posting remains for the entire period. It is sufficient to advise the facility owner or manager that the posting should remain for 48 hours. Thisshould not involve any county costs.

18. Tampering Penalties In order to deter any tampering of electronic voting machines and consistent with the *RABA Report* (*Trusted Agent Report to the Maryland Department of Legislative Services by RABA Innovative Solution Cell (RiSC)* dated January 20, 2004 (http://www.raba.com/press.html?id=9), the penalties for tampering with voting devices should be posted. We will provide signs that can be used for this posting. This should not involve any county costs.

Vendor Conditions:
Several conditions involve vendors rather than county elections officials. For example, vendors must provide to the Secretary of State source codes and functioning systems as well as specific documentation regarding voting systems. These conditions are being discussed directly with vendors.

This page was first published on July 14, 2004 | Last updated on December 8, 2004
Copyright California Voter Foundation, All Rights Reserved.

http://www.insidebayarea.com/dailyreview/localnews/ci_2794606

State expected to OK new voting system

Diebold machine's flaws have been fixed since tests in spring, official says

By Ian Hoffman, Hayward Daily Review Staff Writer, June 10 2005
Inside Bay Area

In less than a week, state officials are poised to approve a new Diebold electronic-voting system that several large counties, including Alameda, want to use. But the system showed problems in security, protection of voter privacy and printing of a paper trail during testing this spring.

State elections authorities have obscured the full nature of those problems by blacking out parts of test reports that have been released under the state public records act and declaring other documents too full of Diebold "trade secrets" for public release.

During tests in late April and early May, a chief feature of Diebold's new computerized voting machine — the ability to print out voters' electronic choices so they can be verified and, if needed, recounted — **performed so poorly that the state's testing consultant concluded, "This version is not ready for use in an election."**

Assistant Secretary of State Brad Clark, a former Alameda County registrar, said Thursday the problems have been fixed and the Diebold system desired by county elections officials is ready for state consideration.

A panel advising Secretary of State Bruce McPherson is to vote on approval of the new Diebold touch-screen voting system next week. Elections officials say new systems like Diebold's are essential if California counties are to meet January 2006 federal mandates for handicapped voting and state mandates for providing a voter-verifiable paper record.

"The more options that are out there for the counties to use, the better off we are," Clark said.

Diebold's first efforts to secure approval for its AccuVote TSx in California ended in public distrust of all electronic voting and consideration of criminal charges against Diebold. That's partly because Diebold officials persuaded four counties to spend more than $40 million on the TSx — and state elections officials to approve its use in the 2004 presidential primary — before the system made it through lab tests and federal approval.

Secretary of State Kevin Shelley rescinded the TSx approval in April, and thousands of the machines now sit in climate-controlled warehouses in San Diego, San Joaquin and Kern counties.

Solano County dropped its Diebold machines and switched to another vendor. Alameda County elections officials want to swap out 4,000 older AccuVote TS machines for the TSx, which is

smaller, lighter and equipped with a printer for generating a paper record of a voter's choices for the voter to verify.

Before applying to California for approval, voting-system makers are required by state elections rules to subject their machines to lab tests and federal approval, then draw up procedural and training manuals for using them. None of this was done in October 2003 nor before Diebold applied for approval again in March.

"We're going through the same kind of scenario, not only from Diebold but from the (secretary of state's) elections division," said Jody Holder, a voting activist who unearthed reports on state tests of the new Diebold machines and e-mails between the state and Diebold through a public records request. "You can see from the e-mails between them that they're bending over backward."

"There's a sense of dj vu in this rush," said Kim Alexander, president of the California Voter Foundation, a nonprofit group based in Davis.

During the testing in late April and early May, the state's voting systems consultant, Steven Freeman, found that the TSx machines generally were an improvement on Diebold's earlier machines but still had security flaws. **For example, contrary to state election rules, the system was unable to allow different levels of security access to the machine's software and data, so that lower-level users can perform basic functions but only administrators can change or add software.**

The rest of Freeman's discussion of security problems was blacked out by state lawyers.

But the bigger problems were with the paper-trail printer. Freeman reported "several persistent problems with the paper feed" that resulted in a "jam condition." The printer canister kept popping out of place, he noted.

"Attempts were made to tape the canister down but failures still occurred, and someone had to hold the canister in place," his report says.

Keith Carson, president of the Alameda County Board of Supervisors, persuaded colleagues to have a public hearing so that Diebold and its critics could debate the merits of its voting system. Carson wants to hear what people say before investing another $5.4 million in a touch-screen voting system that the county purchased three years ago for $12 million.

"The question for me is, to what extent can we guarantee that everyone who participates in the voting process can have confidence that their vote counted," he said. "That to me is going to weigh as heavily as the dollars we have invested in a system that has been constantly in question."

Contact Ian Hoffman at ihoffman@dailyreviewonline.com.

FOR IMMEDIATE RELEASE
TrueVoteMD.org
March 8, 2005
CONTACT: Linda Schade 301-270-6665
http://www.truevotemd.org/Press_releases/html/2005-03-08_Press_Release.html

Emerging Scandal on MD Voting Machine Performance

All MD Diebold Machines on Lockdown
Under Investigation for Widespread Statewide Election Day 2004 Failures
MD Election Group Calls for Independent Investigation and De-Certification of Machines

Montgomery County, Maryland. According to county election officials and other sources, all Maryland voting machines have been on "lockdown" since November 2, 2004 due to statewide machine failures including 12% of machines in Montgomery County, some of which appear to have lost votes in significant numbers. The State Board of Elections convinced the media that Election Day went smoothly, when in fact there were serious statewide, systemic problems with the Diebold electronic voting machines -- so serious that the SBE and Diebold still have not figured out how to prevent the loss of votes in the future.

"Election Day was anything but smooth. Votes were lost, computer cards storing votes were unreadable, thousands of error messages were reported, machines froze in mid-voting and machines refused to boot up. The problems with the machines were so widespread and serious that efforts to hide the problems have failed," said Linda Schade, director of TrueVoteMD.org. "It is not sufficient for Diebold and the SBE to investigate themselves. They have misled the public about this problem and an independent investigation is needed. Further, these problems indicate that the Diebold machines should be decertified as required by Maryland law and as provided for in the Diebold contract. This is an opportunity to correct the mistaken purchase of paperless electronic voting machines. Diebold should refund Maryland tax dollars and we should start anew with a system that voters trust because it can be independently audited and recounts can be meaningful."

VOTES LOST According to the IT Report to the Montgomery County Election Board, dated December 13, 2004 there were two broad levels of problems. Seven percent of units (189) failed. This included failure to boot up, screen freezes and a variety of other problems. Screen freezes, which occurred on 106 voting units were "the most serious of errors" because many "froze when the voter pressed the Cast Ballot button." As a result "election judges are unable to provide substantial confirmation that the vote was in fact counted." In addition there were "122 suspect units (5%) were identified because the unit had few votes captured compared to other voting units in the 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," the report stated. The IT report includes other details of Diebold machine failures including smart card and encoder problems as well as thousands of yet unexplained error messages, now called 'ballot exception errors."

UNREADABLE PC MEMORY CARDS Multiple sources also have revealed that the computer memory cards where vote totals are stored inside each voting machine were unreadable in multiple counties.

DIEBOLD UNABLE TO RESOLVE TECHNICAL FAILURE FOUR MONTHS AFTER ELECTION After IT examinations within Maryland failed to decipher the root of these problems, the State Board and Diebold sent voting machines to several out-of-state locations in Texas and Ohio for further testing, according to a Diebold memo dated February 16, 2005. As of the March 3, Montgomery County Election Board meeting, the PC memory card problems as well as those listed above cannot be explained by Diebold, according the IT report.

MACHINE FAILURES STATEWIDE Montgomery County Elections official Sam Statland has acknowledged that local boards around the state are gravely concerned about the Diebold system's performance and are pressuring the State Board of Elections for answers. In testimony before the State House Ways and Means on February 24, 2005, Mr. Statland cited the facts above and asserted that "Since the 2000 election cycle, the State of Maryland has become and still is a 'test site' for electronic voting." In the January State Board of Elections meeting, Linda Lamone discussed the "performance problems" and confirmed that "once [Montgomery County was] finished they will start the same process in the other counties, beginning with Baltimore County."

TRUEVOTEMD CALLS FOR INDEPENDENT REVIEW AND DECERTIFICATION OF MACHINES AS REQUIRED BY LAW TrueVoteMD.org, an election integrity organization, is now calling for an independent investigation and for de-certification of the machines as required by Maryland election law (MD Code, Election Law § 9-102(c)(1)).* TrueVoteMD.org is a founding organization for VoteTrustUSA a national network of state election integrity groups and has been raising the alarm that the electronic Diebold voting system has serious vulnerabilities to computer malfunction and fraud for nearly two years. This information is confirmed by TrueVoteMD's Election Day report "When the Right to Vote Goes Wrong: Md Voters Tell The Story of Election Day 2004" http://www.truevotemd.org/Resources/MDproblems04map.pdf.

"If the gubernatorial race in 2006 is as close as 2002 it would only take four errors per precinct to change the outcome of the election. Maryland cannot risk the election disaster that is impending. Maryland was lucky the presidential election in Maryland was not close; otherwise we would be embroiled in scandal to this day. It is time to put in place a system that is reliable and that voters can trust," concluded Schade. "Three independent reports have raised serious concerns with the security of Diebold machines, now we have seen the worst come to pass. These machines are unreliable and insecure. How many more warnings to Maryland officials need in order to take action to protect the vote?"

*MD Code, Election Law § 9-102(c)(1) (emphasis added). The SBE "shall decertify a previously certified voting system if" that system "[does not] protect the security of the voting process," and "[does not] count and record all votes accurately." Id. § 9-103(a)(2) (emphasis added).

Copies of the source documents mentioned in this release are available upon request by contacting TrueVoteMD.org.

###

TrueVoteMD is a non-partisan election integrity organization made up of candidates, elected officials, election judges, pollwatchers, and voters from all walks of life who support a voter-verified paper audit trail to ensure the accuracy, transparency and security of elections.

TrueVote MD
www.TrueVoteMD.org · 7711 Garland Ave., Takoma Park, MD 20912 ·
301-270-6150

Violations of VSPP Procedures and State Elections law in Certification of Voting Systems

The official Procedures for approval of a voting system for use in California require a complete Application to be submitted before examination may begin. This was not done, and still has not been done.

Among the items that are REQUIRED prior to examination beginning are:
* NASED-approved ITA certificate stating that the item follows FECguidelines. Currently HAVA requires that the "voting system" in totality meet 2002 Voting System Standards (2002 VSS).

California's Election Code **19250 (a)** requires that after January 1, 2005 the SoS may not approve a DRE unless the "system" has received "federal qualification" and includes an accessible VVPAT. In subsection (d) it then defines what "federal qualification" means. The system must have been certified by means of qualification testing as required by the FEC, EAC, and HAVA.

Both HAVA and NASED require that any "voting systems" tested and certified in 2005 must qualify to 2002 VSS. Both reports refer to various "components" having met 2002 VSS qualification but also **state that the "system" as a whole only is qualified to 1990 VSS.** That is against both federal law, state law, and the SoS Procedures.

The SRA, p. 6 claims that GEMS 1.18.22 has completed federal qualification testing to 2002 VSS. Yet the NASED website list of Qualified Voting Systems does not state that.
The referenced Qualification Numbers cited by the SRA contain some components that have been qualified to 2002 VSS, **but the system is qualified to 1990 VSS, and no where does it show GEMS 1.18.22 qualifying to 2002 VSS.**

In fact the updated list of Diebold "voting systems" shows that not one of them has qualified as a "system" except to 1990 standards. Remember, state and federal law, etc. refer to "voting systems", not individual components.

In the SRA p. 15 item 15 the staff declares that copies of the qualification testing reports have been received and are on file.
Yet the SFES reports (page 4 top) that the **final test reports for GEMS version 1.18.22 have not been received from either the hardware nor software ITAs.**

Steve Freeman even concludes his summary by referring to making his recommendations conditional "pending receipt of the ITA reports." **This is the exact same sequence of events that occurred in October and November, 2003 when Diebold kept promising the reports and qualification numbers would shortly be issued.** Even the elections staff themselves assured the VSP panel that everything was qualified and the number would be issued at any moment. **Nearly two years later and the same tactics are still being utilized to get a system California approved.**

* NASED approved testing reports of all tests conducted.
As referenced above, these have not been received yet (as of June 7, 2005).

California Procedures for use of the System (Note: Final Draft Procedures must be received at least 45 days prior to the VSP Panel meeting in which the item will be considered). The Procedures were not received until the week before last. The VSP panel should not be hearing this Agenda Item until at least 45 days after receipt of the Final Draft Procedures.

Other issues:

Barcode on the paper receipt.
I have asked Bruce McDannold for clairification because I have come across the same information both in a previous email and now in this staff report. He claims to not be aware of this issue. The paper record is required by state law to be used for the 1% MANUAL audit and for any recount.

Yet in the SRA, p. 4 they refer to the barcode on the VVPAT "for easier tabulation in an audit after the election." I would like to have clarification on this issue. **State law requires that all paper records of votes be manually counted during the audit and any recounts. Reading a barcode to speed up the process would be against both state and federal law.**

This also raises the problem of what is on the barcode. Both reports discuss the issue of preserving the secrecy of the ballot. They addressed that by removing from the 'printed portion" of the VVPAT the ballot serial number. Yet in an email exchange it is inferred that the ballot serial number may be contained in the information in the barcode. If that is the case then in any audit or recount an individual ballot serial number could be determined and an individual voter identified.

Accessibility
In the SFES p. 2 he asks for "public comment" on the adequacy of the magnification qualities of the AVPM. I also have serious questions whether this system meets the requirements of federal and state law, including the January 21, 2005 Standards for AVVPAT.

Public Comment
We now can see what the SoS's Elections Division considers "Public Comment". See p. 21 of the SRA, section VI. On April 6 an "open house" was held at the SoS headquarters for *invited* representatives of the accessibility community, county election officials, members of the Technical Advisory Board. These invited members of the "public" subsequently wrote comments that were then submitted with this report (but they were not part of the report online).

One point I would like to point out as an example of the bizarre arguments promulgated by some in the disabled community, and cited as a "major issue" raised in the comments was the claim that the "voter verified paper trail cannot be read or verified by someone whois blind". Neither is the screen image of the ballot either, so what. With their logic all of society should be disabled equally for us all to be equal. So we all should be reduced to the least common denominator of ability so we cannot do something that everyone as a whole cannot do. Extremists like this do the disabled community a serious disservice.

Of more important concern as an issue is that several comments pointed out how the TSx does not meet the requirements of HAVA, i.e. curbside voting, insertion of the Smart Card, etc.

Federal Qualification

The SRA, p. 9 Item 6 refers to the "system" having successfully completed federal qualification testing. **It claims that GEMS 1.18.22 meets the 2002 VSS. There is no evidence that it does.** The Qualification Number itself is based upon 1990 VSS. The report refers to some components not yet qualified to 2002 VSS but does not identify them. **This system also appears to be in violation of both NASED rules and HAVA and state law. All systems tested and issued a qualifying number in 2005 are required to be qualified in total to 2002 VSS.** In fact, the NASED April, 2005 Addendum states: *"After January 1, 2005, any revisions which do not make the voting system totally compliant with the 2002 VSS become non-qualified under the national testing program"* (emphasis added). I am unsure how the state and NASED is bypassing both the requirements of HAVA, NASED's own advisories, and California law.

Security considerations

On the bottom of p. 8 of the SRA is the section about the system being secure from fraud or manipulation. The only changes appear to deal with the Supervisor and Administrator cards. Even those changes are not complete as reported by by the SRA and the SFES. Look at the previous staf report that was issued earlier, and the Steve Freeman original report on the security. They use the same language as on p. 9 of the SRA: "In all other aspects, the system is at least as secure as the previously certified Diebold systems."

That does not comfort me. We know that the previous Diebold systems are not secure, as evidenced by the Compuware Report, etc. The election's staff seems to think that the important aspect to a voter verified ballot is "public confidence" that our vote is"accurately recorded" (p. 10 Item 10). No, it is that our vote is accurately recorded and then accurately counted and reported. An effective manual audit of the computerized tabulating system is the only way that public confidence can be increased that our votes are accurately recorded and counted.

Important paragraph that needs further clarification and analysis: SRA p. 20, Item V. The staff appears to have inserted this paragraph in an effort to be able to use the TSx machines that were illegally sold and delivered to San Joaquin/ San Diego/ Kern County in 2003, prior to their being approved for use in California. They refer to a "non-AccuView configuration" that doesn't include the AVPAT.

First I would point out that neither in the federal qualification testing, nor in state testing, nor in the Application itself is there any reference to a "non-AccuView configuration." This paragraph appears to be a disingenuous way of getting the illegal TSx machines already in place to be used for the Special Election.

It is noteworthy that the Staff Report refers to the June 15, 2004 AVVPAT standards, NOT the January 21, 2005 Standards. The January 21, 2005 Standards "shall be effective beginning January 1, 2005 for all DRE voting systems certified on or after that date and beginning January 1, 2006, for all DRE voting systems..." **They are trying to grandfather a voting system that has**

already been "de-certified" because it failed to meet the requirements of state law.

This Application from Diebold calls the TSx with the AccuView printer a NEW system. State law forbade the counties from purchasing or contracting for a voting system that was not state approved. They did both in the spring of 2003, long before the conditional certification. that certification was rescinded because Diebold lied to the state.

If this Application and voting system is certified for use in California it will be as a new system certified in 2005. That means it must be used as a whole, including the AccuView. **I would challenge the Elections Division to come up with any legal authority to grandfather in a previously de-certified system.**

THIS IS A MAJOR ISSUE. WE MAY SEE EFFORTS BY KERN, SAN JOAQUIN, AND SAN DIEGO COUNTIES TO USE THEIR TSx MACHINES FOR THE SPECIAL ELECTION IN NOVEMBER, WITHOUT A PAPER TRAIL.

I have read the Decertification Directive and can find no reference to the possibility of the TSx system conditionally approved on November 20, 2003 being given a "second chance." The burden is upon the Elections Division staff to cite any authority that under either AVVPAT Standards or the Decertification Directive that the TSx systems used in the March, 2004 election can be used during 2005 to conduct elections. In fact, a careful reading of the April 30, 2004 Decertification Directive states explicitly that the Diebold TSx system currently deployed may not be used.

This is completely opposite with what the staff has stated as justification for using the TSx without a printer the rest of this year.

1. It is why Diebold submitted this Application for the TSx with printer as a NEW voting system.

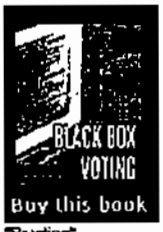
2. The Directive states that NO NEW VOTING SYSTEM may be used in California without a AVVPAT.

3. Number 4 specifically states that the TSx is not included.

4. The January, 2005 AVVPAT Standards REQUIRE that a new voting system MUST HAVE a AVVPAT for certification. That means that the existing TSx machines in San Joaquin, Kern, and San Diego Counties will not become automatically approved if the applied-for new system is certified. They must be identical to the new system to be approved for use.

As is apparent, there are serious deficiencies in the reports, as well as in the transparency of the entire certification process by the SoS. The elections officials from Kern, San Joaquin, and San Diego County will be at the meeting pleading their case once again, just like they did in October and November, 2003. At that time they chose expediency over the interests of their voters. They ignored state law and contracted for, and accepted delivery of voting systems before they were state approved. Now they will once again claim that the November Special Election means they have to have approval of their deficient systems now. We must fight that effort and expose their incompetence and abdication of their duty towards the citizens of their counties.

--Jody Holder



"Riveting"
— *Vanity Fair*
"The gospel of the movement"
— *Time Magazine*

black box voting
CONSUMER PROTECTION FOR ELECTIONS
www.BlackBoxVoting.Org

Open Letter to the Voting Systems and Procedures Panel **5/5/05**
Jim March, Member of the Board of Directors, BBV – 916-370-0347 / jmarch@prodigy.net

These comments are in advance of the next regularly scheduled VSPP hearing of 5/19/05.

The purpose of this memo is to urge the complete de-certification of Diebold Elections Systems Inc. products from the state, with the possible exception of using one optical scanner per precinct to do the HAVA-required "under/over vote scan" – but NOT to compile the vote electronically. Paper ballots must be completely hand-counted or an alternate open-source central paper ballot scanner can be developed on an emergency basis via the UC system.

We at Black Box Voting are aware that this is a radical step. But what we're about to prove to you is that the certification fraud and misconduct proven both by the Secretary of State's office between Nov. 03 and April '04 and in the March/Harris Qui Tam lawsuit and it's $2.6m fine against Diebold **HAVE NOT STOPPED** and are still an ongoing problem.

> ***Continuing the phase-in approach by upgrading InkaVote is the recommended alternative at this time for the following major reasons:***
>
> ***1. Electronic/touchscreen voting is embroiled in nationwide controversy. Growing negative public perception of DREs was reflected in the Field Poll of Nov. 1, 2004 that reported 35 percent of California's registered voters are not confident that electronic votes are recorded accurately.***
>
> ...
>
> ***Risks:***
>
> **** Complete paradigm shift for voters and pollworkers in a poisoned atmosphere.***
>
> Source: "NEXT STEP IN PHASED APPROACH TO NEW VOTING SYSTEM IMPLEMENTATION" - report to the Los Angeles County Board of Supervisors, April 19th 2005: http://lacounty.info/bos/sop/supdocs/17792.pdf
>
> ***In sum, Diebold:***
>
> ***1. marketed and sold the TSx system before it was fully functional, and before it was federally qualified;***
>
> ***2. misrepresented the status of the TSx system in federal testing in order to obtain state certification;***
>
> ***3. failed to obtain federal qualification of the TSx system despite assurances that it would;***

4. failed even to pursue testing of the firmware installed on its TSx machines in California until only weeks before the election, choosing instead to pursue testing of newer firmware that was even further behind in the ITA testing process and that, in some cases, required the use of other software that also was not approved in California;

5. installed uncertified software on election machines in 17 counties;

6. sought last-minute certification of allegedly essential hardware, software and firmware that had not completed federal testing; and

7. in doing so, jeopardized the conduct of the March Primary.

Source: "STAFF REPORT ON THE INVESTIGATION OF DIEBOLD ELECTION SYSTEMS, INC. dated April 20, 2004, produced by the California Secretary of State's office - and later suppressed by Shelley when all links to it and other info critical of Diebold were taken down.

The documents referenced above didn't come from the activist community. The first came from Los Angeles County and while they don't say it's Diebold that "poisoned the atmosphere", that county is a Diebold client and has been using Diebold touchscreens for early voting. Connie McCormack in LA is a long-time proponent of using Diebold and has been beta-testing a special GEMS variant – for anything this harsh to have come from that county indicates a crisis in public confidence that Shelley and company didn't adequately address.

The second was drafted near the conclusion of a period of intense scrutiny of Diebold that culminated in a two-day public hearing specifically related to Diebold, on April 21st and 22nd 2004.

At the hearing Diebold admitted that the older "TS" touchscreens as used by Alameda and Plumas counties were the same (software/firmware/functions) as the TSx newer smaller unit being installed in Kern, San Diego, Sonoma and San Joaquin – yet Diebold was punished by state certification removal for the TSx only.

Glossary:

- VSPP: the division of the California SecState's office that advises the SecState on voting machines.
- FEC: Federal Election Commission.
- FEC 1990/2002 Regulations: two standards for electronic voting. Anything new must meet the 2002 rules.
- FEC Certification: to get a voting machine Federally qualified, the vendor submits the machine to an FEC approved private testing lab ("ITA" for Independent Testing Authority). These are supposed to be acting as "watchdogs", reviewing program code and security issues. They have come under much criticism. FEC cert is required before California state certification can finish.
- "Global" – Global Elections Systems was an independent vendor of voting gear from the early '90s through 2002. Bought by Diebold, now known as Diebold Elections Systems, a subdivision with much independence.
- "GEMS" – "Global Election Management Software", the software now sold by Diebold to "tally" the vote at county elections headquarters – the "back room" piece of the voting system. The same software processes votes from absentee ballots, touchscreens ("TS" and "TSx") and precinct optical scanners. Windows program icon: a fist holding a globe. It is literally infamous for poor security, having been hacked by both Howard Dean and a chimpanzee (and no, not Bush, a real one!)
- Inkavote: small voting system used by LA County. Owned in part by Malaysian gambling interests and a former Prime Minister of Malaysia linked to human rights abuses. And it's STILL better than Diebold, if not by much...
- "RABA Report" – google that with "Diebold" – one of a number of professional criticisms of Diebold voting gear.

That wasn't the only reality ignored by Shelley's office in April '04.

David Jefferson caught Diebold executives and attorneys lying about the nature of various independent tests such as the RABA report. Former Diebold temp employee James Dunn testified under oath in a signed declaration that he was told by Diebold about defects in the PCM500 smart card encoder immediately following Diebold's testimony that the PCM500 flaws were a "surprise".

Diebold had already been caught installing uncertified software in every single California customer county circa Nov/Dec of 2003.

The promised continuation of the Diebold investigation post-April '04 never occurred despite clear indications to the panel on the 21st that the investigation hadn't gone far enough in one key area: figuring out whether or not software used and either customized or written by Diebold should have been subjected to ITA code scrutiny, notably Windows CE on the touchscreens, "VCProgrammer" and the Spyrus smartcard creation/read gear (hardware and esp. software). I

had submitted a set of questions to Mark Kyle on January 14th 2004 (see Appendix A, this document) and these were "re-processed" into an inadequate, "sketchy" version which Diebold sidestepped by "misreading" that can only be characterized as a form of verbal gymnastics (see also Appendix B, an excerpt from the official meeting transcript of April 21st '04). Not only were those questions misphrased by Shelley's staff, but no promised follow-up questions of a more professional or technically clear nature were ever issued.

Mark Kyle then committed a gross violation of open meetings laws across the summer and fall of '04. Multiple vendor certification hearings were scheduled without notification as to which vendors would be heard on which days. Activists who specialized in one system or another wouldn't know which hearings to show up at, incurring costs of a trip of hundreds or thousands of miles unnecessarily if they came at all. The public input which had badly damaged the relationship between industry and bureaucracy between January and April of '04 was crippled and no serious notice was taken within or without of the Secretary of State's office that the investigation which had clearly not finished with Diebold as of April 22nd '04 was never restarted.

What is happening now?

Diebold has claimed "certification" for several more products that they had previously described as "Commercial Off The Shelf" through April '04. According to an Oct. '04 NASED document obtained by Black Box Voting, these are "Windows CE OS", "Spyrus Vote Card Encoder 1.3.2" and "Key Card Tool 1.0.1" (an alternate form of smartcard creator) and "VCProgrammer 4.1.11". These are described as being certified under the FEC 2002 standards. See also:

http://www.bbvdocs.org/general/NASED-Qualified-Systems-Dec03-Oct04.xls

This raises several questions:

a) If these need to be certified NOW, how did the test labs (Wyle and Metamor/Cyber) previously miss the fact that they needed certification? They missed it because Diebold had lied to them previously as Bev Harris and myself have been complaining about since 2003.

b) The FEC 2002 standards refer to a "systematic" approach to overall security rather than certifying "bits and pieces". Yet Diebold has only submitted these "new" bits for certification rather than any "complete system package". The main pieces such as GEMS are still certified

only to 1990 standards (despite recent upgrades to v1.18.18 and above since the 2002 standards came out). Conclusion: the new "systematic" approach to security analysis under the FEC 2002 rules has NOT been performed.

c) But here's the most disturbing part: the items freshly submitted for Federal certification under the 2002 standards between April and October '04 all share one common denominator: ALL WERE ITEMS EXPOSED AND IDENTIFIED AS WRONGFULLY HELD BACK FROM FEDERAL CERTIFICATION BY BEV HARRIS AND MYSELF between Sept. 03' and early '04 in letters to the VSPP, letters to Alameda County officials, online articles, public speeches and our two lawsuits filed late '03 and early '04.

This is disturbing because I can assure the panel today that Harris and I have *never* had the ability to examine a complete California GEMS installation in detail. We've never seen directory listings for a California GEMS box, something I've been trying to get since July of '03 (and was denied by Brad Clark in Alameda).

So either Harris and I managed to stumble across EVERY single bit of uncertified Diebold code

in use from '02 to present or Diebold is only submitting for certification those limited portions of uncertified components that Harris and I caught them misrepresenting.

Here's another issue regarding improper handling of security. FEC standards from both 1990 and 2002 require individualized login to the central tabulator in order to identify after the fact which human being performed which operations. This is a "security basic" – without this, malicious actions can be performed with impunity knowing that even if the evil is detected, the perpetrator won't be. Without this, the "1% California hand recount" is a joke – most of the time a hack will be missed, even if not...so? *There's no risk!*

Diebold's GEMS product (<u>all versions</u>) don't meet this requirement.

There's a login process all right. But to should quote Sr. Engineer (Global/Diebold) Ken Clark:

```
To: <support@gesn.com>
Subject: RE: GEMS administration
From: "Ken Clark" <ken@gesn.com>
Date: Tue, 5 Sep 2000 15:17:35 -0500
Importance: Normal

In-reply-to: <NDBBJBKEHMHBEPDMLKOLAEPBCGAA.ljdglobal@gesn.com>

GEMS has normal users and admin users. Admin users are allowed to
change the election status (and thus remove the locks on the database),
normal users are not.

Looks good in an RFP response, but everyone just logs in as user admin
password global...

Ken
```

Although written in 2000, it's just as true today. In fact, Black Box Voting has now obtained hundreds of pages of GEMS audit logs from dozens of different counties and states, and all show clearly that every single person who logs in uses the same indistinguishable name: "admin."

The question is "why?"

Because in order to login to GEMS as a different human username, one has to **shut down** GEMS and start it back up again. On election day (and at least 12 hours after polls close) this is **impossible** – data is flowing into the central tabulator from precinct/terminal memory cards, large optical scanners for the absentee ballots, modems (if the county is still uninformed enough of the security problems involved to use them) and potentially numerous other data sources.

GEMS is too primitive a database to allow shutdown of the "front end" logged-in user interface while keeping the "back end" data collection process going. Any reasonably modern database can do this, allowing a different user to switch at the front while the data still flows in the back.

This is not theory. In late 2003 a candidate for mayor of the city of Memphis Tennessee (John Willingham, who was already equivalent to a California county supervisor) filed an election challenge and obtained a complete GEMS ".MDB file" as part of court discovery. This is the only "fully legal" GEMS database in outside circulation. A printout of the audit log runs 16 pages and is attached to this memo, covering events during election setup and the election itself (10/9/03). (Note: the last six lines of the audit log from April 24th 2005 record my

use of GEMS to print this log for this report; the audit log is otherwise exactly as provided in court discovery in late 2003.)

Every single line says "User: admin" at the start.

I repeat: As of the November 2004 election, Diebold had not changed this and a check with any California GEMS audit log will confirm it.

This is yet another example of Diebold flaunting FEC regulations which even under Shelley's management this agency **repeatedly** ordered Diebold to comply with. Diebold has not, remaining out of compliance with **both** FEC regulation sets and hence illegal in this state.

The VSPP has not even addressed the issue that three convicted felons and con artists founded Global (bought by Diebold in '02). No one here has even discussed convicted drug trafficker and Global/Diebold executive John Elder. The Shelley-era VSPP skipped over how Elder met embezzler Jeffrey Dean in jail and recruited him into Global Election Systems where he rose to a lead programming position on GEMS, the vote-tally system in use across California *and remained connected to Diebold Election Systems after the buyout.*

But there's more. Together, Jeffrey Dean and John Elder created yet ANOTHER voting system program and began trying to sell it in California, including San Diego and Los Angeles. This new system has never been certified, or even publicly discussed, yet it exists. Do we have to file another false claims suit over this? How many people do we have to sue to get California officials to take these repeating violations seriously?

If Diebold's "solution" is the answer, the question is just plain wrong.

Sonoma County paid $419,000 last year to Diebold just to make them go away. That was ridiculous and was the direct result of the VSPP's regulatory failure under Shelley's management – THEY should have been the one to make that decision. Instead Diebold's continuing unpunished crimes cost a county almost half a million dollars that they spent just to recover an appearance of a democratic process.

It is absolutely normal to require that vendors and workers in specific fields maintain a high degree of integrity. We make truckers take drug tests. We require criminal background checks at nuclear power plants. We ban felons from elected office, we bar conflicts of interest, we do all sorts of things to attempt to maintain honesty and sanity in government and industry regulation.

Allowing Diebold continued access to the electoral process despite their having "poisoned" it (as LA County put it) is intolerable and permanently undermines the mission of the Secretary of State's office by signaling that there is no consequences for misconduct.

The madness has to stop. Diebold was required to comply with all certification processes IN FULL back in April of '04 and they haven't. Just the fact that a few pieces of their system are certified to FEC 2002 (the bits they were caught cheating at) while the main components are to 1990 standards indicates that they haven't fully complied with the 2002 standards.

That's ALL the grounds needed to run them out of the state.

Right now most voters aren't paying attention to electronic voting, Diebold or all this "boring stuff".

New lawsuits will bring it to the citizens attention, once again. They will ask why Diebold wasn't dealt with the first time in a manner that mandated Diebold's compliance - or removal from California's voting process.

Do the panel members recall the founding political slogan of the US? The one used as justification for the break with England and our two wars with England?

No Taxation Without Representation

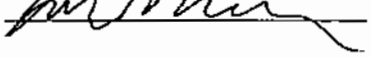
Is this panel and this agency ready to see Diebold's ongoing criminal behavior and California's tolerance of same *get turned into a historically authentic excuse for wide-scale tax protests*?

And we've got a budget crisis **now**?

We're not there yet and I hope we don't get there. But every indication says that's exactly where we're headed.

Enough chances. Enough "tolerance". Enough "compromises". Diebold is FINISHED in this state. Their credibility is in tatters by their own hand. The rest of the industry is ready to strangle them. At first there was mockery of their plight in various political and even mainstream cartoons but that's ended because it's **not funny any more**. The only question is "what are these repeat offenders doing anywhere near our votes!?" Shelley's administration provided no answers. *None are possible other than giving them a giant regulatory boot.*

It's our Democracy. Take it away from Diebold and give it BACK TO US.



Jim March

APPENDIX A: Submission to Mark Kyle, 1/14/04

The Main Questions Diebold Will One Day Face

Jim March – 1/14/04

These should be considered sample interrogatory questions.

1) Did Diebold or any of its subsidiaries and/or contractors modify Windows CE specifically for use on the TS/TSx hardware platforms?

2) If "yes" to #1, please describe these modifications.

3) What is Diebold's position on why Windows CE was not submitted for certification?

4) Did Diebold or any of it's subsidiaries and/or contractors modify the software that programs the "smart-card programmer device" that creates "smart cards" specifically for use on the TS/TSx hardware platforms?

4) Who writes and maintains "VCProgrammer", and what are its functions?

5) In addition to Spyrus, which other smartcard writer/reader systems can VCProgrammer control? Which models of Spyrus product has Diebold supplied to its customers?

6) How much memory is on the smartcards that the TS/TSx box can read? Please list the memory sizes of the normal smartcards Diebold provides its customers, and the largest memory capacities available on cards that can be read by the Spyrus or similar devices? (Note: we are aware of 128k cards.)

7) Why was VCProgrammer never submitted for certification, when it can write at least 128k worth of "data and program files" that can then be read into a TS/TSx box? (See also product specs at http://www.spyrus.com/)

8) Why do various versions of GEMS make attempts to establish an Internet session? Please describe the "Internet-aware" functions of GEMS. (Note: several investigators have noted a phenomenon wherein GEMS is loaded on a Windows NT/2000/XP computer which is attached to the Internet and a "personal software firewall application" is running such as ZoneAlarm. In such events, ZA is looking for unauthorized Internet transmissions from virii, worms, trojans, spyware and the like – and it reports communications sessions being started by GEMS. (Activists have called this the "ET Phone Home mystery".) It will take a test on a corporate-type Local Area Network (LAN) with hardware firewall set up to record transmissions from a GEMS PC with a fixed IP address to sort out, or possibly a packet sniffer on such a LAN. The appearance is that GEMS is trying to initiate a "conversation" with parties unknown, which in turn would defeat any hardware firewall on a county LAN and facilitate remote tampering with the GEMS database. It may be nothing, just GEMS looking for Touchscreens to do ballot download sessions on...but it does NOT happen due to user input of any sort, which in turn smells like week-old fish.)

9) Why does Diebold Election Systems (and Global prev.) write copies of the touchscreen "Ballotstation" application in a form compatible with Windows NT, in addition to WinCE?

APPENDIX B:
Excerpt From Transcript of April 21st '04 VSPP Hearing

Page 199

18 VICE CHAIRPERSON CARREL: I have one question.

19 May I?

20 MR. MARCH: Sure.

21 VICE CHAIRPERSON CARREL: The item that I
22 discussed with Mr. Urosevich and his attorney earlier
23 today regarding the PCM device and Windows CE was in our
24 list to Diebold, and was in there as a result of a request
25 that you made, we added that.

Page 200

1 And so I just wanted your clarification on what
2 you intended by that? Were you talking about smart card
3 encoders in the TSx itself or were you talking -- because
4 the word platform was used, did you include any other
5 peripheral?

6 MR. MARCH: Let's go over that. First of all, we
7 know from their testimony after that little debate that
8 the TSx is capable of all the same card burning functions
9 as a PCM 500. So one big question is are those separate
10 card burning functions built into the TSx, were they
11 certified or was only the vote tallying portion of the TSx
12 certified?

13 We know from the Bev Harris stash that there were
14 multiple versions of a program called VC Program, one of
15 several different applications that are used to program
16 smart cards.

17 VC Programmer is one. We know that there's
18 versions of it -- for every version they release, they do
19 it in two editions. One that's Windows NT compatible and
20 one that's Windows CE compatible.

21 So they can run that same voter card encoder on a
22 standard PC laptop running Windows NT XP2000 series, or
23 they can run it on any of their CE devices, which includes
24 the TS, TSx -- I assume it includes the TS. It definitely
25 includes TSx. It definitely includes the PCM 500.

Diebold Election Systems
Software Qualification Test Report
GEMS 1-18-15

Original Report Version 1.0 created 1/03/03

Prepared For:

The National Association of State Election Directors

Prepared By: CIBER ITA Division

CIBER, Inc.
Independent Test Authority

ciber

CIBER, Inc.
7501 South Memorial Parkway
Suite 107
Huntsville, AL 35802

Description	Pass	Fail	N/A	Comments
testing, audit trails, and documentation.				
The general features and capabilities of the access policy shall be specified by the vendor. Such generic capabilities might well include software access controls, hardware access controls, effective password management, the protection abilities of a particular operating system, and the general characteristics of supervisory access privileges.	√			
Access control measures shall be designed to permit access to system states in accordance with the access policy, and to prevent all other types of access. These measures may include: the use of data and user authorization, program unit ownership and other region boundaries, one- end or two-end port protection devices, security kernels, computer -generated password keys, special protocols, message encryption, and other controlled access security modems.	√			
Control methods shall be defined to preclude unauthorized access to the access control system itself.	√			
All software (including firmware) for all voting systems shall incorporate measures to prevent access by unauthorized persons, and to prevent unauthorized operations by any person. Unauthorized operations include, but are not limited to: modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.	√			Firmware not reviewed by software ITA.
The vendor shall provide a penetration analysis relevant to the operating status of the system, and its environment. This analysis shall cover the individual use of program units, the planned or inadvertent sharing of program units, and the resulting transitivity relationships. It shall identify all entry points and the methods of attack to which each is vulnerable. Such penetration analysis will be subject to strict confidentiality and non-disclosure by the test authority. For security reasons, the penetration analysis shall not be routinely distributed to the jurisdictions that program elections. The penetration analysis, however, will be part of the escrow deposit.			√	Penetration Analysis not reviewed by software ITA.
The integrity of the applications software and data must be preserved.	√			
Security procedures and logging records shall be used to control access to system functions.	√			

CIBER recommends to the NASED committee that GEMS Software Version 1-18-15 be certified and assigned NASED certification number N03060011815.

The New Diebold Printers

by John Gideon

Diebold Election Systems has begun showing its new voter verified paper record printer to election officials around the country. The new system is still not qualified by an Independent Testing Authority approved by the EAC.

This new system consists of a thermal printer that attaches to the **Diebold AccuVote TSX** touch-screen voting machine. The voter has the ability to look at a paper printout of the vote in the printer and verify that record before finalizing their vote; or so the company says. This add-on printer satisfies many states' voter verified paper trail requirement.

A closer examination of this device, as described in news articles, **shows that the paper record is actually on a 290 foot roll of thermal paper. The printing on the ballot is so small that when the voter looks at the record to verify it, they are looking through a magnifying piece of plastic.** Are these problems? Is there a better solution?

My first question was about the thermal paper. I wrote a reporter for the Akron Beacon Journal, Stephen Dyer, who wrote an article on this new printer. **I questioned the thermal paper and whether it would preserve the ballots for the 22 months that are required by federal law. His response back was, "It's on 15lb. paper** that's supposed to hold off longer than dot-matrix printing....." Being a bit skeptical I then called a large supplier of thermal paper products and asked if there was anything special about 15lb. Thermal paper. The sales person told me that all thermal paper is 15lb.

I then asked the sales person to tell me if she would feel comfortable storing federal records on thermal paper for any length of time. **Her response was that records on thermal paper can last 5 to 7 years.** That is hardly as long as records printed by a dot-matrix printer but longer than I suspected. **She then qualified her statement by telling me that everything depended on those records being kept away from light sources and heat during storage and a lack of handling.**

So, instead of paper ballots that can be stored anywhere secure we are now going to be asked to allow records of our ballots to be printed on thermal paper that must have special storage.

Also a problem with this new system is the fact that all records are printed, in the order that they were cast, on a single roll of paper. If anyone wanted to match ballots to voters who cast those ballots this system simplifies that task. The right to the secrecy of the vote is under attack when these machines are used.

Finally, many state's voter verified paper record laws state that the records must be human readable or readable by the voter without the use of another device. This would include the use of a magnifying glass. The fact that the printing on the paper record is so small that it requires a magnifying glass to read it is certainly problematic especially when you consider that those ballots must be read during audits and/or recounts.

Many states that are requiring the printing of a voter verified paper record or ballot, are doing so because they realize that there must be some means exterior of the machine's software to audit the machines. These paper records are to be that vehicle to an accurate audit. **The printing of these ballots on thermal paper, on a single roll, in print that is too small to be seen with the naked eye and in a non-machine readable format does not allow easy auditability. It seems that Diebold is throwing more obstructions into the way of auditing elections and doing less to ensure fair, transparent, auditable elections.**

Not wanting to throw up my hands and point out problems without having solutions, here is my solution. **Diebold has only to add a serial port to their voting machines to allow an off-the-shelf printer to be used for printing the paper records.** They can add some extra software that will enable the printer and direct the printer to print the record before the voter pushes the final "Vote" button.

Counties can then contract with a computer supply house to buy enough printers to equip their machines. **Those printers would be much cheaper than Diebold will be charging for their printer and they would use regular printer paper** that can be bought by the pallet from any paper supplier or from Costco. My solution is probably too easy; but why does this all have to be so hard?

ELECTIONS CODE SECTION 19250-19252

19250. (a) **On and after January 1, 2005, the Secretary of State may not approve a direct recording electronic voting system unless the system has received federal qualification and includes an accessible voter verified paper audit trail.**

(b) On and after January 1, 2006, a city or county **may not contract for or purchase a direct recording electronic voting system unless the system has received federal qualification and includes an accessible voter verified paper audit trail.**

(c) As of January 1, 2006, **all direct recording electronic voting systems in use on that date, regardless of when contracted for or purchased, shall have received federal qualification and include an accessible voter verified paper audit trail.** If the direct recording electronic voting system does not already include an accessible voter verified paper audit trail, the system shall be replaced or modified to include an accessible voter verified paper audit trail.

19251. For purposes of this article, the following terms shall have the following meanings:

(a) **"Accessible"** means that the information provided on the paper record copy from the voter verified paper audit trail mechanism is provided or conveyed to voters via both a visual and a nonvisual method, such as through an audio component.

(b) "Direct recording electronic voting system" means a voting system that records a vote electronically and does not require or permit the voter to record his or her vote directly onto a tangible ballot.

(c) "Voter verified paper audit trail" means a component of a direct recording electronic voting system that prints a contemporaneous paper record copy of each electronic ballot and allows each voter to confirm his or her selections before the voter casts his or her ballot.

(d) "Federal qualification" means the system has been certified, if applicable, by means of qualification testing by a Nationally Recognized Test Laboratory and has met or exceeded the minimum requirements set forth in the *Performance and Text Standards for Punch Card, Mark Sense, and Direct Recording Electronic Voting Systems*, or in any successor voluntary standard document, developed and promulgated by the Federal Election Commission, the Election Assistance Commission, or the National Institute of Standards and Technology.

(e) "Paper record copy" means an auditable document printed by a voter verified paper audit trail component that corresponds to the voter's electronic vote and lists the contests on the ballot and the voter's selections for those contests. **A paper record copy is not a ballot.**

19252. To the extent that they are available for expenditure for the purposes of this article, federal funds or moneys from the Voting Modernization Fund, created pursuant to subdivision (b) of Section 19234, shall be used. No moneys from the General Fund shall be expended for the purposes of this article.

SOLUTION: OPEN VOTING CONSORTIUM

More and more, citizens are expressing dissatisfaction with a voting system that is largely privatized and systematically excludes people from participating in the most basic process of any democracy. In short, the answer to closed voting is open voting.

As the San Jose Mercury News pointed out over a year ago, "The government unwisely ceded development of electronic voting machinery to private companies like Diebold Voting Systems, whose proprietary software is under electronic lock and key. The secrecy of the source code, a slew of malfunctions, and a lack of a paper copy that voters can look at have eroded confidence in touch-screen voting."[10]

Open Voting Consortium (OVC) seeks to **restore the ability of the people to be involved** in one of the most basic activities in any democracy: counting the votes. As Mike Himowitz of the Baltimore Sun put it, "Critics also complained that these systems use proprietary software from their vendors to tabulate and store votes -- code that's not available to the public. In essence, the most critical part of the election -- counting the votes -- had been snatched from public view and stashed away in a 'black box.'"

Traditional software companies hate **open-source software** because no one owns it or collects royalties for it. But the process works. The Linux operating system, now used on millions of servers around the world, is a premier example of open source software. Computer experts say Linux is **far more secure** than Microsoft Windows -- largely because friendly hackers have examined it closely and suggested improvements that help keep intruders out."[11]

OVC has developed prototypes of publicly programmed voting and vote-counting machines. The voting machines **print** the actual **paper ballot** that is used for counting. They also write a permanent record of the ballots to CD-ROM. This **prevents ballot box stuffing** and "lost" ballots. The prototypes demonstrate a design that will **protect the rights of the disabled** to vote without assistance, and support all scoring methods in use such as instant runoff voting.

OVC is seeking funding to turn these prototypes into tested, certified voting systems. These voting systems will be secure, reliable, and open to inspection. The **software** will be **free**, and the **hardware** will use **inexpensive**, off-the-shelf parts. See the Ballot Reconciliation Procedure Guide[12] for the step-by-step path taken by each vote from the voting booth through counting and archiving for potential re-counting. For further information, and to support clean elections, please visit **www.OpenVoting.org**.

Open Voting Consortium can **reduce costs** and **increase public confidence** in the voting system. Standardized, open, public software will attract many engineers in the open source community to assist in software development and testing. The open source development and maintenance model has proven successful with some of the most widely used programs on the Internet.

If you want to have the option of an open voting system available for counties in your state, let your Secretary of State and State Assembly know today. Help America Vote Act of 2002 (HAVA) funds should be available to support research and development of open voting systems. The Open Voting Consortium works with public universities to research and develop open voting systems. Why not have public money be made available for public universities to develop a public voting system for your state?

To arrange a FREE DEMO of the OVC voting system, please contact Lara Shaffer at 831-419-0758.

---

[10] http://www.kentucky.com/mld/mercurynews/news/opinion/8383100.htm
[11] http://www.dalelane.co.uk/cache/ovc_news4.htm
[12] http://www.openvotingconsortium.org/ad/brp-guide.pdf

NO DEAL WITH DIEBOLD!

PROBLEM: DIEBOLD IS AN IRRESPONSIBLE BUSINESS PARTNER

• From the office of California Secretary of State; *STAFF REPORT ON THE INVESTIGATION OF DIEBOLD ELECTIONS, INC*[1], April 20, 2004: "In sum, Diebold:

1. marketed and sold the TSx system **before it was fully functional**, and **before it was federally qualified**;
2. **misrepresented** the status of the TSx system **in federal testing** in order to obtain state certification;
3. **failed to obtain federal qualification** of the TSx system despite assurances that it would;
4. **failed even to pursue testing** of the firmware installed on its TSx machines in California until only weeks before the election, choosing instead to pursue testing of newer firmware that was even further behind in the ITA testing process and that, in some cases, required the use of other software that also was not approved in California;
5. **installed uncertified software** on election machines in 17 counties [including Humboldt[2]];
6. sought last-minute certification of allegedly essential hardware, software and firmware that had **not completed federal testing**; and
7. in doing so, jeopardized the conduct of the March Primary."[3]

PROBLEM: QUESTIONABLE PERSONNEL

• "I am **committed to helping Ohio deliver its electoral votes** to the president next year." - Wally O'Dell, CEO, Diebold, 2003 (The New York Times, 9 November 2003; "Machine Politics In the Digital Age"). The Diebold CEO also organized a $600,000 fund-raising party for the Mr. Cheney (Akron Beacon Journal, 1 July 2003).

• Jeffrey Dean has **23 convictions for computer-embezzlement**. In 2000 Dean became head of research and development at Global, and worked on the voting and tabulation machines. He also became a director of Global that same year. As Diebold was buying Global, Dean left the company, but Diebold hired him back as a consultant.[4]

• Diebold and rival Election Systems and Software are run by brothers Bob and Todd Urosevich, respectively. The two companies count approximately 80% of the votes in the U.S.[5]

PROBLEM: VOTER CONFIDENCE CANNOT BE ASSURED

• A mission-critical system that actually counts votes must be tamper-proof. Diebold's GEMS **vote tabulation** program is **wide open to election fraud.**

"Right now you can open GEMS' .mdb file with MS-Access, and alter its contents. That includes the audit log. ... Jane ... did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That's why we've never put a password on the file before."

— Ken Clark, Principle Engineer at Diebold, email, 18 Oct 2001[6 7]

The use of MS Access — well known as **not secure** — to count votes is appallingly **unprofessional** for a mission-critical product — lacking mandatory password protection is worse.

• In their study of 2002 Diebold computer source code, four computer security experts "conclude that this voting system is **unsuitable for use in a general election.**" They go on to say "Our analysis shows that this voting system is **far below even the most minimal security standards** applicable in other contexts."[8]

• Diebold machines have a long history of **miscounting votes.**[9]

In summary, Diebold wants our business. But it is not clear they care how they get it or what they will do once they get it. Diebold shows little regard for the integrity of the voting system and leaves no basis for confidence in the results they produce.

WHAT WOULD BE BETTER? – FLIP THE PAGE TO LEARN ABOUT OPEN VOTING CONSORTIUM

---

[1] Diebold bought Global Election Systems in January 31, 2002.
[2] http://www.ss.ca.gov/elections/ks_dre_papers/randgsummary.pdf
[3] http://www.ss.ca.gov/elections/ks_dre_papers/diebold_report_april20_final.pdf
[4] http://www.blackboxvoting.org/bbv_chapter-8.pdf, pg. 84
[5] http://www.ecotalk.org/UrosevichBrothers.htm
[6] http://www.equalccw.com/smokinggun.pdf
[7] http://www.scoop.co.nz/stories/HL0307/S00065.htm "Inside A U.S. Election Vote Counting Program"
[8] http://www.avirubin.com/vote.pdf "Analysis of an Electronic Voting System", T. Kohno et al
[9] http://www.votersunite.org/info/Dieboldinthenews.pdf

Voting Technology Costs and Considerations

http://www.verifiedvotingfoundation.org/article.php?list=type&type=77
see above-referenced webpage for live links to articles referenced in this article.

Most of the analyses of the costs of evoting systems have looked at the disparity in initial capital costs as compared to other types of voting systems, such as optical scan voting systems. Those initial capital costs are at least a factor of 2 or 3 higher than for precinct-count optical systems, depending on the average number of voting stations per polling place in a given jurisdiction.

Proponents of evoting systems argue that those initial higher capital costs will be recovered over time via reduced costs for printing paper ballots. However, the payback times (for paperless e-voting systems) are estimated at 15 to 20 years, which may well exceed the operational lifetime of such systems.

In states, such as California, which will require all e-voting systems to provide an voter-verified paper audit trail, the operating costs will be even higher, and the payback times even longer.

In addition, there are significant hidden costs associated with e-voting machines. For example, the process of conducting logic and accuracy tests (typically required before each election) are significantly more labor intensive than corresponding tests on optical ballot scanners.

The former require test votes to be entered by hand, while the latter can be tested by simply counting a standard test deck of optical scan ballots. **In addition, an e-voting solution requires a significantly higher number of total machines, since each polling place will require 4 to 8 machines, as opposed to a single optical scanner per polling place.**

The more machines you have, the higher the costs for storage, hardware maintenance contracts, software maintenance contracts, and replacement of parts (e.g., batteries). Once these costs are factored in, along with the costs of consumables for the voter-verified paper audit trail, the operating costs may exceed those of a precinct-count optical scan solution, even when factoring in the costs of the pre-printed optical scan ballots.

E-voting systems provide not only a less verifiable voting system than do optical scan paper ballot systems, they are also significantly less cost-effective. The accessibility features that evoting systems provide (e.g., enabling blind voters to vote in secret and with independence) can be provided just as well by ballot marking devices, which enable voters with disabilities to mark and verify standard optical scan ballots. **Thus, while adding voter-verified paper audit trail printers makes an evoting solution less bad than it otherwise would be, it really amounts to putting a band aid on what is a fundamentally flawed and expensive design.**

Here are some more resources related to voting technology costs:

Miami-Dade Elections: Paperless Voting Costs Soar
by Tere Figueras Negrete, The Miami Herald
May 26, 2005

Elections Chief Pares Massive Budget Request
by George Bennett, Palm Beach Post
May 14, 2005

Optical Vote Scan Machines Cheaper, More Accurate, Group Says
by Jarrett Carroll, Legislative Gazette
April 20, 2005

Voting Systems Serving 750 Voters

Five Direct Record Electronic Voting Machines

~ $17,500 without vvpb printers
~ $20,000 with vvpb printers

One Ballot Marking Device + One Precinct Scanner

~ $10,000

www.VotersUnite.Org