PLRC *Pacific Life Research Center*

631 Kiely Boulevard * Santa Clara, CA 95051 * Phone 408/248-1815 * Fax 408/985-9716 * E-mail bob@plrc.org

PLRC-040925 Last updated 25 September 2004

UNDERSTANDING THE "WAR ON TERRORISM":
MANIPULATING ELECTIONS
Part-2: America's High-Tech Voting Machines[1]

Compiled by Bob Aldridge

> *"The right of voting for representatives is the primary right by which all other rights are protected. To take away this right is to reduce a man to slavery ..."*
> *– Thomas Paine (1737-1809).*

On 29 October 2002, Congress passed the *Help America Vote Act of 2002* (HAVA). Ostensibly it corrects all the voting irregularities and glitches encountered in Florida during the November 2000 presidential election. To make these corrections, HAVA provides $3.9 billion to subsidize replacement of punch-card ballots and mechanical lever voting machines with high tech electronic equipment. In this paper I will discuss these new voting machines, who makes them, how they are certified, the deficiencies they are experiencing, and how they are used to swing elections.

In presenting the deficiencies, I will be borrowing from the works of several of this nation's leading voting machine experts and their analyses. These people are not objecting for the sake of being different, or for personal gain. They are critics because they understand the limitations and risks of computerized voting. They hold high academic positions as computer scientists, they have consulted to companies and provided investigations for states. They have consulted to congress and testified before committees. As far as I can determine, these critical experts are in favor of electronic voting. After all, that is their field and profession. But they do deplore the rush to buy these machines – rushing before federal funding disappears – when the machines are not adequately secure against voting mishaps and election fraud. To facilitate my references to these experts, I have listed them and their credentials in Appendix-A.

Let me now start this discussion by looking at who makes these new touch-screen voting machines, also referred to as Direct Reading Electronic (DRE) voting machines.

[1] This paper is part of a series on understanding why we are fighting terrorism. There is nothing new in it that hasn't been published elsewhere, and of course the coverage is not comprehensive. The purpose of this paper is to compile some pertinent information together so that a pattern can be seen. BA

VOTING MACHINE MANUFACTURERS

Four companies have most of the voting machine market cornered. They are:

- Diebold Election Systems. (North Canton, Ohio). Diebold Inc., the parent company, bought Global Election Systems in September 2001 and renamed it Diebold Election Systems. Global Election Systems had earlier bought I-Mark Systems in 1997. Diebold manufactures the **AccuVote-TS** DRE. Diebold is also one of the leading manufacturers of Automatic Teller Machines (ATMs) for banks.

- Sequoia Pacific Voting Systems Inc. (Exeter, California). Parent company is Smurfit Packaging Corporation (St. Louis, Missouri); which in turn is owned by Jefferson Smurfit Group plc. (Dublin, Ireland). Sequoia reached an agreement on 4 August 2003 to incorporate the VoteHere company's technology into its **AVC Edge** machine.

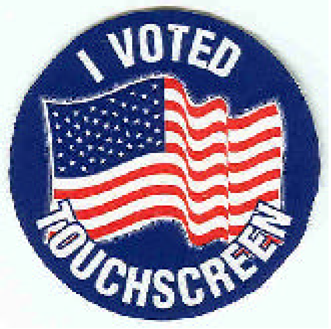
- Election Systems And Software Inc. (ES&S) (Omaha, Nebraska) was formed in 1997 by the merger of American Information Systems Inc and Business Records Corp. It is a subsidiary of McCarthy Group, Inc., which in turn is jointly held by a holding firm and the Omaha World Herald Co. (Publisher of Nebraska's largest newspaper). ES&S manufactures the **iVotronic** DRE

- Hart InterCivic Inc. (Austin, Texas) Hart manufactures the **eSlate 3000** DRE)

The first three are often referred to as The Big Three. Two smaller manufacturers often mentioned are Advanced Voting Solutions Inc. (Frisco, Texas) and Unilect Corp. (Dublin, California).

The four largest firms, or at least their owners and main executives, are heavy donors to the republican campaigns. It has been widely publicized that Diebold's chief executive, Walden O'Dell of Ohio, wrote a political fund-raising letter in 2003 to republican supporters saying he was "committed to helping Ohio deliver its electoral votes to the president next year."[2] Personal opinions do not necessarily reflect those of the company, and individuals can't be expected to not have sone strong feelings. However, "From 2000 to 2002, [Diebold] gave $200,965 to the republican party and none to the democratic party."[3] After the Enron example, and many others, it is not unnatural to be suspicious of how the Bush administration is providing billions of dollars for these voting machine companies with virtually no oversight, and how those companies are using it.

What compounds the issue is the veil of secrecy that enshrouds the voting machines and how they operate. This issue will be discussed in greater detail below, but if there were more transparency the political persuasion of the executives would not be such a big issue. If citizens were assured that their votes would be counted correctly, that rigged elections were absolutely impossible with the voting systems we use, and that democracy is not being hijacked by corporate interests, nobody would care which political parties the business executives donated to.



[2] Quoted in Gumbel, 14 October 2003, and many others of the printed media.

[3] Polman, 5 May 2004,

As it is, the “proprietary software” that goes into touch-screen voting systems is a highly guarded trade secret. How the votes are tabulated and counted inside these machines is absolutely opaque. This major departure from past, meticulous methods of verifying the vote counting and observing the process is alarming. Stanford University computer science professor, Dr. David Dill, commented on this lack of transparency in today’s electronic voting system: “Suppose you had a situation where ballots were handed to a private company that counted them behind a closed door and burned the results. Nobody but an idiot would accept a system like that. We’ve got something that is almost as bad with electronic voting.”[4]

Every election seems to reveal some hints of deceptive programming for electronic voting. Dr. Rebecca Mercuri commented on early voting in Dallas during the November 2002 election. Voters pushed the democrat button and invariably the republican candidate’s name appeared on the screen. Eighteen machines were eventually shut down because of “misalignment” problems. “And those were the ones where you could visually spot a problem,” Mercuri said: “What about what you don’t see? Just because your vote shows up on the screen for the democrats, how do you know it is registering inside the machine for the democrats?”[5]

It is hard to believe that such crooked tactics could take place. Dr. Mercuri told a US House of Representatives sub-committee: “Although (in many states) convicted felons and foreign citizens are prohibited from voting in US elections, there are no such laws regarding voting machine manufacturers, programmers, and administrative personnel. Felons and foreigners can (and do!) work at and even own some of the voting machine companies providing equipment to US municipalities.”[6] All of the Big Three are represented in scandals that have made the news recently:

- Phil Foster, Sequoia vice president of sales for southern region was indicted in Louisiana in January 2001. He was charged with two counts of conspiracy to commit money laundering and kickbacks on sales of voting machines, and one count of conspiracy to commit malfeasance in office. Charges were dismissed in April 2002 in exchange for grand jury testimony, with immunity, against others involved, including the Louisiana’s state commissioner of elections.
- In 2002, the Arkansas secretary of state pleaded guilty to 1995 bribes and kickbacks from a voting machine company that was a forerunner to ES&S. Another person involved testified against him under condition of immunity. That person is now a vice-president of ES&S.
- John L. Elder, head of Diebold’s ballot-printing business in Everett, Washington, was convicted and imprisoned during the 1990s for selling cocaine. Elder has had a clean record since that time and undoubtedly deserves the position he holds. It is ironic, nevertheless, that ex-felons are purged from the voter roster in some states while another ex-felon designs the ballot they cannot use.

It is understandable that an ex-addict and drug seller who has reformed should be given another chance. After all, the purpose of our criminal justice system is supposed to be to rehabilitate offenders. However, it is another matter when people with a past history of bribery, money laundering, and malfeasance hold

[4] Poovey, 23 August 2004.

[5] Quoted in Gumbel, 14 October 2003.

[6] Mercuri, 22 May 2001.

decision-making positions in the mechanism that insures democracy. It is not only natural, but also prudent, to be suspicious.

A cogent example took place in the 1990s when Chuck Hagel was chief executive of American Information Systems (now known as ES&S) which made e-voting machines. In 1996 Hagel decided to run for the US Senate. He won and was the first republican senator elected from Nebraska in 24 years. A Nebraska Election Administration official estimates that 85% of Hagel's wining votes in 1996 and 2000 were counted on machines from the company he runs.[7]

Then we come to more conflicts of interest after the machines are manufactured. They must then be tested and certified.

COMPANIES THAT TEST AND CERTIFY VOTING MACHINES

Three so-called Independent Testing Companies (ITAs) certify voting machines to federal standards. It is up to the states to certify them for individual state requirements. Most states simply rely on federal standards while others have done some investigation on their own. I will discuss some of the latter later on.

The three federal Independent Testing Authorities are:

- CIBER Inc. (Greenwood Village, Colorado), tests voting machine software.[8]
- SysTest Labs (Denver, Colorado), tests voting machine software.
- Wyle Laboratories Inc. (El Segundo, California), tests voting machine hardware.

There is doubt about how independent these testing authorities really are. They work under contract from a vendor to certify the voting machine the vendor manufactures. As far as the certification is concerned, Dr. David Dill explains: "These Test Authorities use the word 'Certified' as if it were some magical holy blessing. It's been 'Certified.' What does that mean? We didn't get any answers."[9]

Dill continued that a friend of his "got the right passwords to call up Wyle [Laboratories] and ask them what they do, and he got a description. The basic description, ... is that they bake the machines to see if they die. They drop them to see if they break. And then what they do is run scripts over the computer program to check for bugs. A script is just another computer program to check for superficial things. ... It is basically nothing more than a style-checker, like running a spell-check."[10]

[7] Cited in Disinfopedia, "ES&S".

[8] "According to Federal Election System records, CIBER donated $48,000 to republicans during the last four years ... The company made no donations to democrats." (Ackerman, 30 May 2004.)

[9] Quoted in Pitt, 20 October 2003.

[10] Quoted in Pitt, 20 October 2003.

Forty two of the 50 states rely on these three "independent" testing labs for state certification. But when California Secretary of State Kevin Shelley asked Wyle Laboratories about the testing results, he was told the information was proprietary and could be discussed only with the manufacturer. "And so the secretary of state was introduced to the looking-glass world of voter-machine regulation. Over the years, repeated references to 'federal testing' by election officials have given the impression that the government oversees the certification of touch-screen voting systems. While there are guidelines for the machines, no federal agency has legal authority to enforce them."[11]

I will return to the problems with testing standards under a separate heading below. Right now I will move on to discuss this secrecy business in more detail.

LACK OF A VOTER-VERIFIED PAPER TRAIL

The Help America Vote Act of 2002 (HAVA) specifies: "The voting system shall produce a permanent paper record with a manual audit capacity," and that the "paper record produced ... shall be available as an official record for any recount conducted with respect to any election in which the system is used."[12] Compliance with having a paper record is not mandated until 1 January 2006.[13] It is important to note that this paper "record" has apparently been interpreted by the voting machine manufacturers as nothing more than a hard-copy printout of what is on the computer. This paper record is nothing more than a backup in case the computer disk crashes or disappears. It is not the same as a *voter-verified* paper trail.[14]

A voter-verified paper trail is a paper printout of the ballot which the voter can verify through a glass screen at the time of voting (but he cannot touch it) before he or she make their vote final. If changes are required they can be made. The faulty printed ballot is sent to a scrap container and not counted. A new one becomes visible behind the screen. When the voter is satisfied with the paper ballot being viewed, the vote is cast and the paper copy goes directly into the ballot box. This paper trail then becomes a permanent record which will be available in case a manual recount or audit is required.

On 21 November 2003, California secretary of state, Kevin Shelley, mandated that by 2006 all voting machines in the state will have a voter-verified paper trail – a paper ballot printed and verified by the voter at the time the vote is cast. It is expected that California's action will have a chain effect in other states. Kevin Shelley now has ethical problems related to how he, or his staff, distributed the federal funds to

[11] Ackerman, 30 May 2004.

[12] HAVA, Section 301(a)(2)(B)(i and iii).

[13] HAVA, Section 301(d).

[14] The term *voter-verified* denotes a paper printout of the ballot which the voter can verify through a window before he makes his vote final. The term *paper trail* means that printout will become a permanent record which will be available in case a manual recount or audit is required.

improve voting.[15] This could be a political move to discredit him and, by association, his initiative. But it is hoped that his pioneering of the voter-verified paper trail will remain in place.

It appears that only Nevada will have a voter-verified paper trail during the November 2004 presidential election. It will use Sequoia touch-screen machines in all its precincts and is the only state that has demanded a paper trail. So perhaps Nevada will have a safe election. Nevada's primary election is reported to have gone smoothly.

Even after January 2006, when paper trails will be used in many states across the country, electronic voting machines can still be rigged. Dr. Rebecca Mercuri told Congress in 2001 that "Fully electronic systems do not provide any way that the voter (or election officials) can truly verify that the ballot cast corresponds to that being recorded. Any programmer can write code that displays one thing, records something else, and prints yet another result. There is no way to insure that this is not happening inside a voting system."

A voter-verified paper trail, however, is somewhat more secure. It is true that the machine may record something different than what is shown on the screen or the printout the voter can view behind a glass, but the accurate vote would be there on paper in case of a recount. A voter-verified paper trail can be audited.

Dr. Michael I. Shamos is in favor of electronic voting while at the same time a critic of present circumstances. He, also, believes people are naive in believing that a paper trail will insure a correct vote count. After the Florida presidential election fiasco in 2000, Congress jumped to electronic voting machines, particularly the ATM-type touch-screen machines, to prevent such a debacle in the future. The Help America vote Act was passed in 2002 and provided $3.9 billion in funds. Such a lush potential for profit caused a flurry of activity with scant consideration for the public. The product was rushed to market by taking advantage of every legal loophole available. Shamos believes the entire process "of designing, implementing, manufacturing, certifying, selling, acquiring, storing, selling, using, testing, and even discarding voting machines must be transparent from cradle to grave, and must adhere to strict performance and security guidelines that should be uniform for federal elections throughout the United States."[16]

Although it is not the answer to all the problems associated with voting machine security, a *voter-verified paper trail* is essential. In January 2004, a special election was held for a seat in the legislature covering Palm Beach and Broward Counties in Florida. The winner had a scant 12-vote lead out of 10,844 cast. A recount required by state law for a margin of win under 0.25% was triggered. There was also a suspicious inconsistency of 134 less votes cast as voters who signed in at the polls. But there was no paper trail so it was not possible to comply with the law or verify to the voters that their votes were counted.

It has also been suggested that mandatory surprise audit recounts in 0.5% of all jurisdictions, both domestic and overseas, be conducted to make certain the voting machines are working correctly and to discourage voter fraud.[17]

[15] In what appears to be a political dispute, Secretary of State Kevin Shelley has been accused of awarding no-bid contracts to democratic allies. Until the state auditor completes an investigation of Shelley's spending, Governor Schwarzenegger has frozen $45 million in federal funds. Voting rights groups and county election officials exerted enough pressure to free $15 million, but as of this writing another $30 million is still frozen. This has stalled, among other things, the printing of millions of easy-to-understand voters guides and voter educational projects for soldiers in Iraq. There is still pressure on the governor to release the remaining funds to insure informed voters in the November 2004 election.

[16] Shamos, 24 June 2004.

[17] See Holt, 25 May 2003.

Paper records were considered mandatory for the electronic voting machines used in the August 2004 recall election in Venezuela. After the election, which didn't turn out the way Washington desired because President Hugo Chavez avoided being recalled by a wide margin, the opposition claimed that computerized voting machines skewed the count in Chavez's favor. There were some possible irregularities apparent during the audit, but they seemed to go both ways and fell within the range of mathematical probability. International observers who monitored the audit concluded that the opposition's fraud allegation was baseless. Contested elections which can be effectively audited will reach a credible conclusion.

Legislation has been introduced in Congress to mandate a voter-verified paper trail. representative Rush Holt and 149 others introduced H.R.2239 in the House to amend the Help America Vote Act of 2002 to require a voter verified permanent record under Title III of the Act. It was referred to the House Committee on House Administration on 22 May 2003. A companion bill, S.1980, was introduced in the Senate by Senator Bob Graham and five co-sponsors. It was refered to the Senate Committee on Rules and Administration on 9 December 2003.

These bills will, of course, expire with the 108th Congress at the end of 2004, and if not enacted before then will have to be re-introduced in 2005.

SOFTWARE SECRECY

The software designed for electronic voting machines is considered by the manufacturer to be proprietary information, and is therefore kept in closest secrecy. Critics maintain that since billions of dollars of tax money is being used to buy these machines, the public should know what they are getting. After all, they contend, these machines and their software are not just vending machines or ATMs at the bank. These machines comprise "the integrity of the election process [which] is fundamental to the integrity of democracy itself."[18]

Voting machine manufacturers argue that the source code, which is the core of the software program, is always certified by an Independent Testing Authority (ITA). Joe Richardson, a spokesman for Diebold, seemed to echo the voting-machine manufacturers' sentiments when he stated that "we don't feel it is necessary to turn it over to everyone who asks to see it, because it is proprietary."[19]

Apparently Diebold does release some software code for review to who they describe as "respectable, unbiased third-party experts." They have done so for reviews in Ohio and Maryland, providing the third party signs a non-disclosure agreement. The statement on their website reads: "Diebold Election Systems has and will continue to open up its system for review by respectable, unbiased, third-party experts such as those evaluations conducted in Maryland and Ohio. We are confident in the integrity and security of our system, and that the electronic voting format holds the greatest potential for ensuring impartial, secure and accurate elections."[20]

[18] IEEE Report, and Wallach, 27 February 2004.

[19] Quoted in Schwartz, 24 July 2003.

[20] Available at http://www.diebold.com/dieboldes/ohio.htm

That may be so, but how can one be sure that what they received is actually the software in the machines they sell. It is once again a case of having to trust them. Dr. Mercuri was part of a lawsuit in Palm Beach County, Florida, where plaintiffs wanted to inspect a suspicious Sequoia machine. They were stonewalled with the trade-secret-agreement argument. "It makes it really hard to show their product has been tampered with," she said, "if it's a felony to inspect it." Mercuri went on to say: "There are literally hundreds of ways to do this ... hundreds of ways to embed a rogue series of commands into the code and nobody would ever know because the nature of programming is so complex. The numbers would all tally perfectly."[21] Journalist Andrew Gumbel adds: "Tampering with an election could be something as simple as a 'denial of service' attack in which the machines simply stop working for an extended period, deterring voters faced with the prospect of long lines. Or it could be done with evasive computer codes known in the trade by such names as 'Trojan Horses'[22] or 'Easter Eggs.'[23] Detecting one of those, Dr. Mercuri says, would be almost impossible unless the investigator knew in advance it was there and how to trigger it."[24]

Despite all these obstacles in examining voting machine software, some studies have been made and have yielded frightening results.

GEORGIA – A PIONEER OF TOUCH-SCREEN MACHINES

Irregardless of all this secrecy, the software for one of the manufacturers, Diebold's AccuVote-TS touch-screen machine, became known. As I have pieced the story together from various media reports and professional studies, it all started in Georgia during the November 2002 mid-term election. At that time Georgia had 22,000 Diebold touch-screen machines – more than any other state. But these machines were not equipped to provide a paper trail. In two closely-watched races – Sonny Purdue for governor and Saxby Chambliss for US Senator – opinion polls had the democratic candidates ahead by between 9-11 and 2-5 percentage points respectively. But when the votes were counted, a major last-minute swing gave the election to the republican candidates – a swing of up to 16 and 12 percentage points respectively for the two races.[25] For the highly-finessed opinion polls to miss by that wide a margin was unprecedented. It was particularly suspicious since the machines "had been 'patched' at the last minute following a major software breakdown."[26] With no paper trail, however, this vote could not be contested.

[21] Quotations from Gumbel, 14 October 2003.

[22] A Trojan Horse is a malicious program that will lie dormant until something triggers it, such as a certain date and time.

[23] I have been informed that if you search the web for "Easter Eggs" with Google.com, you will get a list of websites that reveal Easter Eggs in Microsoft programs. I've tried it. It works.

[24] Gumbel, 14 October 2003.

[25] Colorado, Minnesota, Illinois, and New Hampshire also experienced these large, unexpected, last-minute vote swings to provide winners for the republican party.

[26] Gumbel, 29 October 2003.

Some Georgia citizens decided to look into the matter. One wrote to the Georgia secretary of state's office asking for a copy of the state certification letter. He was told that none existed in that office and was refered to the Georgia Technology Authority. That office replied that it was "not sure what you mean by the words 'please provide written certification documents'."[27] As stated by one of the concerned citizens, Atlanta graphic designer Dennis Wright: "If the machines were not certified, then right there the election was illegal."[28]

That is not the end of the breakdown. Journalist Andrew Gumbel reported in London's *Independent*: "Shortly after the election, a Diebold technician called Rob Behler came forward and reported that when the machines were about to be shipped to Georgia polling stations in the summer of 2002, they performed so erratically that their software had to be amended with a last-minute 'patch.' Instead of being transmitted via disk – a potentially time-consuming process, especially since the author was in Canada, not Georgia – the patch was posted, along with the entire election software package, on an open-access FTP, or file transfer protocol, site on the Internet."[29] That, alone, was a massive security breach because it opened the software to tampering. But it gave the concerned Georgia citizens an opportunity to evaluate the secret source code.

Roxanne Jekot Analysis.

Roxanne Jekot examined the code from the Internet line by line. "There were security holes all over it," she said, "from the most basic display of the ballot on the screen all the way through the operating system."[30] She pointed out that the program was designed for the Windows 2000NT operating system but she found that it also worked satisfactorily on the much less secure Windows 98.[31] Jekot was also amazed at how shoddy the code was. She expected to have difficulty reading it but soon learned that a lot of it could just as well have been written by her first-year students.

Diebold tried to mitigate the finding of their computer software on the Internet by claiming it was an obsolete version and that many parts have been revised. Because of trade secrecy we would have to trust them to believe them, which most critics don't. "It was documented throughout the code who changed what and when. We have the history of this program from 1996 to 2002," says Jekot. "I have no doubt this is the software used in the [2002] elections."[32]

Hopkins Report / IEEE Report .

Still another study of the source code for Diebold's AccuVote-TS touch-screen machine was conducted after being found on the company's Internet site, during January of 2003. Computer science researchers

[27] Quoted in Gumbel, 14 October 2003.

[28] Quoted in Gumbel, 14 October 2003.

[29] Gumbel, 14 October 2003.

[30] Quoted in Gumbel, 14 October 2003.

[31] Other sources reveal that the AccuVote software was originally designed for Windows 95 but was later changed to Windows CE.

[32] Quoted in Gumbel, 14 October 2003.

Dr. Aviel D. Rubin (Johns Hopkins University in Baltimore, Maryland), and Dr. Dan S. Wallach (Rice University in Houston, Texas), along with two computer science doctoral students,[33] performed a meticulous study of the software. They reported their findings in a paper which was first published by Johns Hopkins University on 23 July 2003 (Technical Report TR-2003-19 – often called the Hopkins Report). Later it was published in the journal for the Institute of Electrical and Electronics Engineers (IEEE) on 27 February 2004.[34]

Topping the list of security flaws in the Hopkins Report is the ability of an outsider to fabricate counterfeit voter cards, or smartcards[35], which will allow voting an unlimited number of times. Here's how the voting process works. After checking at the poll, the voter is given a smartcard to activate the machine. The smartcard is inserted similar to inserting the ATM card in an automatic teller machine. This brings up the ballot and the voter touches the candidates of his choice on the screen. When the selection is finished, the voter reviews the marked ballot, makes any changes necessary, and then touches the spot to cast the ballot. The smartcard is then ejected. After that, the machine won't accept that smartcard again until it has been reprogrammed by a poll worker for the next voter.

Diebold's voter cards do exploit the advantage of smartcards over normal magnetic strip cards – the ability to perform cryptographic operations. The lack of cryptography allows an attacker to make his own homebrew smartcards which will allow him to vote over and over and over again. One of several ways to get the information necessary to make homebrew smartcards is to have an accomplice vote. Then, instead of turning in the smartcard received from the poll worker, he turns in some sort of fake card. The attacker can then use reverse engineering to get the code from the stolen smartcard, alter it to allow multiple votes, and stuff the digital ballot box.

If the attacker were a poll worker, or had a poll worker accomplice, the process would be simpler still. The end result would be an overvote (more ballots counted than people who registered to vote) but it would not be possible to tell legitimate votes from the frauds. And, with no paper trail at present, there would be no way for a meaningful audit, or a manual recount.

There are also two other cards of the same type but with slightly different programming. They are the administrator card and the ender card. The first gives the holder access to additional administrative controls of the Diebold technology, and both cards can end the election – that is, shut down the machine. In a precinct which is heavily partisan toward one candidate, a group of attackers could simultaneously shut down all the machines during a peak period to stop the election until poll workers could get the stations set up again. This denial-of-service attack would likely deter many people from voting because they couldn't wait, and thus reduce the votes for one candidate. In this type of attack there would be no overvotes because the voters had not yet checked in.

[33] The doctoral students are Tadayoshi Kohno (University of California at San Diego, La Jolla, California) and Adam Stubblefield (Johns Hopkins University, Baltimore, Maryland).

[34] See IEEE Report, 27 February 2004.

[35] The voter card or smartcard is a plastic memory card similar to an ATM card. But, rather than having a magnetic strip like an ATM card, it has an imbedded digital chip which can store data and perform cryptographic operations.

There were other techniques described in the Hopkins Report to alter the vote count by insiders (all attacks except the last item listed can be done by poll workers) which I will itemize but not describe. They are arcane in nature and anyone interested in pursuing them further can refer to the IEEE Report which is listed in the References. The other techniques of vote manipulation on Diebold machines by insiders are:

- Modify system configuration.
- Modify ballot definition.
- Cause votes to be miscounted by tampering with configuration.
- Impersonate legitimate voting machine to tallying authority.
- Create, delete, or modify votes.
- Link voters with their votes.
- Tamper with audit logs.
- Delay the start of an election (denial-of-vote attack).
- Insert backdoors into code. This can be done only by the Operating System developer or the voting machine developer.

When the Hopkins Report first came out, Dr. Douglas W. Jones (University of Ohio) remarked that "this paper makes it quite clear that the errors I had pointed out to representatives of Global Election Systems [now Diebold Election Systems] when they first came to Iowa with the AccuTouch [now AccuVote] system have not been corrected in code that was available on Diebold's [Internet] server half a decade later."[36] Jones told Global Elections Systems people of these flaw in November 1997, shortly after they had acquired I-Mark Systems. The dates of the software examined by the Hopkins group was over the years 2000-2002 – three to five years later.

Dan Wallach, one of the Hopkins Report's co-authors, said he has similar concerns about the non-encryption of Hart-InterCivic machines, but that company won't release its software without a non-disclosure agreement. That would prevent any publication of problems found.[37]

The IEEE Report did state that since the earlier version of this report appeared on the Internet (the Hopkins Report), Diebold has apparently made some corrections. The details have not been made public. The IEEE Report summarizes: "We found significant security flaws; voters can trivially cast multiple ballots with no built-in traceability, administrative functions can be performed by regular voters, and the threats posed by insiders such as poll workers, software developers, and janitors is even greater. Based on our analysis of the development environment, including change logs and comments, we believe that an appropriate level of programming discipline for a project such as this has not been maintained. In fact, there appears to have been little quality control in the process."[38]

Then the report concludes: "The model where individual vendors write proprietary code to run our elections appears to be unreliable, and if we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate. We owe it to ourselves and to our future to have robust, well-designed election systems to preserve the bedrock of our democracy."[39]

[36] Jones,"The Case of the Diebold FTP Site."

[37] Cited in Messmer, 25 July 2003.

[38] IEEE Report, 27 February 2004.

[39] IEEE Report, 27 February 2004.

A major criticism of the Hopkins Report was that it looked at the software in isolation and did not consider physical security at the election site which might mitigate the security flaws. The report's authors admitted this in the report. One was the possibility that if the touch-screen machine were connected to a modem that a hacker could interact with it. Even if the AccuVote-TS is never connected to a modem during voting hours, the voting results are transmitted via something called a PCMCIA card which can be read and modified by a pocket-size computer.

Diebold claimed that the software analyzed by the Hopkins group was an older version and that many of the security flaws had been corrected. Future studies, however, will illustrate that those security flaws were still present after the Hopkins Report was released.

MARYLAND – ANOTHER EARLY BUYER OF TOUCH-SCREENS

Maryland was another early recipient of many Diebold touch-screen machines. Computer experts in that state also examined the Diebold code found on the Internet. They found 328 software flaws, 26 of them critical, putting the whole system "at high risk of compromise. ... If these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results," their report states.[40]

SAIC Report.

After the Hopkins Report was released, the State of Maryland hired Science Applications International Corporation (SAIC) of San Diego, California, to run a risk assessment study of the Diebold AccuVote - TS machine. One of the principle tasks was to evaluate the Hopkins Report. In its executive summary, the SAIC Report states: "In general, SAIC made many of the same observations, *when considering only the source code."*[41] (emphasis theirs.) The SAIC Report goes on the say that Maryland's procedural controls and general voting environment mitigate or eliminate many of the vulnerabilities. (Apparently some still remain.) But, SAIC says, this mitigation does not "in many cases meet the standard of best practice or the State of Maryland Security Policy."[42]

SAIC points out that current security controls depend on the voting system being disconnected from any network communications. If were connected to a phone line, the risk rating would immediately soar. The report acknowledged that the touch-screen voting terminals themselves aren't, but the Global Election Management System (GEMS) server[43] is connected to the to the State Board of Elections intranet, which has access to the Internet. After pointing out that the GEMS server contains Microsoft Office products

[40] Quoted in Gumbel, 14 October 2003.

[41] SAIC Report, Executive Summary.

[42] SAIC Report, Executive Summary.

[43] The Global Election Management System (GEMS) is a Diebold software program that runs on Microsoft Windows (WinEDS). It allows election management to control ballot layout and election tabulation, counting, and reporting. It covers all election ballots: touch-screen, optical scanner, and absentee. The word "Global" in the name is a hangover from Diebold's predecessor – Global Election Systems.

not required by the voting system, the remainder of that paragraph as well as the following paragraph is "Redacted." When the discussion resumes again, the report recommends testing for time-triggered exploits (e.g., Trojans). Perhaps the "redacted" material discussed how hostile attacks could be or have been made to plant certain delayed actions. The report then urged immediately removing the GEMS server from the intranet.[44]

The Executive Summary of the SAIC Report concludes: "The System, as implemented in policy, procedure, and technology, is at high risk of compromise. Application of the listed mitigations will reduce the risk to the system. Any computerized voting system implemented using the present set of policies and procedures would require these same mitigations."[45]

The SAIC Report. while agreeing with the technical security flaws described in the Hopkins Report, was analyzing a current version of the Diebold Source Code. Although the version is "redacted" in the body of the report, it is given in Appendix D as 4.3.1.5. This indicates that the security risks identified by the Hopkins team still existed in code being used in September 2003.

From the tone of the SAIC Report I got the impression it was somewhat defensive of the Hopkins Report. It made me wonder, since Maryland had already invested in 16,000 Diebold touch-screen machines, if the report were commissioned to justify its decision. That suspicion is raised further when dates are compared. The SAIC Report is dated 2 September 2003 but the Sate of Maryland didn't release it to the public until September 24th. When it was finally released there were a significant number of blank pages and paragraphs where information had been "redacted." Later reports by studies in another state, however, would give more details on voting machine vulnerabilities.

RABA Report.

On 10 November 2003, the State of Maryland commissioned RABA Technologies to evaluate Maryland's plan to use touch-screen voting. Part of the task was to review the Hopkins Report, the SAIC Report, and to examine Maryland's Information Technology Security Certification and Accreditation Guidelines. Then, on 19 January 2004, RABA computer security experts performed a Red Team exercise to simulate an attack that would stress and test the actual computer voting system to be used in the March primaries.

The key findings were summarized: "The State of Maryland Election System (comprising technical, operational, and procedural components), as configured at the time of this report, contains considerable security risks that can cause moderate to severe disruption in an election."[46] Then the report indicated there were near-time mitigating recommendations for each vulnerability and that if, and only if, all of those mitigating recommendations were in place the machines would be worthy of trust for the March 2004 primary election. But, RABA strongly felt, between the March primary and the November general election additional actions must be taken. And, ultimately, paper receipts in some fashion will be needed.

The RABA Report also verified that the Hopkins team were analyzing a current version of the computer code. RABA signed a non-disclosure agreement with Diebold to obtain the current version. After

[44] See SAIC Report, Section 2.2.2

[45] SAIC Report, Executive Summary.

[46] RABA Report, p. 3.

reviewing the Hopkins Report, RABA said the "single most relevant finding ... is that the general lack of security awareness, as reflected in the Diebold Code, is a valid and troubling revelation," and continued: "We generally agree with the Hopkins Report on purely technical matters."[47] By agreeing with the Hopkins study, RABA tacitly disclosed that the Hopkins team was looking at a present-day, currently-in-use software code.

OHIO STEPS BACK FROM TOUCH SCREENS.

Of Ohio's 88 counties, 68 still use the punch-card system. Ohio set a goal to replace all punch-card machines with touch-screens by the March 2004 primary election. Dr. Douglas Jones of the Iowa Board of Examiners said: "On reading the Hopkins paper, I immediately called for the decertification of Diebold's direct recording electronic voting machines. I believe this is entirely justified by the magnitude of the security flaws identified in that paper, and completely independently, I believe it is justified by the fact that Diebold's predecessor, Global Election Systems, knew about that one flaw and did nothing to correct it over half a decade."[48]

InfoSENTRY Report.

On 15 August 2003, Ohio Secretary of State J. Kenneth Blackwell commissioned two studies on voting machines. The studies were to include the products of all four manufacturers. These studies by InfoSENTRY Services, Inc. (Raleigh, North Carolina) and Compuware Corporation (Detroit, Michigan) were completed on 21 November 2003. On 2 December 2003, Blackwell released Volume 1 only of the InfoSENTRY Report.[49]

Dr. Douglas Jones, a member of the Iowa Board of Examiners for Voting Machines and Electronic Voting Equipment, did not seem too impressed with Volume 1 – the only one publicly available. He capsulized that it "says very little about the voting systems, while focusing on issues of certification and security planning."[50] He did point out that the report did reveal large weaknesses in state security procedure which need to be corrected.

Compuware Report.

The Compuware Report was also dated 21 November 2003 and released to the public by Secretary Blackwell on 2 December 2003. A total of 57 security vulnerabilities which might be exploited during an election were identified in the systems from the four manufacturers. Those risks were categorized as high, medium, and low. Those pertaining to each manufacturer are:

- Diebold had 5 high, 2 medium, and 8 low.
- ES&S had 1 high, 3 medium, and 13 low.
- Hart InterCivic had 4 high, 1 medium, and 5 low.
- Sequoia had 3 high, 5 medium, and 7 low.

[47] RABA Report, p. 7.

[48] Jones,"The Case of the Diebold FTP Site."

[49] The other volumes not released to the public covered the Ohio Secretary of State Office (Vol. 2), Diebold (Vol. 3), ES&S (Vol. 4), Hart InterCivic (Vol. 5), and Sequoia (Vol. 6).

[50] Jones,"The Case of the Diebold FTP Site."

Compuware says if these security issues are left unmitigated they "would provide an opportunity for an attacker to disrupt the election process or throw the election results into question."[51] One amazing weakness identified by Compuware was the supervisor smart card PIN[52] for Diebold's AccuVote-TS machine. It is a four-digit number and what appears on every smart card issued by Diebold is the factory default – "1111." It cannot be changed.

Two days after the Compuware Report was released, George Geczy, a partner in DG Technical Consulting and co-chair of Hamilton Chamber Science & Technology Committee, sent an e-mail to the Elections Office of the Ohio Secretary of State. In pointing out one mistake in the Compuware Report, he said: "In their audit they declared the infrared interface used in systems such as the iVotronic to be secure as it is proprietary and 'will not connect to normal Windows, Linux, or Mac machine.' However, it is in fact very easy to reverse-engineer infrared communication. A device as simple as a 'Palm Pilot' handheld computer can receive and transmit most custom infrared signals, and so the use of an infrared interface does NOT preclude hacking and unauthorized access through this method." Geczy went on to explain that, in particular, if the data were not encrypted it would be very simple to reverse-engineer, and that: "Given the Compuware Report's comments on the lack of encryption and security in other elements of the system ... hacking an iVotronic could be as simple as walking into the voting booth using a correctly programmed Palm Pilot ... to simulate a supervisory [personal electronic ballot] access device."[53]

State of Ohio Action.

On 2 December 2003, when Ohio Secretary of State Blackwell released the InfoSENTRY and Compuware reports, he also issued a press release halting all touch-screen machine purchases and ordering all manufacturers to remedy the flaws identified. The state's schedule originally called for touch-screen machines to be installed in time for the March 2004 primary election. That milestone was now delayed until the November 2004 general election. The press release also said the state would petition the federal government for an extension of the HAVA deadline for purchasing electronic voting machines in order to allow time for the manufacturer to correct deficiencies.

After a second audit round by Compuware which was completed in July 2004, it was determined that Diebold[54] had still not corrected all the security flaws discovered in the first audit. On 16 July 2004, Secretary Blackwell issued a press release saying the Diebold machines would not be used for the 2004 election. The press release stated: "The decision is based on preliminary findings from the secretary of state's second round of security testing conducted by Compuware Corporation showing the existence of previously identified and yet unresolved security issues."[55] In the press release Blackwell reiterated: "As

[51] Compuware Report, p. 20.

[52] PIN stands for Personal Identification Number. It is the code or password to access a machine or program.

[53] Geczy, 4 December 2003.

[54] The State of Ohio had contracted with Diebold to install touch-screen voting machines. This seems natural because Diebold is an Ohio-based corporation.

[55] Ohio Press Release, 16 July 2004.

I made clear last year, I will not place these voting machines before Ohio's voters until identified risks are corrected."[56] This decision may also have been prompted by legislation requiring all voting machines in the state to have a voter-verified paper trail by 2006. Ohio Governor Bob Taft signed that bill the previous May 2004. It was also prudent to forestall buying the machines until they were paper-trail equipped.

CALIFORNIA SUES DIEBOLD

In a discussion concerning how a state can be sure that the software tested is the same as that in the machine being used, Dr. David Dill commented that it "is actually a much harder technical problem than most people would think. With current hardware, it is very difficult to make sure that the program running on the machine is the program we think is running on the machine. There is a general theme of secrecy that is frustrating to me. ... claims are made about these systems, how they are designed, how they work, that frankly I don't believe. In some cases ... because the claims they are making are impossible. I am limited in my ability to refute these impossible claims because all the data is hidden behind a veil of secrecy."[57]

Gubernatorial Recall Election, 7 October 2003.

After the California's 7 October 2003 gubernatorial recall election, it was discovered Diebold may have installed some uncertified software. This may have been why in Alameda County "Votes for Lt. Gov. Cruz Bustamante [a democrat] were being given to a lesser-known candidate ..."[58] Of course that gave republican Arnold Schwarzenegger a greater lead over Bustamante, reminiscent of Florida's butterfly ballot fiasco.[59] (This will be discussed later.) On October 30th, California's assistant secretary of state, Marc Carrel, announced a halt on certifying machines from Diebold.

Then in a local election on 4 November 2003 in Alameda county, it was discovered that 4,000 Diebold machines were using software that hadn't been certified by the state. Following right on the heels of the Hopkins Report, this created an air of distrust which prompted California Secretary of State Kevin Shelley on November 12th to order a month-long audit of all Diebold touch-screen machines in the state. The audit would look for uncertified hardware or software patches that would violate state election laws.

In the following month, December, the auditors reported that the 17 counties which had purchased Diebold machines had been using software not certified by the state.[60] Moreover, in three of those counties – Los Angeles, Trinity, and Lassen Counties – the software wasn't even certified by the federal government.

[56] Quoted in Ohio Press Release, 16 July 2004..

[57] Quoted in Pitt, 20 October 2003.

[58] Mahler (San Joaquin News Service).

[59] Elaine Ginnold, Alameda County's assistant registrar of voters, claims it was human error that caused the miscount of votes. [Cited in Mahler (San Joaquin News Service)]

[60] Florida, also, had uncertified voting software. On 3 February 2004, Florida's chief of the Voting System Certification Bureau told the Florida Senate Committee on Ethics and Elections that half of counties in the state are using some form of uncertified software. (See Jones, "The Case of the Diebold FTP Site.")

How did this uncertified software get on California machines? Votewatcher Jim March posted an e-mail, dated 14 January 2002, from Diebold executive Ken Clark – an e-mail that was reported leaked by a whistleblower. One paragraph throws some light on the company's cavalier manipulation of software. After discussing how to avoid a major version number change in touch-screen software by calling it a fix, Clark goes on: "Strictly adhering to our release policies, the California change should also require a major version number bump to GEMS (because of the protocol change). We can't reasonably expect all of California to upgrade to [GEMS] 1.18 this late in the game though, so we'll slip the change into GEMS 1.17.21 and declare this is a bug rather than a new feature. What good are rules unless you can bend them now and again."[61]

On November 21st, shortly after the audit started, California Secretary of State Shelly announced that by 2006 all voting machines in the state must have a voter-verified paper trail. Then on 20 January 2004 the RABA Report was concluded for the state of Maryland. This indicated that electronic voting machines could be hacked, passwords broken, and the vote count altered. This information coming on the heels of the Hopkins Report (now the IEEE Report) and the discovery of uncertified software in California prompted Shelley to further action. First, he called on Diebold to turn over its software code to a team of independent experts chosen by him to examine it. Second, he ordered security steps for the March primary election which were recommended in the RABA Report, including disconnection electronic voting machines from the Internet and installing Microsoft security patches.[62]

County election officials, however, were slow to react to new security precautions. "Only one county registrar of 14 who responded to inquiries said she planned to implement specific steps recommended by the computer scientists to correct serious security flaws."[63] Only three counties said they had read the RABA report. The registrar of Los Angeles County – the state's largest – even said Diebold had assured her that the software code tested by RABA Technologies was an older version.[64] The registrar of Alameda County said she believed "the new software is going to have the security recommendations."[65]

But Michael Wertheimer, author of the RABA Report and formerly a senior technical director for the National Security Agency, disagreed: "I can honestly say the problems we are describing will not be addressed in any immediate update."[66] Regarding the tendency to depend on manufacturers and neglecting the warnings from computer scientists, California Voter Foundation president Kim Alexander pointed out

[61] Quoted in March, 23 September 2003.

[62] The RABA Report described how the Red Team had altered voting cards to cast multiple votes, modified ballots and altered election results by plugging a keyboard into the touch screen, picked a security code in a matter of seconds, and gain control of the vote-counting computer with malicious software. The RABA team also discovered Diebold had not installed 15 Microsoft security patches for the Windows system that runs Diebold's software. (See Ackerman, 6 February 2004.)

[63] Ackerman, 6 February 2004.

[64] Cited in Ackerman, 6 February 2004.

[65] Quoted in Ackerman, 6 February 2004.

[66] Quoted in Ackerman, 6 February 2004.

that the “vendors who are in the business of profiting off the sale of voting systems do not have a vested interest in being forthcoming about security glitches.”[67]

There were actually ten counties which challenged Shelley’s constitutional authority to order safeguards that would assure safe elections. They accused him of undermining public confidence in voting systems. In a countermove, four other counties filed suit in Sacramento County Superior Court to mandate implementation of the security fixes for Diebold systems. This plea was dismissed by the judge, “saying there is no evidence that California’s upcoming elections are in danger of being manipulated.”[68]

California’s March 2004 Primary Election.

California’s 2004 primary election on March 2nd, where more than 40% of the state’s voters used touchscreens, raised new concerns. Problems arose in many of the 14 counties which used them. San Diego, Alameda, and Orange Counties perhaps experienced the worst. In San Diego County, about 36% of the county’s 1,611 polling places failed to open on time because of a technical problem. It was 11:00 AM before all were up and running. Some 18% of Alameda County’s 1,096 polling places experienced a similar problem. Both counties used Diebold machines which booted up unfamiliar screens when voting cards were inserted.

On April 21st Secretary Shelley released a report accusing Diebold of jeopardizing California’s primary election with inadequately tested equipment, saying “Diebold’s conduct has created an untenable situation for both county and state election officials.”[69] The problem in San Diego and Alameda Counties seemed to be malfunction of hundreds of voter-card encoders which match voters to the appropriate ballot. “Less than two months before last year’s election, Diebold urged the emergency approval of the encoders, claiming the election could not be conducted without them. However, the company then failed to alert election officials about a battery problem that affected the encoders’ operation.”[70] The result was that thousands of voters were disenfranchised by being turned away.

A few comparisons: Per the 2000 census, San Diego County is 33.5% minority.[71] If the 36% of precincts where people were turned away coincided with the areas where minorities are predominant, that would have a significant effect of skewing the election results toward republicans in the November general election. Likewise in Alameda County, where 405,554 democratic ballots were cast in the 2002 primary, compared to 64,707 republican.[72] Disenfranchising voters in the November 2004 general election would greatly benefit the republican party.

[67] Quoted in Ackerman, 6 February 2004.

[68] Nissenbaum, 19 February 2004.

[69] Quoted in Ackerman, 22 April 2004.

[70] Ackerman, 22 April 2004.

[71] San Diego County Quick Facts From The US Census Bureau.

[72] Alameda County Election Summary Report.

Orange County uses machines made by Hart InterCivic which do not have a screen. Nevertheless, the new system confused poll workers who gave more than 7,000 voters the wrong electronic ballot. Voters were prevented from voting for candidates in their own district but could vote for another district. In the end, 21 precincts had more votes cast than there were registered voters. This affected five congressional races, four state senate races, and five assembly races.[73]

Two state senators – Ross Johnson (R-Irvine)[74] and Don Perata (D-Oakland)[75] were upset by the primary election problems. They called on Secretary of State Shelley to decertify all paperless voting machines before the November general election, threatening legislative action if he didn't. Johnson said: "Democracy is too important to turn over completely to a machine, much less a machine that is a lemon."[76] He continued: "Our democracy works because people accept the results of elections. If you put that into question, it attacks the very foundation of a democratic society."[77]

In 16 March 2004, Shelley laid down the guidelines for all California touch-screen machines to have a voter-verified paper trail by July 2006 – in time for the November general election that year. Senators Johnson and Perata sponsored Senate Bill 1438 to codify Shelly's administrative order. SB 1438, however, went a step farther and requires a voter-verified paper trail by the next statewide election (after 2004), which is the 2006 primary.

The State Assembly passed SB 1438 with a unanimous 73-0 vote on 26 August 2004 and the State Senate passed it with a unanimous 31-0 vote on August 27th. The legislation was sent to Governor Schwarzenegger 3 September 2004. He has 30 days to act on it (either sign or veto) or it will become law without his signature.

The Uncertified AccuVote TSx.

On 22 April 2004, a state advisory panel discovered that an uncertified new Diebold model, the AccuVote-TSx, had been sold to San Diego, San Joaquin, Solano, and Kern Counties. The panel – made up of seven top aides to Shelley and David Jefferson, a computer scientist for Lawrence Livermore National Laboratories – unanimously recommended decertifying more than 14,000 AccuVote-TSx machines in those four counties. California officials claim they had given conditional certification of these machines for the March primary because Diebold had assured them federal approval was imminent. But that was not the case. A report the panel released a day earlier, April 21st, "found Diebold had jeopardized the March primary by selling an untested and poorly functioning system, and by misleading state officials

[73] Cited in Zetter, 11 March 2004.

[74] California State Senator Ross Johnson is vice-chairman of the Senate Elections And Reapportionment Committee.

[75] California State Senator Don Perata is chairman of the Senate Elections And Reapportionment Committee.

[76] Quoted in Fletcher, 12 March 2004.

[77] Quoted in Nissenbaum, 20 February 2004.

about federal approval of the system."[78] The advisory panel also recommended that Shelley investigate criminal and civil charges against Diebold because of the company's conduct.

The newer model Diebold AccuVote- TSx apparently uses a wireless means of transmitting data from the touch-screen machine to the GEMS server. Diebold says this is only for preliminary results and the actual voting results are hand carried on PCMCIA[79] flash cards. Further investigation disclosed that the electronic hookup between the voting machine and GEMS server is made before the vote totals are computed. According to Dr. Douglas Jones: "This means that the flash cards holding the official results for each precinct are exposed to corruption by any network insecurity, and therefore, that the official canvass can be corrupted if someone hacks into the machine. Furthermore, it is emerging that the version of Windows CE used by Diebold is both heavily customized and full of dynamically loaded libraries. As a result there are strong grounds for the conclusion that the operating system is not unmodified commercial off-the-shelf software (COTS), and that with this extensive use of dynamic linkage, we cannot even tell if the system being run on a particular voting machine resembles the system that was disclosed in the configuration documents submitted with the system when it went through the [federal] approval process."[80] What that means is the Diebold AccuVote - TSx machines sold to California not only have a previously undisclosed security flaw, but are also uncertified.

Finally, on 30 April 2004, Secretary of State Shelley decertified all touch-screen machines in the state, sating: "We will not tolerate deceitful tactics as engaged in by Diebold and we must send a clear and compelling message to the rest of the industry ..." Shelley then laid out 23 security measures for touch-screen machines to be used in the November 2004 election, and said if they are met he would re-certify the machines on a county-by-county basis. These security measures include being disconnected from any network, providing paper ballots for those who prefer not to use the touch-screens, providing the source code for any system to the secretary of state upon demand, and posting the vote count from each touch-screen at the polling place.

Ten counties which use other makes of machines had the best hopes of being re-certified. When Sequoia Voting Systems made their source code available the re-certification began. Some counties have balked, and even filed court cases challenging Shelley's authority. But California's secretary of state has constitutional powers to make such decisions.

Shelley also asked California Attorney General Bill Lockyer "to investigate allegations of fraud, saying Diebold had lied to state officials."[81] On 7 September 2004 Lockyer decided to take over a false-claims lawsuit against Diebold which had been filed the previous November by whistleblowers. Lockyer joined

[78] Ackerman, 23 April 2004.

[79] Personal computer Memory Card International Association (PCMCIA) is a non-profit trade association which defines technical standards and educated the public regarding flash cards, miniature cards, and smart cards used for storing and transmitting data.

[80] Jones,"The Case of the Diebold FTP Site."

[81] Associated Press, 30 April 2004.

the lawsuit after his investigation found “sufficient evidence of them defrauding the state.”[82] But the attorney general closed a criminal investigation against Diebold. Alameda County also joined the false-claims lawsuit. The lawsuit seeks reimbursement for Diebold voting machines purchased in the state.

THE SEQUOIA SOFTWARE LEAK

Sequoia Pacific Voting Systems was the second of the Big Three to have its software leaked publicly on an unprotected Internet site. Riverside County in California uses Sequoia AVC Edge touch-screen voting machines. Jaguar Computer Systems provides election support for that county and it was on their FTP server that the software was discovered in October 2003. Unlike the Diebold software that was leaked, which was a rawer source code with programmers’ notes and comments, the Sequoia code was the cleaner binary as it is used in the voting machines. Binary code can be reverse engineered to find out how it works but takes about four times longer to do so.

Although Sequoia had disparaged Diebold for using the Windows operating system which is well understood by computer hackers, as opposed to Sequoia’s purported proprietary system designed especially for electronic voting, this leaked code showed that Sequoia also used the Windows system. The AVC Edge machine uses WinEDS (Election Database System for Windows) which runs on top of the regular Microsoft Windows operating system.[83] In the WinEDS folder is some off-the-shelf software called MDAC[84] that doesn’t require the certification and audit mandated for proprietary e-voting software.

In the usual type of disclaimer, Sequoia spokesman Alfie Charles said the software that had been found “was an older version that had been substantially modified.”[85] Charles continued: “While this breach of security is grossly negligent on the part of the county’s contractor, the code that was retrieved is used to accumulate unofficial results on election night and does not compromise the integrity of the official electronic ballots themselves.”[86]

Dr. Peter Neumann of Stanford Research Institute does not agree: “This means that anyone could install a Trojan Horse in the MDAC that won’t show up in the source code.”[87] A Trojan Horse is a malicious program that will lie dormant until something triggers it – such as a certain time and date or a certain number of votes cast. Then it is activated to alter the program, or rig the election. *Wired News* explains: “Jaguar employees, Sequoia employees, or state election officials could insert code that wouldn’t be detectable in

[82] Quoted in Folmar, 8 September 2004.

[83] Cited in Zetter, 29 October 2003.

[84] According to *Wired News*, this software is Microsoft Data Access Components (MDAC), which is used to send information between a database and a program. Version 2.1 was on the website. Microsoft has issued a patch designated version 2.8 to correct security flaws in the earlier version 2.1. (See Zetter, 29 October 2003.)

[85] Schwartz, 3 November 2003.

[86] Quoted in Zetter, 29 October 2003.

[87] Quoted in Zetter, 29 October 2003.

a certification review of the code or in security testing of the system."[88] Neumann then pointed to the necessity for a voter-verified paper trail: "The idea of looking at source code to find problems is inherently unsatisfactory. You need to use a machine with accountability and an audit trail."[89]

Dr. Rebecca Mercuri is also skeptical about the security problems arising from the software of two companies being unprotected: "Are these companies staffed by folks completely ignorant of computer security, or are they just blatantly flaunting that they can breach every possible rule of protocol and sell voting machines everywhere with impunity?"[90]

Dr. Aviel Rubin adds: "This argument that everything needs to be kept secret is not viable because stuff does get out whether companies intend it or not. Now two out of the three top companies have leaked their system. Scientists are being made afraid to look at these things, which in the end will be bad for our society. Why shouldn't everyone want scientists to look? If there's any feeling that there may actually be danger to our elections, how can we not be encouraging researchers to look at our systems?"[91]

Others seem to support the argument that secrecy leads to vote rigging and fraud. Attorney Cindy Cohn at Electric Frontier Foundation says: "Our society and our democracy is better served by open voting systems. The way to create a more secure system is to open the source code and to have as many people as possible try to break into the system and figure out all the holes. The clearest way to have an insecure system is to lock it up and show it to only a few people."[92]

THE LACK OF VOTING MACHINE STANDARDS

The original source code audit by a federally certified laboratory for one of the touch-screen voting machines described above indicated that "the software of this voting system was the best the examiners had ever seen and that they were particularly impressed by its security."[93] Five computer scientists who signed a letter to concerned citizens of Ohio asked "why would a federally certified testing laboratory declare a voting system to be secure while 5 other reviews of that same system found major flaws? ... This calls into question the [federal] standards themselves as much as it calls into question the competence of the federally certified examiners."[94]

Administering HAVA, setting the standards, and overseeing disbursement of the money was to be the responsibility of a bipartisan Election Assistance Commission. Commissioners were to be appointed by the president, with the advice and consent of the senate, withing 120 days of enactment of the Act. That

[88] Zetter, 29 October 2003.

[89] Quoted in Zetter, 29 October 2003.

[90] Quoted in Schwartz, 3 November 2003.

[91] Quoted in Zetter, 29 October 2003.

[92] Quoted in Zetter, 29 October 2003.

[93] Jones, et al, 26 February 2004.

[94] Jones, et al, 26 February 2004.

would put the deadline around the first of March 2003. But, bureaucratic stonewalling delayed the Commission's start until March 2004. No oversight was in place before touch-screen voting machines started rolling off the production line. These high-tech DREs are now considered even more susceptible to vote manipulation and fraud than Florida's butterfly ballot.

Dr. Michael I Shamos told a subcommittee of the US House of Representatives Committee on Science in June 2004 that "the system we have for testing and certifying voting equipment in this country is not only broken, but is virtually nonexistent," and must be created from scratch to restore public confidence.[95]

A month later Shamos told Congress: "There is no systematic science of voting machine technology, no engineering journal devoted to the subject, no academic department, not even a comprehensive text book. There are no adequate standards for voting machines, nor any effective testing protocols. ... When a flaw is detected in a voting machine, there is no compulsory procedure for reporting it, studying it, repairing it, or even learning from experience. The voting machine industry is unregulated and it has not chosen to regulate itself."[96]

Shamos goes on to point out that the only set of standards applicable to electronic voting systems is the Federal Voting Systems Standards (FVSS) which places responsibility on the vendor to comply with no test procedures for doing so. These "are incomplete and out of date. For example, one of the principal election security worries is the possibility of a computer virus infecting the voting system. Yet the FVSS place virus responsibility on the voting system vendor and do not provide for any testing by the Independent Testing Authority (ITA). ... It is hardly reassuring to have the fox guarantee the safety of the chickens."[97]

HAVA assigns the National Institute of Standards and Technology (NIST) the main responsibility for overseeing development of voting machine standards.[98] Yet the Bush administration has tragically underfunded the grants authorized by the HAVA legislation.[99]

The only standards for secure computer systems certification that the NIST works with is The Computer Security Act of 1987. Pentagon computer systems are monitored and certified under this Act but it can't be used for voting machines. Congress has exempted itself from compliance. Therefore, as Dr. Mercuri pointed out, the accuracy and integrity has never been certified for any computer-based voting system used in federal elections.[100]

The burden falls upon an organization called the National Association of State Election Directors to appoint the Independent Testing Authorities (ITAs) that test the voting machines. Dr. Shamos says this process

[95] Shamos, 24 June 2004.

[96] Shamos, 20 July 2004.

[97] Shamos, 24 June 2004.

[98] See HAVA, Part 4 (Sections 271-273).

[99] See Shamos, 20 July 2004.

[100] Mercuri, 22 May 2001.

is dysfunctional and points out that the National Association of State Election Directors' website contains this peremptory statement: "The ITAs DO NOT and WILL NOT respond to outside inquiries about the testing process for voting systems, nor will they answer questions related to a specific manufacturer or a specific voting system. They have neither the staff nor the time to explain the process to the public, the news media, or jurisdictions."[101] Shamos says the ITA procedures are entirely opaque and finds it "grotesque that an organization charged with such a heavy responsibility feels no obligation to explain to anyone what it is doing."[102]

While discussing the Hopkins Report, Dr. Douglas Jones agrees that "the biggest issue raised by the Hopkins paper deals not with Diebold but with the adequacy of the current [Federal] Voting Systems Standards. ... Under the 1990 standards, the source code auditors who read the code for the I-Mark Electronic Ballot Station [predecessor to Diebold's AccuVote] back in 1996 described it as the best voting system software they'd ever seen! ... despite the flaws the Hopkins group identified that must have been present then. This brings into question not only Diebold's code, but our entire current system of voting system certification."[103]

Five computer-scientists ended their open letter to concerned citizens of Ohio by stating: "In the long run, we must insist on voting systems that meet a standard of auditability comparable to the standards we apply to the financial world, ... We must insist on the same level of oversight for counting votes as we have routinely insisted on for counting dollars. ... With the technology available today, we see no way that such oversight can be provided without maintaining a voter-verified paper record of each vote cast."[104]

A voter-verified paper trail is probably the minimum requirement to insure security for touch-screen machines. Sensible voting machine security standards would contain more than that, including:

- A voter-verified paper trail for vote audits.
- No part of the voting system – touch screen, optical scanner, vote tabulator server, or whatever else may be used – allowed to be hooked up to the Internet or any other network, modem, or intranet connection.
- Absolutely no wireless transmission of voter data of any type, including infrared.
- Data stored on flash cards for transit must be encrypted ad escorted by bi-partisan observers.
- Adequate number and types of passwords with encryption where necessary.

IS THERE ANY EVIDENCE THAT LACK OF SECURITY HAS BEEN EXPLOITED?

Voting Machine companies manufacture a device which facilitates the guarantee of a democratic government by representation, a device that should by all accounts be the most secure in the land, yet

[101] Quoted in Shamos, 24 June 2004.

[102] Shamos, 24 June 2004.

[103] Jones, "The Case of the Diebold FTP Site."

[104] Jones, et al, 26 February 2004.

as I have illustrated above voting machines are anything but secure. For the November 2004 election, electronic voting machines – both touch-screen and optical scanning – will be under physical security measures which depend on the integrity of election officials and poll workers. It was illustrated in the 2000 presidential election that such integrity is not always forthcoming. It is naive to believe that vote fraud and rigged elections cannot happen in America. It pays to be aware of and alert to the possibility of rigged elections and how they can take place. Some very recent events justify such awareness and alertness.

Leaked Diebold E-Mails.

During the summer of 2003, a large archive (1.8 gigabytes) of Diebold internal e-mail was leaked by an insider to reporter Brian McWilliams of Wired News. This was apparently motivated by the Hopkins Report and the archive covered the period up to 2 March 2003. One exchange between Ken Clark, of Diebold, and Nel Finberg, also of Diebold, was particularly revealing. The full text of this exchange is posted on the website for the School of Information Management & Systems (SIMS) of the University of California, Berkeley.[105] I will summarize it here.

On 16 October 2001, Nel Finberg of Diebold wrote an internal e-mail to Ken Clark stating that Jennifer Price of the Independent Testing Authority (ITA) Metamor (later CIBER) said she could access the GEMS database and alter the audit log without a password. Then Finberg asked: "What is the position of our development staff on this? Can we justify this? Or should this be anathema?"[106]

Clark replied on October 18th that it is easy to open the GEMS database with Microsoft Access, just double-click on it. Then you can change its contents. He points out that a password could be added but that wouldn't mean much because someone has to know the password. Then Clark adds that "the audit log is modifiable by that person at least (read, me). Back to perception though, if you don't bring this up you might skate through Metamor." Then Clark advises: "Bottom line on Metamor [later CIBER] is to find out what is going to make them happy."[107]

That much admits a security flaw in the system. It is astounding that anyone with a personal computer could, with a store-bought Microsoft program, open an electronic voting file and alter the contents.

But that is not all. Other passages in Clark's e-mail suggest that is exactly what has been done. Clark says he had threatened to put a password on the file when dealers, customers and support people "have done stupid things to the GEMS database structure using Access." But, he explains: "Being able to end run the database has admittedly got people out of a bind though." And continues: "Jane (I think it was Jane) did some fancy footwork on the [database] file in Gaston [County, North Carolina] recently. I know our dealers do it. King County [Washington] is famous for it. That is why we never put a password on the file before."[108] It is quite obvious that the Diebold system is vulnerable and apparently the voting database has been tinkered with.

[105] See SIMS, 2001.

[106] Quoted in SIMS, 2001.

[107] Quotations in this paragraph from SIMS, 2001.

[108] Quoted in SIMS, 2001.

One might question the authenticity of the memos. That was in fact done at first: "Initially, there were serious questions about the authenticity of the Diebold memos, but Diebold's legal actions against the web sites holding those memos were very effective at putting those questions to rest."[109] Diebold engaged the law firm of Walker & Jocke (Medina, Ohio) to try shutting down the websites displaying the memos, or at least get them to remove the memos. The bluff was called. To pursue the threatened legal action Diebold would open itself to legal action for fraud. Some websites removed the memos but the issues had spread too far to hush up. Diebold's action accomplished nothing but to confirm the authenticity of the e-mail memos.[110]

Other Suspicious Reports.

Several incidents have come to the attention of observers and votewatchers which indicate that vote manipulation does happen. These are only a few that have been noticed and are probably the proverbial tip of the iceberg. These examples also illustrate that optical scan machines which count paper ballots are also vulnerable when hooked up to a modem or the GEMS system. Some votewatchers are absolutely correct when they say that the lack of security with optical scanners is under-reported. Most, if not all, absentee ballots are counted by optical scan machines.

Alameda County, California. Robert Chen, of Diebold, wrote an e-mail on 28 October 2002 which "shows that the GEMS system in Alameda County [California] was on-line, reachable directly from the outside world."[111] This correspondence was leaked to Bev Harris of Black-Box Voting, a watchdog group on election irregularities. Alameda County uses Diebold touch-screens with a GEMS server. Jim March has posted the entire memo, along with a detailed technical analysis of this e-mail and its implications.[112] March concludes: "Therefore, during that 'window' of a couple hours after polls close, an ordinary PC in a Diebold basement could dial in, run a script, change votes specific to that county and get out again. *In about 5 to 10 minutes tops, per county*. And it would take only one conspirator among the 'techies' to get the data necessary to do actual evil."[113] (Emphasis his.)

San Luis Obispo County, California. California election laws forbid starting a vote count before the polls close. Many months after the 5 March 2002 primary election, a tally of absentee votes from 57 of the San Luis Obispo County's 164 precincts was found on Diebold's open-access Internet site. The count was time-stamped at 3:31 PM during California's 2002 primary election on March 5th. It was a mid-election tally of absentee votes from Diebold GEMS server. This mid-election tally was illegal procedure. And it was particularly disturbing to find this on Diebold's website.[114] This county was using a Diebold

[109] Jones, "The Diebold FTP Story."

[110] For a fuller description of this chain of events see Jones, "The Diebold FTP Story," pages 21-23. Also see McWilliams, 7 August 2003; Thompson, 12 September 2003; and March, 19 September 2003.

[111] Jones, "The Diebold FTP Story."

[112] See March, 23 September 2003, pages 11-13..

[113] March, 23 September 2003, page 12.

[114] For a fuller discussion of this incident see March, 24 October 2003. Also see Thompson, 12 September 2003 and Gumbel, 29 October 2003. This incident is also discussed briefly in Jones, "The Case of the Diebold FTP Site."

optical scanner with a GEMS server at the time. The file on Diebold's website was password protected, and the password was "sophia" – all lowercase. County election registrar, Julie Rodewald, said a Diebold employee named "Sophia" was there on election day. A fuller "evaluation in progress" has been made by Bev Harris and Jim March.[115] This example illustrates that even the GEMS server on optical scanners is vulnerable to a hostile attack. But at least there is a paper trail for audit.

California's Gubernatorial Recall Election. During the 7 October 2003 recall election in California, two counties were using Diebold touchscreen machines and 11 were using Diebold optical scanners with GEMS servers.[116] Of the 7,842,630 votes cast in the state, 1,403,375 (17.89%) were cast on Diebold machines. One votewatcher noticed that lower order candidates were getting an unusually high percentage of votes from counties using Diebold machines, as compared to the percentage of the state's total votes those machines cast. Seven of these lower order candidates received over twice their proportionate percentage – ranging from 39% to 91% of their total votes coming from Diebold machines.[117] (Remember the 19 candidates that were running for governor if the recall was successful?) Perhaps that election was rigged. But, although 11 of the 13 counties had paper ballots for audit, there was no recount so we will never know.[118]

Another important "piece of evidence that all was not right – and still isn't – is the alarmingly high number of ballots that registered a blank on the key issue of whether or not to recall Gray Davis."[119]

King County, Washington. During the 14 September 2004 primary election in Washington state, votewatcher Bev Harris was an observer in King County (which includes Seattle). County director of the Records, Election, and Licensing Department, Dean Logan, told the *Seattle Times* that workers on GEMS would be in pairs, never alone, and that access to GEMS is carefully controlled. Harris notes otherwise: "Our observation showed that there was no password to the terminal during the uploading of election results, as it was already open; there was no locked room, rather, the door was left open with people wandering in and out, that observers were often left alone in the room with no election officials present, that at many times observers were sleeping, reading books, or outside the room talking with others; we also observed that several people typed into the central tabulator terminal without logging themselves in as separate users."[120]

[115] See Harris and March, 7 September 2003.

[116] The two counties using Diebold touch-screens were Alameda and Plumas. The 11 using Diebold optical scanners were Fresno, Humboldt, Kern, Lassen, Marin, Placer, San Joaquin, San Luis Obispo, Santa Barbara, Trinity, and Tulare.

[117] Of the total California ballots cast, 17.89% came from Diebold machines. Yet the following low-order candidates for governor received the indicated percentage of their votes from Diebold machines: Palmieri 68.3%, Kunzman 91.75%, Sprague 65.10%, Macaluso 39.37%, Price 47.18%, Quinn 50.80%, and Martorana 39.28%. The other 12 candidates received percentages from Diebold machines that reasonably matched the state figure.

[118] For more information, see Miller, 8 October 2003.

[119] Gumbel, 29 October 2003.

[120] Harris, 15 September 2004.

Director Logan told the *Seattle Times* later that GEMS is not connected to phone modems or other computers on election day. He also reiterated that the room is always locked and the machine is passworded. But Harris says "this is what we saw: The GEMS central tabulator was connected to a bank of several dozen modems. The GEMS central tabulator at the [optical scan] location was connected to dozens of networked optical scan machines. The GEMS computer had only one person working with it at [both locations]. The GEMS tabulator required no network password because it was open all evening. The door was not kept locked and people were wandering in and out."[121]

In a video, Logan stated that GEMS worked perfectly with no problems and the modems worked correctly. Harris pointed out that on election night, workers were not able to load 5 vote centers and 84 precincts into the GEMS system. The modems (modems?) failed to work and the results had to be hand-carried in. So there is the confusing information of when machines are connected to modems and what type of information is transmitted over them. Harris points out that "the act of manipulating the election with the GEMS central tabulator is easily achieved by inserting a very short (6 line) text file on any disk or CD, which self-executes upon placing the disk in the central server computer. The procedures I observed on 9/14/2004 (popping disks in and out of the server during the middle of the count, with very sloppy disk management) put the security risk at a high level for King County."[122]

Riverside County, California. California law is very strict that no one but an election official can handle, count, or canvass ballots. It is equally specific that only election officials can touch live voting machines during an election. Technicians from the machine manufacturer do not count. These statutes were violated during the 2 March 2004 California primary election in Riverside County. Riverside County is the first California county to go all touch-screens. It has some 4,200 Sequoia AVC Edge touch-screens.

One of the closest races was between Linda Soubirous and incumbent Bob Buster for County Supervisor. Kevin Pape was also in the race. After the polls closed, 46 of the county's 157 precincts had been counted. Buster had 47% of the vote. He needed 50% plus one vote to win outright and avoid a runoff. Soubirous had 37% and Pape 15%. These results were posted at 8:13 PM and then there were no further reports. About a half-hour later an observer phoned Brian Floyd, Soubirous' campaign manager, that the counting had stopped.

Floyd and another campaign worker, Art Cassel, went to election headquarters to investigate. They found the counting room deserted except for two men – Michael Frontera and Eddie Campbell – who turned out to be Sequoia Voting System employees. Frontera was sitting at a vote tabulation computer typing and Campbell was standing next to him talking. "Their presence was unusual to say the least, and even the possibility that they might be making changes to the vote tabulation software in the middle of an election was alarming ... Cassel and Floyd said the man at the keyboard, a Sequoia vice president called Mike Frontera, was wearing a county employees ID badge – something that has not been adequately explained by anyone."[123]

Soon the electronic ballot boxes (PCMCIA flash cards) began arriving from the precincts and were piled all over the room. Election workers started feeding them into the central tabulator. As the vote counting

[121] Harris, 15 September 2004.

[122] Harris, 15 September 2004.

[123] Gumbel, 24 June 2004.

continued, another one of those dramatic swings took place which put Buster at 50% plus a mere 92 votes. A runoff was averted.[124]

By March 4th, two days after the elections, as absentee ballots were tallied, Buster's lead shrunk to 50% plus 45 votes. On this date, Floyd and Cassel saw Sequoia employee Eddie Campbell in the administrative building. He pulled a memory card from his pocket that looked like a PCMCIA card. He said to county employee Paul Shook: "Let's see if this will work."[125] Floyd abruptly asked: "Where are you going with that?"[126] Campbell refused to say or even give his name.

Campbell then went into the tabulating room with the head of the registrar's technology department, Brian Foss. Foss logged Campbell onto the terminal, presumably with his own password, and then left the room. Campbell then apparently entered Foss' password into other terminals and inserted his card to upload information onto the machine. Cassel said he recognized the WinEDS tabulation software screen on the computer. Then, as votewatcher Bev Harris relates: "Campbell took the card back, put it in his pocket, told Floyd and Cassel it was his 'personal' card, and left the building with it, got on a plane and flew out of the state to Denver."[127]

That is Cassel and Floyd's version as reported by Bev Harris and Andrew Gumbel. Gumbel's paper, *Los Angeles City Beat*, submitted a list of 44 questions to County Registrar of Voters Michelle Townsend to be answered for public information. Townsend was investigated by the county district attorney and was exonerated by the county. But before responding to the 44 questions, she abruptly resigned in mid-term, citing family reasons.[128] Andrew Gumbel writes: "Townsend leaves not only a mass of unresolved questions about the contested supervisor seat, but also about the fate of e-voting in this state."[129]

<u>The Elusive Windows CE Operating System.</u> Votewatcher Jim March notes that to surreptitiously install a "dial out" number in GEMS, to secretly connect it to the internet so the data base of votes can be altered, would require modifying the Windows operating system.[130] Standard operating systems do not have to be tested or certified by an ITA but it would be risky to alter a Microsoft program. But Windows CE is not a standard operating system. Jim March explains:

> Under the rules, 'standard software' doesn't need to be certified. *But there is no such thing as a standard version of Windows CE.* WinCE isn't like other copies of Windows; it isn't a product, it's a 'kit' which is formalized and **customized** by the company adapting this 'mini operating system' to the specific system hardware. (Most WinCE implementations are handhelds with no keyboard.)

[124] Had a runoff occurred, it would have been only between Buster and Soubirous. Those who had previously voted for Pape would likely turn to Soubirous, which could have given her a comfortable win.

[125] Quoted in Harris, 26 March 2004.

[126] Quoted in Gumbel, 24 June 2004.

[127] Quoted in Harris, 26 March 2004.

[128] Michelle Townsend had been an unrelenting advocate of touch-screen voting and, as Riverside County's registrar of voters, pioneered the first touch-screen machines in California. She was leading a lawsuit against California's secretary of state, Kevin Shelley, to revoke the list of 23 security measures he mandated.

[129] Gumbel, 24 June 2004.

[130] See March, 23 September 2003.

> Which means if the comm drivers or other pieces of WinCE are hacked ... there would be no way of cross-referencing the file size, file date/time stamp or CRC check against known editions of those files as supplied in a Microsoft retail box. You couldn't tell if they've been Frankensteined! (All emphasis and boldface his.)[131]

It's a little technical but I think anyone can get the idea. Windows CE is a skeleton operating system which is tailored to use on touch-screens by Diebold. Yet it is treated as a standard operating system when it comes to certifying the voting machine software – the testing labs don't have to look at it. And Diebold doesn't want the testing labs to think too much about it, as this leaked internal e-mail from Talbot Iredale[132] dated 15 March 2002 indicates:

> Don,
>
> We do not certify operating systems with Wyle [Laboratories]. Therefore we do not need to get WinCE 3.0 certified by Wyle. What we need to get certified is BallotStation 4.3.2. We do not want to get Wyle reviewing and certifying the operating system. Therefore can we keep to a minimum the references to the WinCE operating system.[133]

Why is Iredale so anxious to steer the testing lab away from Windows CE? It seems obvious that there is some untested code in that operating system that Diebold doesn't want known. That being true, every Diebold touch-screen voting machine in use contains untested and uncertified software.

Conflicts Of Interest. The following list is far from complete but it illustrates why many election officials are such loud defenders of electronic voting. "What election officials do not mention, however, are the close ties they have with the voting machine industry. A disturbing number end up working for voting machine companies."[134]

Michael Frontera (see section above about Riverside County) is a former Denver Elections Commission executive. In that position he placed a $6.6 million order for Sequoia voting machines. Shortly after that he went to work for Sequoia as a vice president.[135]

Bill Jones left office as California's secretary of state in 2002. He then became a paid consultant to Sequoia Voting Systems.

Bill Jones' assistant secretary of state went to work full time for Sequoia.

Former secretaries of state from Florida and Georgia became a lobbyists for ES&S and Diebold.[136]

Many election officials are happy to accept voting machine companies' largess, even while still in office.[137]

[131] March, 23 September 2003.

[132] Talbot Iredale is head of Diebold Election System's team.

[133] Quoted in March, 23 September 2003.

[134] *New York Times* editorial, 12 September 2004.

[135] Cited in Harris, 26 March 2004.

[136] Cited in *New York Times* editorial, 12 September 2004.

[137] Cited in *New York Times* editorial, 12 September 2004.

The Election Center, which does election training and policy work, takes money from Diebold and other machine companies, which sponsored meals and a dinner cruise during the Center's August 2004 national conference.[138]

The National Association of Secretaries of State derive 43% of their budget from voting machine companies and other election-related businesses.[139]

The Columbus Ohio *Dispatch* reported in 2003 that one voting machine company offered concert tickets and limousine rides while competing for a contract worth up to $100 million or more.[140]

This is the type of graft that is common in most large businesses today and it is probably to be expected when trying to sell voting machines. But when the corruption stretches to rigging elections it threatens our freedom and existence as a democracy. Yet, when one looks at the multi-billion dollar windfall provided the voting machine makers by the Help America Vote Act, and who sponsored it, one must wonder if some payback is expected.

CONCLUSION

This paper is being written prior to the 2 November 2004 presidential election. In that election some 50 million voters, almost one third of America's voting population, "are expected to vote on touch-screen machines ... federal regulators have virtually no oversight over testing of the technology. The certification process, in part because the voting machine companies pay for it, is described as obsolete by those charged with overseeing it."[141]

And the entity overseeing HAVA, the Election Assistance Commission, still armed only with obsolete standards from the early 1990s, has been described as "so toothless, they'd probably have a tough time biting through butter."[142] Due to late appointment and confirmation of commission members, the first public meeting wasn't held, and the chairman wasn't elected, until 23 March 2004.[143] Journalist Dick Polman comments: "They weren't named by the Bush administration until last winter (one year after the congressional deadline), they have a staff of only seven, and they're trying to oversee a multibillion-dollar industry on an initial budget of $1.2 million. The Election Assistance Commission can try to devise some national standards for the touch-screens in time for the Nov. 2 [2004] election – because none exist at the moment – but they'd lack the power to enforce them."[144]

[138] Cited in *New York Times* editorial, 12 September 2004.

[139] Cited in *New York Times* editorial, 12 September 2004.

[140] Cited in *New York Times* editorial, 12 September 2004.

[141] Poovey, 23 August 2004.

[142] Polman, 5 May 2004.

[143] Election Assistance Commission members are DeForest B. Soaries Jr. (chairman), Gracia M. Hillman (vice-chair), Paul DeGregorio, and Ray Martinez.

[144] Polman, 5 May 2004.

If we should have an outcome similar to Florida 2000, any dispute over the results or allegations of fraud cannot be settled or verified because there will be no voter-verified paper trail, except in Nevada. In addition to these touch-screen machines which are highly susceptible to being rigged, most of the remaining voters will be having their votes counted by electronic optical scanners. These, also, have experienced incidents in the past of skewing the vote count in favor of republican candidates, particularly with regard to the vote tabulation devices. It will be a very slim chance, indeed, that the Bush administration, and its neoconservative backers, will lose this election.

Touch-screen voting machines would be nice because they are simple to use and can accommodate voters with a wide range of disabilities, including blindness. But until their security flaws are resolved, they are extremely susceptible to fraud and rigged elections. Dr. David Dill confides: "As a computer scientist, I know that the worst problem that could happen is that you have someone at the company, such as a programmer who knows all the details of the code, or a mysteriously overqualified janitor, who could basically insert something malicious into the code. ... Malicious code could be concealed in ways that are practically impossible to detect by any means, and certainly wouldn't be detectable given what we understand to be the detection and inspection process. ... you can change the results of an election, and it can't be detected by inspection or testing. Period."[145]

When I started the research for this paper, I was amazed at the preponderance of material and the depth of studies that exist. It is overwhelming and very frightening. One need only start a simple search and follow the leads and links. If anyone still has doubts that elections in the US can be easily rigged, I urge them to start such a search. In addition, this paper treats the technical aspects of voting machine hardware and software very superficially. For anyone wishing to pursue this area in more detail, I recommend starting with the treatise by University of Iowa Professor Douglass W. Jones (See Jones,"The Case of the Diebold FTP Site."). The website of Jim March might also be useful for the Diebold system (See March, 10 October 2003). Then go on the various reports discussed in this paper. An Internet address for all of these is provided in the References. (Some of the e-mail addresses shown are not a hypertext, and will have to be copied-and-pasted to your Internet page address bar.)

As Roxanne Jekot states it: "Corporate America is very close to running this country. The only thing that is stopping them from taking total control are the pesky voters. That's why there's such a drive to control the vote. What we're seeing is the corporatisation of the last shred of democracy."[146]

# # # # #

REFERENCES [147]

Ackerman, Elise; "Voting Machine Maker Dinged," San Jose (CA) *Mercury News*, 17 December 2003.

Ackerman, Elise; "Securing Electronic Voting," San Jose (CA) *Mercury News*, 6 February 2004.

Ackerman, Elise; "Senators Aim To Bar Touch-Screen Voting," San Jose (CA) *Mercury News*, 11 March 2004.

Ackerman, Elise; "E-Voting Probe Criticizes Vendor," San Jose (CA) *Mercury News*, 22 April 2004.

[145] Quoted in Pitt, 20 October 2003.

[146] Quoted in Gumbel, 14 October 2003.

[147] If the links don't work, key the URL into your browser address bar.

Ackerman, Elise; “E-Voting Panel Wants To Dump Troubled System,” San Jose (CA) *Mercury News*, 23 April 2004.

Ackerman, Elise; “Lax Controls Over E-Voting Testing Labs,” San Jose (CA) *Mercury News*, 30 May 2004.

Alameda County Election Summary Report; Direct Primary Election, 2 March 2004. Available on Alameda County official website at file://A:/official%20final%20summary.htm

Alexander, Kim; “California Voting Technology Update,” The California Voter Foundation, 20 April 2004. Available at http://www.calvoter.org/news/cvfnews/cvfnews041504.html

Alexander, Kim; “Update: CA Paper Trail Bill Moves Ahead,” The California Voter Foundation, 27 August 2004. Available at http://www.calvoter.org/news/cvfnews/cvfnews082704.html

Althaus, Dudley; “Fraud Claims By Chavez Critics Rejected,” *Houston Chronicle*, 20 August 2004.

Associated Press; “Calif. Official Bans Some Voting Machines,” published in *The New York Times*, 30 April 2004

Computer Security Act of 1987, The (Public Law 100-235), 8 January 1988. Available at http://www.house.gov/science_democrats/archive/compsec1.html

Compuware Report – “Direct Recording Electronic (DRE) Technical Security Assessment Report,” prepared by Compuware Corporation, Columbus, Ohio, 21 November 2003. Commissioned by the State of Ohio and posted at http://www.sos.state.oh.us/sos/hava/files/compuware.pdf

Diebold AccuVote-TSx website at file://F:/DOCUME~1/Bob/LOCALS~1/Temp/P8SZN92W.htm

Different Strings; “Ohio Released Information On Security Problems With Electronic Voting Machines,” 5 December 2005. Available at http://www.differentstrings.info/archives/003263.html

Disinfopedia; “ES&S,” a project of the Center for Media & Democracy. Available at http://www.disinfopedia.org/www.disinfopedia.org/wiki.phtml?title=ES%26S

Election Assistance Commission, US; website at http://www.eac.gov

Ervin, Keith; “2 Felons’ Roles In County Elections Questioned,” *The Seattle Times*, 11 February 2004.

Fitzwater, Jeffrey; “Recent Legislation Affects Ohio Voting,”*The Post*, an independent student-run daily newspaper at Ohio University, 6 May 2004. Posted at http://www.thepost.edu/N.php?article=N2&date=050604

Fletcher, Ed (*Sacramento Bee*); “Senators Assail Touch-Screen Voting,” Verified Voting Foundation, 12 March 2004. Available at http://www.verifiedvoting.org/article.asp?id=1538

Folmar, Kate; “State Attorney General Joins Lawsuit On Voting Machines,” San Jose (CA) *Mercury News*, 8 September 2004.

Foreman, Liz: “Blackwell: Security First In Ohio Voting,” TV-WCPO Channel-9 News (Cincinnati, Ohio), 3 December 2003. Available at http://www.wcpo.com/news/2003/local/12/03/vote.html

Geczy, George; “Election Voting Device Information,” E-mail to Ohio Secretary of State/Elections Office, 4 December 2003. Available at http://seclists.org/lists/politech/2003/Dec/0033.html

Goetz, Aron; “Voting System procurement Process promises Fireworks,” *Electionline Weekly*,31 January 2003. Excerpted at http://www.electionline.org/site/docs/html/danedits.plus.dougedits_of_1-31_story.htm

Goldston, Linda; “Paper Copies Required On Vote Devices,” San Jose (CA) *Mercury News*, 22 November 2003.

Gumbel, Andrew; “All The President’s Votes?,” *The Independent* (London), 14 October 2003.

Gumbel, Andrew; “Mock The Vote,” *Los Angeles City Beat*, 29 October 2003. Available at http://www.wesjones.com/mockthevote.htm

Gumbel, Andrew; “Down For The Count,” *Los Angeles City Beat*, 24 June 2004. Available at http://www.wesjones.com/downforthecount.htm

Harris, Bev and March, Jim; “The San Luis Obispo Election File Mystery,” *Scoop*, 7 September 2003. Available at http://www.scoop.co.nz/mason/stories/HL0309/S00067.htm

Harris, Bev (submitted by anonymous); "Riverside County Security Breach," *Black Box Voting: Consumer Protection For Elections*, 15 September 2004. Available at http://www.blackboxvoting.org/?q=node/view

Harris, Bev; "King County Election – Security Flaws Observed With Tue. 9/14/04 Primary," *Black Box Voting: Consumer Protection For Elections*, 15 September 2004. Available at http://www.blackboxvoting.org/?q=node/view/614&PHPSESSID=1aae83c96608becebe14c6fc0af2125b

HAVA – *Help America Vote Act of 2002* (Public Law 107-252), 29 October 2002. Available at http://www.electionline.org/site/docs/pdf/hr3295.pl107252.final.pdf

Heichler, Elizabeth; Criticism Of Electronic Voting Machines' Security Mounting," *Computer World*, 12 December 2003.

Holt, Congressman Rush; "On Election Day 2004, How Will You Know If Your Vote Is Properly Counted?", official website at http://holt.house.gov/issues2.cfm?id=5996, accessed 25 May 2003.

IEEE Report – Kohno, Tadayoshi; Stubblefield, Adam; Rubin, Aviel D.; and Wallach, Dan S.; "Analysis Of An Electronic Voting System," *IEEE Symposium on Security and Privacy 2004*, 27 February 2004. Available at http://www.avirubin.com/vote.pdf

InfoSENTRY Report – "Computerized Voting Systems Security Assessment, Volume 1: Summary of Findings and Recommendations," a report prepared by InfoSENTRY Services, Inc., 21 November 2003. Commissioned by the State of Ohio and posted at http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf

Jacobs, Paul; :Panel Urges Paper Option For Touch-Screen Voting," San Jose (CA) *Mercury News*, 29 April 2004.

Jones, Douglas W.; "The Case of the Diebold FTP Site," at http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html

Jones, et al – Jones, Douglas W.; Dill, David L.; Neumann, Peter G.; Rubin, Aviel; and Wallach, Dan; "To The Concerned Citizens An Elected Officials Of The State Of Ohio," a letter dated 26 February 2004. Available at http://66.102.7.104/search?q=cache:1cMAUQtI7CMJ:www.cs.uiowa.edu/~jones/voting/ohioletter.pdf+Infosentry+Ohio+Volume+2&hl=en

LaMar, Andrew; "E-Voting OK'd In Santa Clara County For Fall," San Jose (CA) *Mercury News*, 15 June 2004.

Landes, Lynn; "2002 Elections: Republican Voting Machines, Election Irregularities, and 'Way-Off' Polling Results," *Dissident Voice*, 9 November 2002. At http://www.dissidentvoice.org/Articles/Landes_2002Elections.htm

Mahler, Les (San Joaquin News Service); "Call To End Touch-Screen Voting Worries County Officials," Verified Voting Foundation at http://www.verifiedvoting.org/article.asp?id=1624

March, Jim; "BBV: Jim March Gets His Cease & Desist – And Responds," Democratic Underground Forums, 19 September 2003. At http://www.democraticunderground.com/discuss/duboard.php?az=show_topic&forum=104&topic_id=367391&mesg_id=367391

March, Jim; "A Deconstruction Of A Doug Lewis/Election Center Review Of The Potential For Electronic Vote Fraud," 23 September 2003. Posted at http://www.equalccw.com/lewisdeconstructed.pdf

March, Jim; "Diebold's Vote Tally Software – Security Review Instructions," 24 October 2003. Posted at http://www.equalccw.com/dieboldtestnotes.html

McWilliams, Brian; "New Security Woes For E-Vote Firm," *Wired News*, 7 August 2003. Available at http://www.wired.com/news/privacy/0,1848,59925,00.html

Mercuri, Rebecca, PhD.; Testimony before the Subcommittee on Environment, Technology, & Standards of the US House of Representatives Committee on Science, 22 May 2001.

Mercury News (San Jose, CA); "Florida Vote Screams At Us: Get A Paper Trail," 19 January 2004.

Mercury News Editorial; "Touch-Screen Audit Should Ease Doubts," 17 November 2003.

Mercury News Editorial; "Registrars Need A Security Lesson," 18 February 2004.

Mercury News Editorial; "For Voters, Seeing Is Believing," 15 August 2004.

Messmer, Ellen; “University Researchers Criticize Electronic Voting Machines As Security Risk,” *Network World Fusion*, 25 July 2003. Available at http://www.nwfusion.com/news/2003/0725diebold.html

Miller, Mark Crispin; “Irregularities In California Race!!” Posted on *What Really Happened: The History The Government Hopes You Don’t Learn*, 8 October 2003, at http://www.whatreallyhappened.com/diebold2003.html

New York Times editorial; “On The Voting Machine Makers’ Tab,” 12 November 2004.

Nissenbaum, Dion; “Judge Rejects Plea For Electronic Voting Safeguards,” San Jose (CA) Mercury News, 19 February 2004.

Nissenbaum, Dion; “Lawmakers Unveil E-Vote Security Bill,” San Jose (CA) Mercury News, 20 February 2004.

Nissenbaum, Dion; “Governor Urged To Free Voting Funds,” San Jose (CA) Mercury News, 14 September 2004.

Ohio Press Release, “Blackwell Halts Deployment Of Diebold Voting Machines For 2004,” released by the Ohio Office of the Secretary of State, 16 July 2004.

O’Neil, Deborah; “Voting Machine Scandal Upsets Commissioners In Two Counties,” *St. Petersburg Times* (FL), 8 November 2001.

Pitt, William Rivers; “Electronic Voting: What You Need To Know,” Truthout interview posted at http://www.truthout.org/docs_03/printer_102003A.shtml

Poletti, Therese; LeMar, Andrew; and Garcia, Edwin; “State Curbs Use of E-Vote,” San Jose (CA) *Mercury News*, 1 May 2004.

Polman, Dick (Knight Ridder); “Manufacturers Defend Touch-Screen Voting Machines,” Columbus (GA) *Ledger-Enquirer*, 5 May 2004.

Poovey, Bill (Associated Press); “Nation’s Voting Machines Tested In Secret,” MSNBC News, 23 August 2004.

RABA Report – “Trusted Agent Report: Diebold AccuVote - TS Voting System,” commissioned by the State of Maryland, 20 January 2004. Available at http://www.raba.com/press/TA_Report_AccuVote.pdf

SAIC Report – “Risk Assessment Report: Diebold AccuVote-TS System and Processes,” commissioned by the State of Maryland, SAIC-6099-2003-261, 2 September 2003. Available at http://www.dbm.maryland.gov/dbm_-publishing/public_content/dbm_search/technology/loc_voting_system_report/votingsystemreportfinal.pdf

San Diego County Quick Facts From The US Census Bureau; 2000 census, at http://quickfacts.census.gov/qfd/states/06/06073.html

SB 1438 Senate Bill – Status; 10 September 2004. Available at http://leginfo.ca.gov/pub/bill/sen/sb_1401-1450/sb_1438_20040910_status.html

SB 1438 Senate Bill – Vote Information; 26 August 2004 and 27 August 2004. Available at http://info.sen.ca.gov/pub/bill/sen/sb_1401-1450/sb_1438_vote_...

Schwartz, John; “Computer Voting Is Open To Easy Fraud, Experts Say,” *The New York Times*, 24 July 2003.

Schwartz, John; “File Sharing Pits Copyright Against Free Speech,” *The New York Times*, 3 November 2003.

Seelye, Katharine Q.; “Demand Grows To Require Paper Trails For Electronic Votes,” *The New York Times*, 23 May 2004.

Shamos, Michael I., PhD, JD; Testimony before the Subcommittee on Environment, Technology, & Standards of the US House of Representatives Committee on Science, 24 June 2004.

Shamos, Michael I., PhD, JD; Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the US House of Representatives Government Reform Committee, 20 July 2004.

SIMS – “Re: Alteration Of Audit Log In Access,” School of Information Management & Systems, University of California, Berkeley, 2001. Available on the Internet at http://www.sims.berkeley.edu/~ping/diebold/lists/support.w3archive/200110/msg00122.html

Thompson, Alastair; “Diebold Internal Mail Confirms US Vote Count Vulnerabilities,” 12 September 2003. Posted at http://www.scoop.co.nz/masonstories/HL0309/S00106.htm

Voters Unite; “Sequoia In The News – A Partial List Of Events,” available on the Internet at http://www.votersunite.org/info/Sequoiainthenews.pdf

Wasserman, Jim (Associated Press); “Citizens Sue Over E-Voting, Wanting More Safeguards,” published in San Jose (CA) *Mercury News*, 18 February 2004.

Zetter, Kim; “E-Vote Software Leaked Online,” *Wired News*, 29 October 2003. Story posted at http://www.wired.com/news/privacy/0,1848,61014,00.html

Zetter, Kim; “Legislators Urge E-Voting Halt,” *Wired News*, 11 March 2004. Available at http://www.wired.com/news/evote/0,2645,62627,00.html

Zetter, Kim; “California Bans E-Voting Machines,” *Wired News*, 30 April 2004. Available at http://www.wired.com/news/0,1294,63298,00.html

GLOSSARY

ATM	Automatic Teller Machine.
DRE	Direct Reading Electronics..
ES&S	Election Systems And Software Inc.
FVSS	Federal Voting Systems Standards.
GEMS	Global Election Management System.
HAVA	Help America Vote Act of 2002.
IEEE	Institute of Electrical and Electronics Engineers.
ITA	Independent Testing Authority.
MDAC	Microsoft Data Access Components.
NIST	National Institute of Standards and Technology.
PCMCIA	Personal Computer Memory Card International Association.
PIN	Personal Identification Number.
RABA	RABA Technologies LLC.
SAIC	Science Applications International Corporation.
SIMS	School of Information Management & Systems (University of California, Berkeley).
SRI	Stanford Research Institute.

APPENDIX-A

INDEPENDENT, THIRD-PARTY, VOTING-MACHINE EXPERTS

Dill, David L., PhD, is a professor of computer science and electrical engineering at Stanford University, and has been on the faculty since 1987. His primary research interest is in the theory and application of formal verification techniques to systems designs. Because of his contribution to verification of circuits and systems, he has been appointed a Fellow of the IEEE.

Jekot, Roxanne, is an occasional teacher at Atlanta's Lanier Technical College and a computer programmer for 20 years. She runs a software consulting firm in Atlanta, Georgia.

Jones, Douglas W., PhD. is an associate professor of computer science at University of Iowa and member of the Iowa Board of Examiners for Voting Machines and Electronic Voting Equipment.

Mercuri, Rebecca, PhD, is a computer science professor at Bryn Mawr College, PA, and one of the leading independent experts on electronic voting technology. She is also a research fellow at Harvard's John F. Kennedy School of Government and has been employed by and consulted by many Fortune-500 firms. She has also composed and presented training courses for industry and government agencies.

Neumann, Peter, PhD. is the principal scientist at the Computer Science Laboratory of Stanford Research Institute, Menlo Park, California. He has been at SRI's Computer Science Lab since 1971, after spending 10 years at Bell Labs in Murray Hill, New Jersey.

Rubin, Aviel D., PhD, is an associate professor of computer science at johns Hopkins University in Baltimore, Maryland. He is also technical director of the Hopkins' Information Security Institute.

Shamos, Michael I., PhD, JD, is a professor of computer science and a faculty member of Carnegie Mellon University in Pittsburgh, PA since 1975.He is also an attorney admitted to practice in Pennsylvania and before the United States Patent and Trademark Office. From 1980-2000 he participated a statutory examiner to examine every electronic voting machine in Pennsylvania during that period. He held an identical post in Texas and examined every electronic voting machine in that state between 1987-2000.

Wallach, Dan S., PhD, is an assistant professor of computer science at Rice University, Houston, Texas.