13
Security Breaches

San Diego County and the states of Maryland, Arizona and Ohio planned to buy new voting machines, and Diebold planned to sell them. All told, these contracts were worth over a quarter of a billion dollars. Despite all the information that had come out, officials were barreling right ahead with their purchase orders.

Such confidence must be supported by a powerful factual underpinning, but so far I haven't been able to find it. Could someone please share the secret decoder ring with us, so we, too, can see why these machines should be trusted?

Election officials explained that all this criticism was just so much hooey; they trusted the machines and those computer scientists didn't know what they were talking about. Diebold announced, after the SAIC report gave it a failing grade, that the report (yes, the same one) said its voting system gave voters "an unprecented level of security." Er — I guess you could call it "unprecedented."

Many election officials are still giving Diebold's encryption scheme a clean bill of health, but I'm not sure many of them can spell the word "algorithm," much less explain it. Why do we allow election officials to pronounce opinions on computer programming anyway?

I have yet to see any of Diebold's programmers answer a single question about these software flaws. Public-relations team, yes. Software engineers? Total silence. I would like to hear from principal

14
A Modest Proposal:
Everybody out of the pool

The next chapter is called "Practical Activism," and it's full of ideas to help us take back our vote. But what, exactly, are we fighting for?

In June 2003, I queried many in the voting-activism community about what, exactly, we should *do* with a voter-verified paper-ballot system when we get it. No one seemed quite sure. It's been a long, hard fight and I'm confident that we're going to get the paper ballot — but not soon enough, and it's not worth a thing if we don't audit.

Congressman Rush Holt from New Jersey proposed HR 2239 to mandate voter-verified paper ballots, get rid of risky remote-access tools and require a spot-check audit. His bill has been a giant step in the right direction but still doesn't address auditing.

The optical-scan machines in Volusia County, Florida, demonstrate that paper ballots don't necessarily provide security, and what you are about to read shows that undesirable characters have gained high levels of inside access.

In King County, Washington, an individual named Jeffrey Dean obtained a contract to program the voter-registration system. According to sources within the King County elections office, Dean also had a key to the computer room, the passcode to the GEMS computer and 24-hour access to the building. So here's a man with access to our personal information and to the programs that count 800,000 votes.

According to the Diebold memos, Jeffrey W. Dean apparently had access not only to King County, but also to the entire suite of optical-scan software used in 37 states and the security-sensitive Windows CE program for the touch screens. He had access to our votes, but what Jeffrey Dean is not allowed to have is access to handling any checks.

That is because his criminal sentence for twenty-three counts of felony Theft in the First Degree forbids him to handle other people's money, now that he has been released from prison. According to the findings of fact in case no. 89-1-04034-1:[2]

> "Defendant's thefts occurred over a 2 1/2 year period of time, there were multiple incidents, more than the standard range can account for, the actual monetary loss was substantially greater than typical for the offense, the crimes and their cover-up involved a high degree of sophistication and planning in the use and alteration of records in the computerized accounting system that defendant maintained for the victim, and the defendant used his position of trust and fiduciary responsibility as a computer systems and accounting consultant for the victim to facilitate the commission of the offenses."

An embezzler who specialized in sophisticated alteration of computer records was programming the King County voting system, and is also mentioned specifically in the Diebold memos in connection with programming the new 1.96 version optical-scan software and the touch-screen Windows CE program. Let's look at some of the features Dean says he programmed for a "ballot on demand" optical scan application:

> *Jeffrey W. Dean, January 22, 2002 RE: serial numbers on ballots*: "The BOD [Ballot on Demand] application that we have been running in King County since 1998 does put serial numbers on the ballots (or stubs) along with a variety of optional data. The application also will optionally connect the ballot serial number to a voter."[3]

Diebold told The Associated Press that Dean left the company when they took over.[4] Actually, Diebold was loaning money to Global Election Systems while Dean was its senior vice president and a director, and after the buyout, Diebold retained Dean as a consultant:

> *From: Steve Moreland, 4 Feb 2002*: "I am pleased to announce that effective today, John Elder will be assuming the role of General Manager of the Printed Products department of Diebold Election Systems, Inc. ... Jeff Dean has elected to maintain his affiliation with the company in a consulting role, reporting to Pat Green. The Diebold Election Division management team greatly values Jeff's contribution to this business and is looking forward to his continued expertise in this market place.

While in prison, Jeffrey Dean met and became friends with John Elder, who did five years for cocaine trafficking. At the time of this writing, Elder manages a Diebold division and oversees the printing of both ballots and punch cards for several states.

Punch-card manufacturers manage a high-risk security point because this is where the die cutting is done. By setting the cut so that some chads dislodge more easily than others, it is possible to manipulate a punch-card election. Diebold's printing division also bids on printing for other voting-machine vendors, such as Sequoia.

Jeffrey Dean was released from prison in August 1995, and Elder was released in November 1996. In their prison-release documents, both wrote that they had lined up employment at Postal Services of Washington, Inc. (PSI Group), the firm that sorts 500,000 mail-in absentee ballots for King County. [5]

King County contracts the mailing of its absentee ballots out to Diebold's print and mail division, which was run by Jeffrey Dean and is now run by John Elder. This division subcontracted with PSI Group to sort King County's incoming absentee ballots.

Sorting the incoming ballots is a high-risk security point for absentee ballots. We know how many absentee ballots we send out but don't know many are filled out and sent back in, especially if they pass through a middleman before being counted by elections officials. Elections officials may tell you they count the ballots before outsourcing for precinct sorting, but in major metro areas, up to 60,000 ballots arrive in a single day and elections offices are generally not staffed to handle this. It also makes no sense to count ballots by precinct and then send them out for sorting.

Jeffrey Dean, when released from prison, had $87 in his inmate account. He had been ordered to pay $385,227 in restitution for his embezzlements. Most of us would find it difficult to bankroll a business

under those circumstances, yet somehow Dean (and his wife, Deborah M. Dean) managed to become the owners of Spectrum Print & Mail. According to securities documents for Global Election Systems, Dean had been running Spectrum since 1995 — shortly after Dean was released from prison — and in September 2000, Spectrum was purchased for $1.6 million by Global Election Systems.[6]

We've had a cocaine trafficker printing our ballots, an embezzler programming our voting system and our absentee ballots being funneled through a company that hires people straight out of prison. And when we try to find out what software is actually authorized, we get the buffalo shuffle. I don't believe there is a certification program in existence that can protect us from inside access. We need criminal background checks, full financial disclosure for all state elections officials, and robust, fraud-deterring audits.

Everyone out of the pool. We have to disinfect it.

In an audit, when there is an anomaly with a spot check, you pull the whole subset of records for a more careful examination. We just spot-checked Diebold. I'd say we found an anomaly.

These public-policy issues can't be addressed with certification or even by mandating paper ballots. We need procedural protections. We just "got lucky" and discovered Diebold's files. What about the other companies? The truth is, we have no idea how big this problem is. Every time we ask questions, we get the wrong answers.

We need a short-term moratorium on counting votes by machine. I know it sounds radical. If, temporarily, we have to do the old-fashioned thing and count by hand, let's just roll up our sleeves and do it. We shouldn't require citizens to vote on systems that can't be trusted.

Now we need to pull the subset of voting-system vendors, give everyone a background check and send an auditor in to check their records. And perhaps their memos. We need to get an independent evaluation of the software on *all* of our voting machines, to find out what the heck is actually on them.

Public Policy

It's time to rethink our public policies for voting. We took away transparency, and look what happened: We got bit. Now we need to

bring transparency back.

The Declaration of Independence does not say, "Governments are instituted among men, deriving their just powers from the consent of the computer programmers."

Unless ordinary citizens with no computer expertise can *see* with their own eyes that votes are being counted accurately, the audit system must be considered a failure. In a democracy like ours, you don't need to be a lawyer to sit on a jury. You shouldn't need to be a computer programmer to count a vote.

The "many eyes" method simply means that we let as many independent parties as possible view the vote-counting. I spoke with Christopher Bollyn, a reporter who has written several articles about the erosion in integrity of our voting system as it migrated to computerized counting. He described an election he witnessed in France:

When it comes time to count, as many citizens as can fit in the room are allowed to come in and watch the counting. Sworn election officials, some from each party in the election, in front of all the observers, count the ballots into piles of 100. Each set of ballots is placed in a bag. Then, one bag at a time, the election officials count the ballots, announcing each one. They tally up one bag and move to the next, until all are done.

It takes a relatively short time to count 1,000 votes, and by having many election precincts throughout the country, all of France can be counted in a matter of hours, in front of thousands of eyes.

In the U.S., we complain that our citizens don't think their vote matters. Here's a concept: Let people *see* their vote. Not a video representation of a vote hiding in a black box, but the *actual vote*. Count votes before they leave the neighborhood. Invite people in to watch the counting. And add a 21st Century twist: Install a Web camera, so citizens can watch the vote-counting live, on the Internet.

If we want people to care about voting, we musn't take the people out of "we, the people."

Procedural Safeguards

To correct current procedural flaws, we need to bring in the right kinds of experts — auditors — and we need to keep the system simple. Here are some procedural safeguards we should consider:

• Verify the machine tally while still at the polling place. Run a report of the tally from the polling place before phoning, modeming or driving anything to the county. Post this report on the door of the precincts and make copies available to the press.

• Compare the polling-place tally with the matching totals assigned by the central county office. If there is a discrepancy, pull out the paper ballots and do an audit.

• Provide clearly delineated accounting for the votes that appear separately from the precinct totals, like absentee votes and provisional votes. Polling-place tallies should always match what is posted at the polling place. Separate the other votes cleanly and record them in a way that is easily understandable for everyone.

• Hand audits must be a routine part of every election, not just used for recounts. Hand-audit any anomalies.

• Make "random" spot checks truly random by using a transparent and public method for random selection.

• Allow the press, and any citizen, to audit if they pay for it. If they discover that the election was miscounted, reimburse them. Find ways to do these audits inexpensively.

• Allow each party to select a handful of precincts to hand-audit. Discretionary audits shine light into any precincts deemed suspicious.

• Require audits for insufficient randomness (e.g., three candidates get 18,181 votes; voters arrived in alphabetical order).

• Require that the audit be expanded if discrepancies are spotted, *whether or not the discrepancy would overturn the election.*

• When voting machines miscount, require that fact to be disclosed, and if it is the fault of the vendor, require such failures to be disclosed to prospective buyers.

• *Consider a 100 percent audit of the paper ballots.* It may be easier and cheaper to do a 100 percent audit than to counter the political tricks that will arise when we introduce judgment (like what constitutes an "anomaly") into a robust spot-checking procedure.

The biggest objection to proper auditing is that it takes too much time. If we aren't willing to invest the time to safeguard the system, maybe we should rethink the idea of using voting machines altogether.

* * * * *

Words are important: "Paper ballot," never "receipt." A paper

ballot is a legal record and substantial. A receipt is a small slip of paper we might stick in our pocket.

Two Proposals

I. The Mercuri Method

Who created the voter-verified balloting concept? Dr. Rebecca Mercuri did. She wrote of her design concept in a paper called **"**A Better Ballot Box,"[7] the first and probably the most widely accepted design for a hybrid electronic/paper ballot system, though of course it still needs the auditing procedures.

The Mercuri Method allows proprietary voting machines made by private manufacturers but requires that they modify touch-screen or DRE machines to generate paper ballots. The system should record votes electronically, then print a paper ballot and display it behind a plastic or glass panel, which prevents the voter from removing it from the polling place, or accidentally mangling it so that it can't be easily read. The voter reviews the ballot. If it does not represent her choices, she calls an election official, who voids the ballot, and she votes again. Once she approves the ballot, it drops into a ballot box for later tallying. This voter-verified paper ballot must be the definitive record of the vote.

The electronic count can be used to provide preliminary results, but the official result must come from the paper ballots.

II. All Paper Ballots, All Hand-Counted

Victoria Collier grew up discussing vote fraud around the dinner table. Her father, James Collier, and her uncle, Kenneth Collier, wrote *Votescam: The Stealing of America*,[8] published in 1992, the first hard-hitting book about high-tech vote fraud. In 1970, Ken Collier ran for Congress against Claude Pepper in Dade County, Florida, picking up about 30 percent of the vote. As the electronic voting-machine totals weighed in, Ken Collier and campaign manager James Collier noticed that they suddenly lost 15 percentage points. They didn't get another vote for the rest of the night.

According to the Collier brothers, "[when they] compared the

official vote results with a print-out of the vote projections broadcast by the TV networks on the final election night, they found that Channel 4 had projected with near-perfect accuracy the results of 40 races with 250 candidates only 4 minutes after the polls closed. Channel 7 came even closer; at 9:31 p.m., they projected the final vote total for a race at 96,499 votes. When the Colliers checked the 'official' number ... it was also 96,499."

"In hockey, they call that a hat trick," the Colliers write. "In politics, we call it a fix."

"Listen, here's my idea," says Victoria Collier. "After the public touch-screen bonfire (we really need more community-minded events, don't you think?), we should march to our secretary of state's office and demand the restoration of a hand-counted paper-ballot system."

Collier recommends using properly designed, easy-to-use paper ballots and see-through boxes; and that the count be done by hand, in public, videotaped and aired live on television, with the results posted on the precinct wall. If we count all ballots at the polling place on Election Day, it will be much harder to alter ballots. She also recommends other security measures, to prevent ballot boxes from going missing on the way to the county elections office.

engineer Ken Clark, who wrote this about altering the audit log in Access:

From**:** Nel Finberg, 16 Oct 2001: "Jennifer Price at Metamor (about to be Ciber) [Independent Testing Authority –ITA– certifier] has indicated that she can access the GEMS Access database and alter the Audit log without entering a password. What is the position of our development staff on this issue? Can we justify this? Or should this be anathema?"

From: Ken Clark, 18 Oct 2001 RE: alteration of Audit Log in Access; "Its a tough question, and it has a lot to do with perception. Of course everyone knows perception is reality. Right now you can open GEMS' .mdb file with MS-Access, and alter its contents. That includes the audit log.

This isn't anything new ... I've threatened to put a password on the .mdb before when dealers/customers/support have done stupid things with the GEMS database structure using Access. Being able to end-run the database has admittedly got people out of a bind though. Jane (I think it was Jane) did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That's why we've never put a password on the file before ... Back to perception though, if you don't bring this up you might skate through Metamor.

"There might be some clever crypto techniques to make it even harder to change the log ... We're talking big changes here though, and at the moment largely theoretical ones ... "Bottom line on Metamor is to find out what it is going to take to make them happy. You can try the old standard of the NT password gains access to the operating system, and that after that point all bets are off ... This is all about Florida, and we have had VTS certified in Florida under the status quo for nearly ten years.

"I sense a loosing *[sic]* battle here though. The changes to put a password on the .mdb file are not trivial and probably not even backward compatible, but we'll do it if that is what it is going to take. " — Ken

Nel's reply: "For now Metamor accepts the requirement to restrict the server password to authorized staff in the jurisdiction, and that it should be the responsibility of the jurisdiction to restrict knowledge of this password. So no action is necessary in this matter, at this time."

We are leaning heavily on local election officials to set up security.

Setting aside the references to doing "end runs" around the voting system, four examples show that local officials have been unable to restrict access to authorized staff and approved software:

1. A San Luis Obispo County, California, vote database popped up on the Diebold Web site during the March 2002 primary, tallied hours before the polls closed. Election officials can't explain how it got there.

2. A cell phone was used to transfer a vote database in Marin County, California. This is insecure and was never approved by anyone.

3. In November 2000, an unexplained replacement vote database in Volusia County, Florida, overwrote the original votes, causing TV networks to erroneously call the election for George W. Bush.

4. Voting software in 10 states, certified by the ITA and NASED and escrowed by the secretary of state, was replaced by unauthorized versions which came from five men in Canada.

SLO County Mystery Tally

A vote tabulation saved at 3:31 p.m., five hours before poll closing for the March 5, 2002, San Luis Obispo County primary ("SLO County" to the locals) was found on the Diebold FTP site. SLO County Clerk-Recorder Julie Rodewald says that she doesn't know who put that file on the FTP site, and only two people have access to the GEMS computer — the Deputy Registrar of Voters and Rodewald herself. [1]

The SLO file contains votes from a real election. It also contains a problem for Diebold, because in California it is illegal to tabulate votes before the polls close. According to California law, counties are allowed to begin counting mail-in and absentee ballots prior to election day, but results may not be posted before the polls close at 8 p.m.

"We don't release those results. In fact, we don't even print results. We don't know what the results are until 8 p.m.," Rodewald said.

This file contains an audit log which documents GEMS activities step by step for months leading up to the election, stopping precisely at 3:31 p.m. on March 5, 2002.

The votes in the file correspond with the final vote tally, which

can be found on the San Luis Obispo County Web site for that election — but only about 40 percent of the votes had come in by 3:31 p.m. Computer programmer Jim March discovered that this file contained real votes.

Maybe the clock was off? It was for a different time zone? When it said 3:31 it was 8:31? Checking the date and clock is part of the election procedures, marked "important." But more than that, after the polls closed there were more votes.

Was it for training? No one does training during an election.

How do the votes correspond to the final vote tally? The vote distribution parallels that of the final tally.

The SLO vote file was assigned a password and placed on a Diebold-owned FTP site. The password was: "Sophia." Sophia Lee was a Diebold project manager. Was she there that day? Yes. Did Sophia put that file on the Diebold site?

"She's saying she did not post (the data) on election day," Rodewald said. "She said it's something she never would have done."

Did Rodewald give Sophia access to the GEMS computer and the vote database? Rodewald says that neither she nor any of her staff put that file on the Diebold site, nor does she know how it got there.

"Only the deputy (registrar of voters) and myself have access to the computer on election day or any day," Rodewald said.

The large file, which was on the GEMS computer, takes time to upload to an FTP site — even with a fast Internet connection. Rodewald said that the GEMS computer does not connect to the Internet.

Somehow this file made its way from the secure, inaccessible, locked-in-a-room, not-connected computer onto the Diebold company FTP site. Diebold denied that the information was posted on Election Day.

"Diebold is trying to track down when the information was posted," said Deborah Seiler, western regional representative for Diebold. (If Diebold was trying to find out when it was posted, why did Diebold state that it was not posted on a particular day?)

Rodewald says that the votes in the SLO file were absentee votes, which were counted before March 5. She says they are not votes cast at the polling place, which is reassuring, because the only way polling place votes could be on a Diebold company site at 3:31 in the afternoon is if the machines had an E.T. moment and decided to phone home while the election was in progress.

However, the absentee explanation doesn't exactly correspond with the tags in the file. And it doesn't explain why a partially-voted backup file would be parked on a Diebold FTP site. [2] Why should Diebold take any election vote file and keep it on a company site?

Perhaps because just 21 hours before the election, the software wasn't working correctly.

> From: Sophia Lee, 4 Mar 2002: SLO County — "Cards cast for precincts in multiple vote centers are incorrect."

Sophia's memo is a bug report showing that the software is miscounting the day before the election. It references "GEMSReport 1-17-21," a version that does not have a NASED certification number.

Whether or not anything unscrupulous is involved with this file, it seems that unauthorized access was allowed into the system on Election Day, and also that machines were using uncertified software which wasn't working properly.

Transferring votes by cell phone

On October 8, 2003, I spoke with Marc Carrel, assistant secretary of state for policy and planning for the state of California. I asked Carrel about a set of memos indicating that Diebold has used cell phones to transfer vote results.

"That's not certified." he said. True. "Not in California, they haven't," he said, after a stunned pause. Yes, they have. In Marin and Tulare counties, according to the Diebold memos.

I passed the memos to an investigative writer named Tom Flocco (www.tomflocco.com). In his blog he wrote:

> "Diebold sales representative Steve Knecht wrote on April 12, 2000 that 'We are using cell phones in Tulare and Marin,' while also introducing a rather curious, unfamiliar electronic election official called a 'rover:' 'Rovers are the ones who are given the cell phone with the modem for end of night totals upload, not the precinct worker, at least in these two locations.'
> "Guy Lancaster, Diebold software programmer, wrote on April 12, 2000, regarding cell phones: 'I know of no written instructions,' leading us to wonder if there were rules and traceable documentation, or why cell phones were

being used in the first place. ...

"[Diebold sales representative Juan Rivera wrote] 'Also, we did not have to dial the phone manually; the AccuVote did that just as if it was connected to the wall jack.' ... So now we have private cell-phones, laptop computers — and rovers, ostensibly uncertified by any government authority.

"On April 17, 2000, Guy Lancaster wrote more about the Diebold AccuVote internal modem: 'We use what's called 'blind dialing' (ATX0) which means that it'll dial with nothing plugged into it. Thus if the AV won't work without this Dial Tone Emulator, then it's doing something in addition to providing a dial tone.'

Dr. David Dill's webmaster, Greg Dinger, arranged for a friend to assist as an official pollworker. Shortly after the 2003 recall election, Dinger filed this report:

"OK, I have some news," "At the end of the day, the 'head' of the scanner was removed from the base. It was connected to some sort of cell phone for transmitting the results. ... It was wireless. ...

"During the transmission process, errors occurred. The phone apparently reported that a ballot was 'stuck' in the reader. The precinct folks confirmed that this was not the case. There was a phone call placed to some 'support number' which turned out to be a bad number. The lead precinct worker happened to have another phone number, reached some unidentified (to my friend) person, and eventually resolved the issue after a lengthy delay. ...

" ... The precinct leader was provided a cordless phone of some sort. At the end of the day, she pulled the scanner out of the base and moved it to a table. Then the phone was attached (as I understand it) with a short cable. I do not believe the unit was built into the scanner, nor was it connected during the day." [3]

Yeesh. A well-financed operation can penetrate the voting system with the right equipment and the correct information. Cell phones connect to the access tower with the strongest signal. It is relatively easy, though not inexpensive, to set up a rogue access tower. If you do, this cell phone will automatically communicate with you. You could connect the call to your own GEMS server, load the real results, modify them and then call up the real GEMS server to upload your results.

Volusia County, Florida:

John Ellis, hired as an analyst for Fox TV News, knew exactly the margin needed to call the 2000 presidential race for George W. Bush. He was privy to the Voter News Service data, and he spoke several times during the evening to his two cousins: Jeb and George W. Bush.

At 2:09 a.m., the required vote margin appeared from Volusia County, Florida. At 2:10 a.m., this margin was enhanced by a 4,000-vote bump in Brevard County, and at 2:16 a.m., Ellis called the race for George W. Bush. Within four minutes, NBC, CBS and ABC followed suit. [5]

Precisely the right margin appeared on a Volusia County machine (Global Election Systems, now Diebold), amplified by a Diebold/ Global Election Systems machine in Brevard County. Unfortunately, these vote totals were incorrect and soon disappeared, along with a "card no. 3" which helped to create them.

If Al Gore had publicly conceded on election night, would we ever have learned that these votes were bogus? Would there have been a recount, and could the "Help America Vote Act" have passed, triggering the rush to touch-screen machines?

We'll never know, but thanks to an internal CBS report and a memo written by Talbot Iredale, vice president of research and development at Diebold Election Systems, we now know that the unexplained replacement of a set of votes on a Diebold optical-scan machine in Volusia County triggered a premature private concession from Al Gore to George W. Bush and resulted in TV networks' erroneously calling the election for Bush instead of deeming it too close to call. The final "offical" tally showed Gore losing by 527 votes, though the hand recount stopped by the Supreme Court later gave the election to Gore.

> *Fox News Network, 29 November 2000: Brit Hume, host*: " ... It seems a broken computer modem and a faulty memory card were culprits in the erroneous election-night call of George W. Bush as the Florida winner ... computers with a bad memory card caused it to appear for a time that Al Gore had lost more than 16,000 votes, which seemed to put George W. Bush up by 50,000 — at that stage in the night, an insurmountable margin. Every network saw that as a basis for calling the state for Mr. Bush. ... " [6]

Was it a "bad memory card" that produced the 16,000-vote spread? Or is there another explanation? And is it true that these 16,000 mystery votes caused the networks to call the election for Bush?

Let's look at the symptoms of a bad memory card. A memory card, as you'll recall, is like a floppy disk. If you have worked with computers for any length of time, you know that a disk can go bad. When it does, which of the following is most likely:

a) In an Excel spreadsheet that you saved on the "bad disk," is it likely to read a column of numbers correctly the first time: "1005, 2109, 3000 ... " but the second time, replace one of the numbers like this: "1005, 2109, –16,022 ... "?

b) Or is it more likely that the "bad disk" will do one of the following things: Fail to read the file at all; crash your computer; give you an error message; or make weird humming and whirring noises while your computer attempts unsuccessfully to read the disk?

For most of us, the answer is b). But according to news reports, the official explanation from Global Election Systems was that a "bad memory card" reported votes correctly in every race except the presidential race, where it changed Gore's total to minus 16,022.

This kind of explanation gets my nose twitching. Really? Is that what a "bad memory card" does? If so, how many "bad memory cards" have been out there changing vote totals, unbeknownst to voters?

If the symptom of a corrupted memory card was arbitrary vote-changing, as explained to the media in Volusia County, we'd be in real trouble — according to Diebold sales representative Steve Knecht in a March 24, 2000, memo: "*Cards were corrupted throughout California at a rate exceeding our normal 1 in 100 that we've been seeing. Marin is now up to 8 cards corrupted out of 114*."

With these numbers, we'd better hope that the symptoms do *not* include randomly changing the vote totals.

According to an exchange between principal engineer Ken Clark and Donna Daloisio, who was systems administrator for Supervisor of Elections Gertrude Walker in St. Lucie County, Florida, the following symptoms typify a corrupt memory card:

When beginning to upload results the following message appears: "*Please re-insert memory card*." If you take the memory card out and put it back in, you are likely to see this error: "*Pct data error*

OK to continue?" If you say yes, this message appears again: "*Please re-insert memory card*."

When Daloisio described these symptoms, principal engineer Ken Clark shot back this diagnosis: "*Garden variety corrupt memory card*."

The Diebold memos reveal that the story given to the media about Volusia County's sudden vote discrepancy isn't quite the whole story.

On January 17, 2001, Volusia County employee Lana Hires asked the technical staff at Global Election Systems for help. She was being put on the hot seat over Al Gore's strange tally of negative 16,022 votes.

"I need some answers!" she wrote. "Our department is being audited by the County. I have been waiting for someone to give me an explanation as to why Precinct 216 gave Al Gore a minus 16022 when it was uploaded. Will someone please explain this so that I have the information to give the auditor instead of standing here 'looking dumb.' " [7]

Global Election Systems' John McLaurin tossed the hot potato to Sophia Lee and Talbot Iredale. "Sophia and Tab may be able to shed some light here, keeping in mind that the boogie man may me *[sic]* reading our mail.* Do we know how this could occur?" [8]

Talbot Iredale, senior vice president for research and development, explains: "Only the presidential totals were incorrect." Iredale then hits us with this bombshell: [9]

> "The problem precinct had two memcory *[sic]* cards uploaded. The second one is the one I believe caused the problem. They were uploaded on the same port approx. 1 hour apart. As far as I know there should only have been one memory card uploaded."

Where did this second card come from? Iredale then gives a cursory nod to the official explanation given to the media:

> "Corrupt memory card. This is the most likely explaination *[sic]* for the problem but since I know nothing about the 'second' memory card I have no ability to confirm the probability of this."

Again, where did the second card come from?

> "Invalid read from good memory card. This is unlikely since the candidates

*That's a damn curious remark!

results for the race are not all read at the same time and the corruption was limited to a single race. There is a possiblilty that a section of the memory card was bad but since I do not know anything more about the 'second' memory card I cannot validate this."

There's that pesky second card again. He then suggests that perhaps the second card might have been — well — another way to say this would be "election tampering," I guess:

"Invalid memory card (i.e. one that should not have been uploaded). There is always the possiblity that the 'second memory card' or 'second upload' came from an un-authorised source."

So, who is investigating this unauthorized source?

"If this problem is to be properly answered we need to determine where the 'second' memory card is or whether it even exists.

But it turns out that this second card did exist:

"I do know that there were two uploads from two different memory cards (copy 0 (master) and copy 3)."

There were two uploads from two different cards.

- The votes were uploaded on the same port about 1 hour apart.
- Only one memory card was supposed to have been uploaded.
- "Copy 0" uploaded some votes.
- "Copy 3" replaced the votes from "Copy 0" with its own.
- Iredale believes the second one is the one that caused the problem.
- The "problem": 16,022 negative votes for Al Gore

We know that the "problem" was noticed and corrected. An election worker noticed Gore's votes literally falling off the tally, and the number of votes in Precinct 216 was totally out of whack. Eventually, a manual recount was done. No harm, no foul?

That depends on how you look at things. I found a report called "CBS News Coverage of Election Night 2000: Investigation, Analysis, Recommendations prepared for CBS News." [10]

"It would be easy to dismiss the bizarre events of Election Night 2000 as an aberration, as something that will never happen again," the report begins. " ... But, this election exposed flaws in the American voting system, imperfections mirrored in television's coverage of the election results."

Yes. This election exposed flaws, but the imperfections were not really quite "mirrored" in television's coverage of the results. A more apt metaphor would be that the imperfections exposed the tip of an iceberg and then, with the HAVA bill, everyone in America decided to buy a ticket on the *Titanic*.

It is, as one of the computer scientists I've talked with likes to say, like "The Amazing Randi." Don't look there — look here! An illusion. Ridicule the dangling chads. Voter News Service blew it. Don't worry, we caught that crazy error of minus 16,022 votes, it made no difference. We'll give you the Help America Vote Act (HAVA) and promise $3.8 billion (much of which may never materialize) to prevent this fiasco from ever happening again.

Look over here: Chads are bad. Look over there: Let's vote on a black box!

Don't look there: No one paid much attention to the optical-scan machines, which, we now know from Greg Palast's research, used different settings depending on whether you were in a minority district or an affluent suburb. White? Suburban? Set the machine to provide an error message if the ballot was overvoted, so the voter can correct it. Minority? Poor? Accidental overvotes discarded, thank you. Back that up with statistics, of course: "Too dumb to vote." [11]

While we fixated on a butterfly ballot, no one asked about the GEMS program, or demanded to see "card number 3" from Volusia County, or asked who made this card and how it got past all the election procedures and physical security, or whether any other counties had a card number 3.

Here is a chronology of how the election was called for Bush. You decide whether card number 3 made a difference: [12]

7:00 PM: CBS News' estimate, based upon exit-poll interviews, shows Gore leading Bush by 6.6 percentage points.

7:40 PM: Voter News Service (VNS) projects Florida for Gore.

7:48 PM: NBC projects Florida for Gore.

7:50 PM: CBS projects Florida for Gore.

7:52:32 PM: VNS *calls* Florida for Gore.

8:10 PM: CBS News analysts recheck the Florida race and feel even more confident about the call for Gore.

9:00 PM: A member of the CBS News Decision Team notices a change in one of the Florida computations. One of the estimates, the one based solely on tabulated county votes (voting-machine results rather than exit polls) is now showing a Bush lead.

9:07 PM: VNS reports vote data from Duval County that put Gore in the lead. This was then deemed to be an error.

9:38 PM: VNS deletes the Duval County vote from the system. Gore's total in Florida is reduced by 40,000 votes.

10:00 PM: CBS withdraws the Florida call for Gore.

10:16 PM: VNS retracts its Florida call for Gore.

At some point between 10:16 p.m. and 1:12 a.m., Bush took the lead.

1:12 AM: Associated Press, which collects its numbers separately from VNS, shows the Bush lead dropping. VNS differs. Correspondent Ed Bradley begins warning people in the CBS studio of irregularities.

1:43AM: Bradley points out that more than 30 percent of the vote is still uncounted in Dade and Broward counties, Democratic strongholds.

1:48 AM: Bradley does the math: "Bush is ahead by 38,000 votes. And still out there, about 5 percent of the vote is still out, 270,000 votes. So that's a big chunk of votes." Bradley seeks more information from the AP wire and from CBS News correspondent Byron Pitts.

2:00 AM: According to VNS, Bush leads by 29,000 votes. Heavily Democratic counties have not weighed in yet. Ed Bradley is talking about the AP reports, but CBS is not using that information.

2:09 AM: VNS adds Volusia County's incorrect numbers to its tabulated vote. This change increases Bush's VNS lead to 51,000 votes.

2:09:32 AM: Bradley sounds an alarm, but no one pays attention: "Among the votes that aren't counted are Volusia County. Traditionally they're … one of the last counties to come in. That's an area that has 260,000 registered voters. Many of them are black and most of them are Democrat."

2:10 AM: Brevard County omits 4,000 votes for Gore.

Bush's lead in the VNS count includes 16,000 negative votes for Gore and unspecified other voting problems such that Bush's lead appeared to increase by 20,000 votes in Volusia (plus the 4,000 missing from Brevard).

According to the CBS News report: "These 24,000 votes would have nearly eliminated the 30,000-vote final Bush margin the CBS News Decision Desk has estimated. There would have been no call if these errors had not been in the system."

2:16 AM: John Ellis calls Florida for Bush.

2:16 AM: NBC calls Florida for Bush.

2:16 AM: The AP lead for Bush drops by 17,000 votes, to 30,000. This 17,000-vote drop, occurring in only four minutes, is a Volusia County correction. But VNS does not use the correction, and no one at CBS is listening to Ed Bradley or watching the AP wire.

2:16:17 AM: Dan Rather talks with Bradley about the large number of votes still out in Volusia County.

2:17:52 AM: CBS calls Florida for Bush.

2:20 AM: ABC calls Florida for Bush.

2:47 AM: The AP reports that Bush's lead has dropped to 13,934.

2:48 AM: VNS still shows the Bush lead at 55,449.

2:51 AM: VNS corrects part of its Volusia error, and Bush's lead drops to 39,606.

2:52 AM: The AP reports the Bush lead down to 11,090.

2:55 AM: Palm Beach County weighs in with a large number of votes, and VNS reports the Bush lead down to 9,163.

3:00 AM: Rather preps viewers for a Gore concession speech: "We haven't heard yet from either Al Gore or from the triumphant Governor Bush. We do expect to hear from them in the forthcoming minutes."

*3:10–3:15 AM:** Al Gore telephones Mr. Bush to concede.

3:10 AM: CBS begins investigating the VNS numbers. It also, finally, begins watching numbers from the AP. CBS also looks at the Florida Secretary of State's Web site. The three sets of numbers don't match, but all of them indicate the race is much closer.

3:32 AM: From 3 a.m. until now, there is much talk about the expected Gore concession speech.

3:30-3:45 AM:** Gore boards a motorcade for a 10-minute journey to War Memorial Plaza in Nashville, Tennessee, to deliver a concession speech to the nation.

3:40 AM: Bush's VNS lead drops to 6,060 votes.

---

* At this point I have drawn the timeline from three sources: CBS report, an Agence France-Presse [13] (*) report, and Dow Jones News [14] (**). The events reported after 3 a.m. sometimes differ by a few minutes between these reports.

Around this time, Gore Campaign Chairman William Daley places a call to CBS News President Andrew Heyward. Daley asks whether CBS is thinking about pulling back its call for Bush. Heyward wants to know what Gore is planning to do.

According to the CBS report, "Daley says, 'I'll get right back to you,' hangs up and does not call back.

When the lead is down to 6,000 votes, Daley asks whether CBS is thinking about pulling its call for Bush. The answer is they want to know what Gore is planning to do. Is it just me, or does this response bother you?

3:48 AM: "Rather says, 'Now the situation at the moment is, nobody knows for a fact who has won Florida. Far be it from me to question one of our esteemed leaders [CBS management], but somebody needs to begin explaining why Florida has now not been pulled back to the undecided category. ... A senior Gore aide is quoted by Reuters as confirming that Gore has withdrawn [his] concession in the U.S. President race."

*3:45-3:55 AM:** Two blocks away from the plaza, Gore field director Michael Whouley pages traveling chief of staff Michael Feldman to tell him the official Florida tally now shows Bush up by just 6,000 votes, with many ballots left to be counted. By the time the Gore motorcade reaches the plaza, according to Agence France-Presse, he is down by fewer than 1,000 votes. Gore did not, then, give the speech he had planned to give. Instead he consults with his staff.

3:57 AM: According to CBS, the Bush margin has narrowed to fewer than 2,000 votes. CBS News President Heyward orders that CBS News retract the call for Bush.

By 4:05 AM: The other networks have rescinded the call for Bush.

4:10 AM: According to CBS, Bush's lead drops to 1,831 votes, which is roughly where it remains until the first recount.

4:30-4:45 AM:** Gore makes a second telephone call to Bush to retract his concession, saying that he is waiting for all the results from Florida.

5:05 AM:** A Florida election official announces a recount, with the two candidates separated by a few hundred votes.

According to the CBS report, "the call for Bush was based en-

tirely on the tabulated county vote. There were several data errors that were responsible for that mistake. The most egregious of the data errors has been well documented. Vote reports from Volusia County."

Four thousand votes for Gore were omitted from the tabulation in Brevard County, and in Volusia, 4,000 votes were erroneously counted for Bush and 16,022 negative votes were recorded for Gore.

"The mistakes ... which originated with the counties, were critical," says the report. "They incorrectly increased Bush's lead in the tabulated vote from about 27,000 to more than 51,000. Had it not been for these errors, the CBS News call for Bush at 2:17:52 AM would not have been made."

If you strip away the partisan rancor over the 2000 election, you are left with the undeniable fact that a presidential candidate conceded the election to his opponent based on results from a second memory card (card #3) that mysteriously appears, subtracts 16,022 votes, then just as mysteriously disappears. If this isn't disturbing enough, consider these three points:

1) We don't know whether this was an isolated incident. It may have occurred elsewhere, but in smaller, less spectacular totals.
2) The errors were correctable because paper ballots existed and a 100 percent audit was done.
3) The fact that "negative votes" could be applied to a candidate's total demonstrates such a fundamentally flawed software model that it calls into question the competence and integrity of the programmers, the company and the certification process itself.

The Diebold Memos

During the middle of the night on Friday, September 5, 2003, a set of memos leaked into my FTP server. They originally came from a person with inside access to the Diebold server who used an employee I.D. number to obtain and copy them.[15] The memos were first leaked to David Allen on July 29, but, because of technical problems, he says he was unable to extract them from their compressed .tar file.

On Saturday, September 6, I downloaded this 15,000-document tarball, found a utility to open it and started reading. I read 7,000 memos and made 300 pages of notes, divided into five categories,

and didn't come up for air until Monday, September 8.

What I found was not good.

While the certified version of the voting software sat in escrow at the secretary of state's office, unauthorized versions were being put on the FTP site and, from there, downloaded and installed, overwriting the approved software. The memos documented this.

I therefore did three things. I made a copy of everything and put it into the hands of someone I trust. I burned the memos onto a CD and met face-to-face with a U.S. congressman,[16] who asked questions for 30 minutes, and then took the memos to Washington. And I selected 24 memos that describe the practice of substituting unexamined software for the approved version, and posted them on my Web site. [17]

While writing up my notes on the memos, I discovered a curious thing. I wanted to find out whether the software they were uploading (and using in elections) was certified or not. But for some reason, links to the official certification list had been pulled off both NASED and The Election Center's Web sites. I was able to locate an out-of-date version but could find nothing current.

The more I hunted, the odder it looked. If this whole system is based on certification, why is it so hard to find out which versions are certified? It should be a simple matter to compare the NASED certification number with the version number used in elections.

Andy Stephenson, a researcher who worked with me on this project, called R. Doug Lewis of The Election Center to ask for the certification list. Lewis hung up on him. I called the Washington State Elections Division and was told someone would have to call me back. No one did. Linda Franz, of Citizens for Voting Integrity-Washington, found one document through an obscure link on the Johnson County, Kansas, Web site. By searching with an Internet tool that archives old Web pages, I found three reports, which had been pulled off the Web.

Looking at every ITA-tested, NASED-authorized version number available leads to only one conclusion: Diebold has been putting unauthorized software into our voting systems.

When Georgia Secretary of State Cathy Cox says of ballot-tampering, "It would take a conspiracy beyond belief, of all these different poll workers … I don't see how this could happen in the real world," she's dead wrong. If you can slip uncertified software into voting machines, it takes only *one person*, working alone at night.

The Diebold memos made their first public appearance on BlackBoxVoting.org in the form of 24 memos with a commentary about Diebold's use of uncertified software. Everyone yawned except Diebold, which issued a cease-and-desist.

You might be yawning now. Someone used version 1.18.14 instead of version 1.17.23. *Ho hum*.

Except for this: A programmer never changes a version number unless he changes the underlying computer code. If the versions are never submitted for certification, only the individual who programmed the change knows for sure what he put in there.

Certification is the foundation of the voting industry. Remove it, and the whole house of cards tumbles.

"Maybe they'll say it was just to fix bugs," one reporter suggested. Sure. And they'll say it was just to add features or to create a new report format. And that might all be true, but before you breathe a sigh of relief, let me give you a taste of just how out of control this problem has been:

"As far as we know, some guy from Russia could be controlling the outcome of elections in the United States," Lynn Landes wrote.

Lynn, meet Dmitry Papushin, some guy from Russia. He is one of five Diebold programmers who have been putting programs on the FTP site. Take a look at his memos. What he's doing here is placing uncertified software versions on a Web site, and people are using it.

Underlines represent versions that were never certified, or the implementation of poor security procedures.

> *18 Jan 2000 memo from Dmitry Papushin*: "GEMS 1-14-5 is ready.
> *January 25, 2000 memo from Steve Knecht*: "Will all future 1.14x versions be compatible with 1.14.5 if we burn mem cards in San Luis Obispo now?"

> *15 January 2003 memo from Dmitry Papushin*: "Ballot Station 4-3-14 for Windows CE and Windows NT are ready."

> *10 February 2003 memo from Cathy Smothers*: "Can anyone send me the BS CE 4.3.14 .ins file? I have a demo tomorrow and I need this to upgrade the TS units."

From 1999 to 2003, Papushin uploaded more voting-system software

onto the unprotected Diebold Web site than any other programmer. Papushin has been a keeper of the passwords and the king of single-sentence memos. He knows the voting-system programming intimately and has uploaded computer code that programs your smart card, captures your votes at the polling place and accumulates and reports them at the county.

His programming skills and his ability to distribute programs to techs and county officials make him a tempting target for bribery. We assume that Dmitry Papushin has integrity and ironclad ethics. But to deter the unscrupulous from making inappropriate solitications to programmers like Papushin, we need to *enforce* regulations which require that only authorized software be used, and we need fraud-deterring audit procedures.

* * * * *

To examiners of the Diebold files, Ken Clark has become somewhat famous for his blunt writing and ethical shortcuts. Clark's comments in the touch-screen source code are quite a hoot, though not inspiring of confidence in the touch-screen system:

"the BOOL beeped flag is a hack so we don't beep twice. This is really a result of the key handling being gorped. (WriteIn.cpp,v)

" this is completely screwed up. the iIndex calculations are incorrectly based on nybbles for some unknown reason, and so the offsets are incorrect. This works only because the offsets are also incorrect when the card is read." (VoterCard.cpp,v)

"Reserve place in hell for person who renamed CRace and friends to CRaceKey." (BufferedSocket.cpp,v)

"Add and comment out code to work around bogus -1 in ballot level IDs." (BallotRstDlg.cpp,v)

"this is a sick hack to parse out a jurisdiction from a multi-line election title. The jurisdiction field should be eliminiated altogether and this code removed. This whole section is fairly broken wrt GEMS. GEMS doesn't store the "election information" in any kind of multilingual sense, let alone rich text. For now just stuff the english into all languages." (BuildElecDlg.cpp,v)

Deep magic is not working? Tried input of 6 and got back 1" (CIssue.CPP,v)

"The scaling stuff is complete voodo.*[sic]* Trust me or rewrite it to make more sense." (TextCell.cpp,v)

"I justify the label by saying the existing code was crap structurally to begin with." (Votercard.cpp,v)

In a July 1999 memo, Ian Piper wrote, "What is GEMS written in?" Clark replied, "GEMS is written in my office."

So Clark programs the GEMS system that accumulates and reports votes from polling places. We have weak and sometimes unenforced procedures for comparing polling-place results with the county tabulations, so the GEMS program is a tempting target.

Clark repeatedly advises field technicians to skirt U.S. election law pertaining to using only certified software versions.

From: Cathi Smothers, June 05, 2000, to Ken Clark: How do I know which version of GEMS (i.e. 1.16.3, 1.16.4, etc.) to use?"

From: Ken Clark, 5 Jun 2000: "... Baring any certification issues, the latest stable release is what you want to upgrade accounts to ... Right now 1.16.latest is considered stable, 1.16.4 being the current release by my mail ... "Its fair to say the nature of this company and business make this process fairly informal, perhaps more so than I would like. Testing releases go out to customers when they shouldn't, and new features get added to stable branches when they shouldn't ... Sometimes a bug slips into a stable branch, in which case its better to ship a version you trust, or wait for it to get corrected ... "The DLL files shipped on the GEMS CD get updated from time-to-time as well ..."

From: Ken Clark, 6 Jul 1999: I hate more than anyone else in the company to bring up a certification issue with this, but a number of jurisdictions require a 'system test' before every election ... That is why the AccuVote displayes *[sic]* the silly ***System Test Passed*** message on boot up instead of "memory test passed", which is all it actually tests. "No argument from me that it is pointless. You could probably get away with a batch file that prints "system test passed" for all I know."

From: Ken Clark, 7 Jan 2000: "*Any* testing we can do on 1.14 is a good idea. With the risk of sounding alarmist, 1.14 really needs more testing. Even though much of GEMS looks the same from the outside, the guts changed substantially between 1.11 and 1.14. That's why you see all kinds of things completely unrelated to shadow races broken in the early 1.14 releases."

From: Steve Knecht, 14 Jan 2000: "Is it the intention of development staff that California March election will be run on some version of 1.14 or will we end up in the 1.15 range ..."

(*Answer from Ken Clark, 14 Jan 2000)*: "Needless to say, the changes were extensive. The paint is still wet ...

* * * * *

We know nothing at all about Whitman Lee, another Vancouver programmer who uploads software to the FTP site. His memos consist of fixing bugs and uploading replacement software, which he did three dozen times over a 24-month time period.

From: Whitman Lee

"GEMS 1-5-3 is ready to download.

"GEMS has evolved so many times that it breaks some of the pre-election reports..."

"Here is the latest changes since 1.5.8."

"AVTS-3-4-1.zip is up. Here is this short "upgrade" instructions."

"The password for ATTemplate-3-4-1.zip is msd8sdh3isohr."

"GEMS-Reports-1-9-6.zip is ready for download."

"GEMS 1.11.2 is ready."

"The fix will be in GEMS-1-18-9."

* * * * *

Guy Lancaster's specialty is programming the optical-scan system. He has also arranged for uncertified software to enter our optical-scan machines. A lot of it, apparently.

From: Guy Lancaster, 27 Jan 1999: "For those romantics that fell in love with 1.94f, the latest flavor incorporates all the changes made since 1.94f<. This includes the changes in 1.94q, r, s, t*, and u. Pass your orders on to McKinney. * Note: The PC 1.94t release was preempted by 1.94u."

From: Guy Lancaster, 25 Feb 1999: "Our latest 1.94 releases have been rushed out to fix a bug that slipped out with 1.94u and 1.94f>. Namely, 1.94u and 1.94f> fail to detect unvoted ballots and therefore cannot return blank ballots ..."

From Ken Clark, July 2, 2002: "You have to be careful when talking about 1.94f firmware. There is a symbol after each f that corresponds to the actual release of the firmware. They very probably have a 194f that is in reality r, s, t etc."

From Don Bizmaier, Support services specialist, July 2, 2002: "I am not sure where they came from ... but Jeff Co [Jefferson County] KY uses an "S" chip in the Absentee and Mail in AVOS [Diebold optical scan machine] to ignore sequence nimbers *[sic]*."

* * * * *

Talbot "Tab" Iredale, senior V.P. for research and development, was hired when the company was still called North American Professional Technologies.[18] He oversees the programming. You will find his work in the most sensitive sections of the touch-screen source code, and he also programs the Windows CE operating system.[19] According to Rob Behler, Iredale wrote the Georgia Windows CE patches.

From Ian S. Piper 12 Jul 2002 re: Windows CE changes: "Upgrading from WinCE 3.0 (June 7th edition) to WinCE 3.0 (July 5th edition.) When upgrading from the June 7th edition of WinCE 3.0 to the July 5th edition of WinCE 3.0 (we're ignoring the July 2nd and July 4th editions), the settings should remain in the internal Flash memory ... "

From Tari Runyan Tue, 2 Jul 2002: "Is it necessary to upgrade at this point - Early voting starts in 1 month and I am hesitant due to tight timelines ... "

(reply from Talbot Iredale 16 Aug 2002): "Yes, it is recommended to upgrad *[sic]* all units to this version."

From: Rodney D Turner , 31 Aug 2000: "The computer for LA has GEMS 1-16-9 and the AVTS units have 3-13-1-4. The computer for Alameda has GEMS 1-16-10 and GEMS 1-16-9 (there is a short-cut on the desktop for GEMS 1-16-9) the AVTS units have 3-13-1-4. "

From: Talbot Iredale, 31 Aug 2000 Re: Software for Los Angelas [sic], *CA* "Jeff and Rodney, LA and Alameda will need a revised version of GEMS and maybe BallotStation to support the import/export that they require. I am working on it now but I am certain there will be more changes."

From: Larry Dix, 31 Aug 2000 RE: Software for Los Angelas [sic]*, CA* "Tab – Would you be willing to venture an outside guess as to when the revised GEMS version will be ready. This really becomes an issue since I need to coordinate staff to be onsite. Is this also the case for Alameda? Coordination of time and staff is everything on these 2 installs."

From: Ken Clark, 31 Aug 2000 Subject: RE: GEMS-1-17-1: "Is this a "testing" release or not?"

From: Talbot Iredale, 31 Aug 2000 Subject: Re: GEMS-1-17-1: This is no more of a test release than 1.16.9 was though I would not be surprised if we have to make more changes to fully support LA and Alameda.

From: Talbot Iredale, 29 Oct 2002: "... We have found a serious bug in GEMS 1-18-14 ... We will be releasing a GEMS 1-18-15 that fixes this bug within the next 2 days. Please ensure that all accounts that are using GEMS 1-18-14 upgrade to GEMS 1-18-15* prior to the election."

Here are a couple odd memos pertaining to an uncertified version number popping up on the screen in Florida:

*From: Greg Forsythe, 17 Feb 200*0: "Just received a call from Beverly Hill, Alachua County [Florida] ... She is at the SA screen and the version is 1.92-15 ... This copy has 1.92-14. 1.92-14 is certified, 1.92-15 is not. SOLUTION REQUIRED!

From: Greg Forsythe, 17 Feb 2000: "... Solution might be to make the copy the official database showing the correct version."

From: Nel Finberg, 17 Feb 2000: "The problem has been fixed."

From: Nel Finberg, 17 Feb 2000: "... It would be a good idea to get rid of the original diskette in order to remove the perception of version conflicts."

From: Don Vopalensky, 12 Sep 2002: "Ken,Texas now requires ITA certification ... ITA certifications, state certifications, and time constraints play a big part in what needs to be done, and sometimes that means putting fixes or additions back into versions that are already in use ..."

Nel Finberg September 25, 2002: "What will be run in Texas will depend on the outcome of the Texas certification decision, won't it?"

From: Ken 25 Sep 2002: "Hard to say. It never has in the past."

Tari Runyan, July 15, 2002: "this bug affects Co [Colorado] - primary Aug 13 and Ga [Georgia] Primary Aug 20 are we proposing to upgrade again this close to an election?

From Ken - "That would be up to you."

Jeff Hallmark, October 08, 2002: RE: Tippacanoe, IN upgrade to 4-3 first then downgrade to 4-1-11, this is quite fast if one sets up 3 or 4 machines at a time. no backdoor humm..

Sue Page, October 16, 2002: - Maryland ... "We had some units that we downgraded from 4.1.11 to 4.1.6."

From Tyler to Ken Clark, 15 Feb 1999: "... But then again, with regards to the entire NASED certification process, I can never quite get a handle on the relationship between "ostensible" and "reality."... :-)"

Unknown programmers were putting unlooked-at code into our software. Probably, these programmers are honest, but we really have no idea. Regardless, it is idiotic to put seven million votes into the hands of a few unknown people without even doing a background check.

This problem isn't limited to Diebold, and it isn't just the vendors. County officials may or may not know the implications of using uncertified version numbers, but state officials absolutely know better. Washington State elections director David Elliott said on the Dave Ross radio show that, in Washington State, voting software is certified by ITAs like Wyle. However, Washington has been using versions never certified by an ITA.

Dozens of us went looking for the most recent ITA and NASED certification numbers, and all of us came up empty-handed. Finally, after asking Elliott for the NASED certification list in front of members of the Washington legislature (I did this while giving public testimony, a breach of protocol which mortified the legislators and resulted in a reprimand),[21] I was able to obtain a supposedly complete set of NASED certification documents.

I say "supposedly" because someone took a pen and wrote a version number on it that wasn't there originally. In another case, a version number was overwritten in pen but its approval number was not overwritten, resulting in a mismatch.

I wondered why former Washington Secretary of State Ralph Munro, who is now chairman of VoteHere, signed off on GEMS version 1.11.2. (Or did he?) Why did current Secretary of State Sam Reed sign off on GEMS 1.18.18. (Or did he?) Who's minding the store here, guys?

Here is an e-mail from Dean Logan, former Washington state elections director, now director of King County Records, Elections and Licensing Services:

> *Tuesday, November 25, 2003 From Dean Logan to Andy Stephenson*: "King County currently operates GEMS Software version 1.18.18. This version of the software was installed in August 2003 and was used for the September 16, 2003 Primary and the November 4, 2003 General Election. GEMS Version 1.18.18 was certified by the Washington Secretary of State on August 12, 2003 ... From 1999 through August 2003, King County operated GEMS Software version 1.11.2 ... No additional software patches or upgrades have been installed or in use in King County."

(Neither 1.18.18 nor 1.11.2 had a NASED number.)

> *Wed, 03 Dec 2003 From Bev Harris to David Elliott:* "As I mentioned to you after the meeting, I was astonished when Andy Stephenson, Democratic candidate for Secretary of State, discovered that King County, Washington, has been using uncertified software for four years ... In the case of King County -- perhaps there is some old, obscure NASED document that has never been published, which goes out of order numerically, and which is for some reason missing from the discovery documents obtained for a recent citizen lawsuit?

"You did tell me today that you have the complete set and that you will provide it. I really appreciate your help. Because you sat on the NASED committee for so many years and according to your testimony today, even helped to write the standards, your expertise is quite valuable and therefore I would like to get your signature with the documents indicating that what you provide does represent the 'complete set' of version numbers ..."

Dec 4, 2003 From David Elliott to Bev Harris: " ... I can not offer a 'complete set' of the NASED information although they serve as a continuous log of the work done by the ITA's. The last should provide all that came before it. I have contacted the FEC about whether there is an update to the list past 6/5/03 and I was told that they are working on it."

Dec 4, 2003 From Bev Harris to David Elliott: "Thank you for responding so promptly ... I did not get your response until too late to pick up the documents. But that's okay, because the answer is insufficient and perhaps we can rectify that so that when I pick them up next Tuesday, we will have what we need. Your response raises several questions:

("I have contacted the FEC about whether there is an update to the list past 6/5/03 and I was told that they are working on it.")

"This is not an acceptable answer. In fact, I can't tell whether or not any versions were certified after 6/5/03 or not. Are there any new versions after the June 2003 report, or not? ... I would assume that NASED would have some system to inform the secretary of state when they certify new versions ... why do you have to call the FEC for it?

"I will arrange to come to Olympia by 4:30 p.m. on Tuesday, and at that time I really do need ALL the NASED certified version numbers.

Dec. 8 2003 from David Elliott to Bev Harris: " ... I am providing you with copies of the lists that I have received. ... Concerning the Diebold certifications: The optical scan reader was originally certified as the Global CF-1 in 1991. In 1992 software called Vote Tally System VTS version 1.81 was certified and the hardware was re-named the Accu-vote. The VTS software was rewritten and renamed GEMS and was re-certified in 1998. GEMS was re-examined again in 2001 as a part of the certification of the Accu-vote touch screen (DRE) finalized in September of 2002 as version 1.17.17. The most recent examination was completed in July and August of 2003 for GEMS version 1.18.18."

OK, now we get into some problems. GEMS 1.18.18 was used in two King County elections in violation of Washington state law, since it had not been used in elections elsewhere first. According to Dean Logan, the previous version was GEMS 1.11.2, and there were no upgrades or patches, but this cannot have been certified in 1998, as Elliott implies, because it wasn't released until 1999. [22] And if only 1.11.2 and 1.18.18 were used, and there were no upgrades or patches, why did Sophia Lee reference "GEMS 1.17.16" in King County? [23]

King County has been using unauthorized software for six years. A whole bunch of citizens on the BlackBoxVoting.org forums went after all the state certifications, and mostly got stonewalled, but we did document the following problems:

Chelan County Washington is using GEMS version 1.17.21. Not certified.
King County Washington GEMS 1.11.2, 1.17.16, 1.18.18. Not certified.
Placer County used GEMS version 1.17.20. Not certified.
El Paso County Texas used GEMS version 1.17.21. Not certified.
Johnson County Kansas GEMS version 1.18.14. Not certified.
Alameda County California used GEMS version 1.18.13.9. Not certified.
Alameda County California also used GEMS version 1.18.14. Not certified.
Yavapai County Arizona optical scan version 2.0.11. Not certified.
Pima County Arizona optical scan version 2.0.11. Not certified.
City of Tucson Arizona optical scan version 1.94y. Not certified.
Johnson County Kansas optical scan version 2.00g. Not certified.
Yavapai County Arizona touch screen firmware 4.3.11. Not certified.
Los Angeles County California touch screen version 4.3.8. Not certified.
El Paso touch screen firmware version 4.3.9* Not certified at the time
Alameda County California touch screen firmware 4.3.11. Not certified.
Johnson County Kansas touch screen firmware 4.3.11. Not certified.

On December 16, 2003, the State of California held a certification hearing for the Diebold TSx system. An 18-inch-thick pile of copies containing the material you have just read was marched into the middle of the meeting, and California Secretary of State Kevin Shelley made an unusual personal appearance to express his displeasure. The results of an audit ordered by the California voting-systems panel were equally disturbing:

According to *WiredNews*, "At least five California counties were using versions of software or firmware that were different from what Diebold had indicated they were using. *All* counties were using uncertified software ... Marc Carrel, assistant secretary of state for policy and planning, said he was 'disgusted' by the situation and worried that it could call into question any close races that might have occurred in three counties that used federally unqualified software.

' ... And I'm frustrated ... that we're not going further today,' he said. 'There certainly needs to be something done to this vendor.' " [24]

* * * * *

While California was busy clearing up its unauthorized software, Washington state officials were denying that the problem existed.

Post-Intelligencer reporter Wyatt Buchanan got this answer when he asked for a response to the allegations made in this chapter:

"*Elections officials said the two* [Harris and Stephenson] *had never contacted them about their concerns*." [25]

Well no, I suppose not, unless you count six e-mails, a 20-minute conversation with assistant elections director Paul Miller, a confrontation with David Elliott in front of 12 witnesses outside Senate Room 1 in the Washington state capitol, and testimony before members of the Washington state legislature with Elliot present. Buchanan ran a correction, citing incorrect information given by the office of the secretary of state.

Elliott, the Washington state elections director, told Tacoma News Tribune reporter Aaron Corvin on December 17 that "*all software used in elections has been certified by the state*." [26]

All of it?

OK. Stephenson and I will be picking up the signature pages for those certifications.

* * * * *

After issuing a cease-and-desist for publishing 24 memos documenting the use of unauthorized software, after a California audit revealed that 100 percent of Diebold's machines used uncertified programs and California threatened to revoke the company's right to do business in the state, after dozens of journalists including two documentary film producers and the AP wire covered this story, Diebold

Election Systems President Bob Urosevich released a news statement:

> "Diebold Election Systems, Inc. (DESI), is announcing a complete restructuring of the way the company handles qualification and certification processes for its software, hardware and firmware." [27]

I'm sure someone will slap me for saying this, but I'm reminded of the sociopath who discovers his conscience as soon as he goes to trial.

It wasn't just Diebold. On the Mike Webb radio show, Snohomish County (Washington) Auditor Bob Terwilliger admitted that one of his staff members wrote a program modification for his Sequoia touch-screen software. He said it was for the WinEDS central tabulating software (the Sequoia equivalent of GEMS; this software was also found on an unprotected Internet site during the fall of 2003).

What was this patch for? "Just to help run some reports." But it has to access the votes to do that. "It just uses the database." But the database consists of the votes. "I trust the person who made the changes." [28]

Let's suppose everyone in every jurisdiction is honest. That's not likely, but let's pretend. Here is an incomplete list of the bugs fixed on just one release of the Diebold software:

> From: Whitman Lee, 23 Jan 2003
> - Items are not being recorded in the Audit Log.
> - Connect to Data Base security crack.
> - Ballots printed from Ballot Viewer do not correctly reflect selections.
> - Non-administrator users can assign themselves administrator privileges.
> - Races marked "Not Counted" can be downloaded and appear in reports.
> - Regional users can unset the election's status.
> - No error message is displayed if 'Confirm password' and 'Password' fields don't match.
> - Loading a file from backup results in the backup copy being deleted.
> - Central Count drops a batch if a race on the ballot has headers.
> - LA County Export: Election Id incorrect for Nov. 2002 election.
> - Incorrect IP address displayed on the AccuVote-TS Server console.
> - Resetting election on non-Host database gives "Internal Error".
> - Summary Reports Cards Cast totals are incorrect
> - Incorrectly enabled functions and settings when election status is "Set for Election."

It's bugs like these that get elections wrong. Would you rather