Chapter 7
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

7

The first public look – ever – into a secret voting system

Author and historian Thom Hartmann writes:[1]

> "You'd think in an open democracy that the government – answerable to all its citizens rather than a handful of corporate officers and stockholders – would program, repair, and control the voting machines. You'd think the computers that handle our cherished ballots would be open and their software and programming available for public scrutiny...
>
> You'd be wrong.
>
> If America still is a democratic republic, then We, The People still own our government. And the way our ownership and management of our common government (and its assets) is asserted is through the vote...
>
> Many citizens believe, however, that turning the programming and maintenance of voting over to private, for-profit corporations, answerable only to their owners, officers, and stockholders, puts democracy itself at peril."

* * * * *

Historians will remind us of a concept called "the public commons." Public ownership and public funding of things that are essential to everyone means we get public scrutiny and a say in how things are run.

When you privatize a thing like the vote, strange things happen.

For example, you can't ask any questions.

Jim March, a California Republican, filed a public records request[2] in Alameda County, California, to ask about the voting machines they had entrusted with his vote. The county's reply[3]:

> "Please be advised that the county will not provide the information you requested...The County will not allow access or disclose any information regarding the Diebold election system as any information relating to that system is exempted from the PRA (Public Records Act)...The system provided by Diebold Election Systems Inc. ("DESI") is a proprietary system that is recognized as such in the contract between the County and DESI...
>
> ...The County contends that the official information privilege in section 1040 of the Evidence Code is applicable because the information requested was acquired by the County in confidence and the County is required to maintain its confidentiality. Any copying or disclosing of such information would violate the license agreements..."

When I called ES&S to ask the names of its owners, the company simply declined to take my call.

When former Boca Raton, Florida, mayor Emil Danciu requested that Dr. Rebecca Mercuri, perhaps the best-known expert on electronic voting in America, be allowed to examine the inner workings of Palm Beach County's Sequoia machines, the judge denied the request, ruling that neither Mercuri nor anyone else would be allowed to see the code to render an opinion.[4]

When best-selling author William Rivers Pitt interviewed Dr. David Dill, a professor of computer science at Stanford University, about his experience with voting machines, Pitt got an earful about secrecy:[5]

Dr. Dill says that when he started asking questions, he got answers that made no sense. "It is frustrating because claims are made about these systems, how they are designed, how they work, that, frankly, I don't believe," says Dill. "In some cases, I don't believe it 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."

When members of the California Task Force on Electronic Voting tried to find out how the machines were tested, Wyle and Ciber (the primary "Independent Testing Authorities" – ITAs) declined to answer.

"If you go to their Web pages, it says, 'If you'd like to know something about us, please go to hell' in the nicest possible way."

— Dr. David Dill
Stanford Univ.

"We wanted to know what these ITAs do," said Dill. " So we invited them to speak to us...They refused to come visit us. They were also too busy to join us in a phone conference. Finally, out of frustration, I wrote up ten or fifteen questions and sent it to them via the Secretary of State's office. They didn't feel like answering those questions, either."

If the ITAs won't answer questions, what about the manufacturers? "What testing do the manufacturers do?" asks Dill. "If you go to their web pages, it says, 'If you'd like to know something about us, please go to hell' in the nicest possible way."

* * * * *

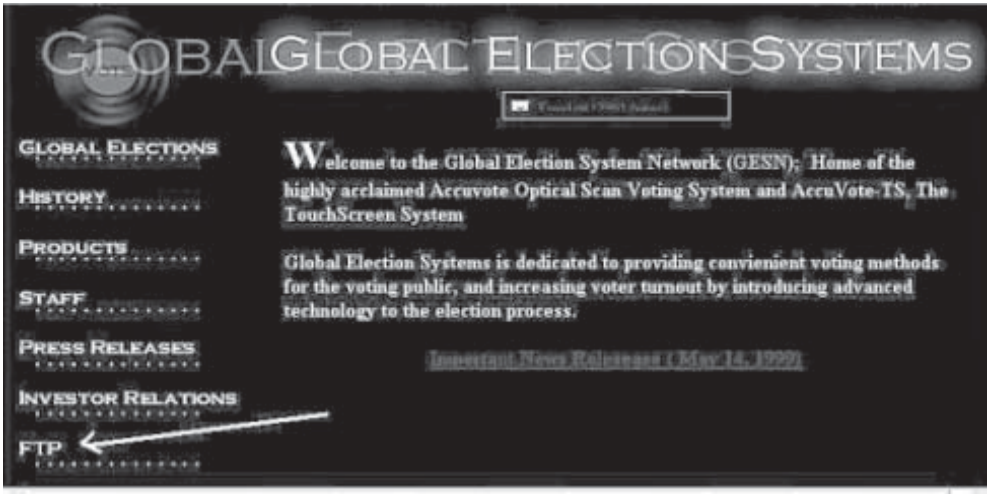
You can't examine a machine or even look at a manual. David Allen, one of the many computer techs who helped coach me through the writing of this book, also happens to be my publisher.

"These things are so secret we're supposed to just guess whether we can trust them," he said. "We've got to get our hands on a technical manual somehow."

I promised him, somewhat doubtfully, that I'd try calling some programmers to see if I could find one to cooperate. I was most interested in ES&S — at that time, I hadn't done much work at all on Diebold Election Systems. I entered "@essvote.com" into the Google search engine, looking for e-mails which might give me names I could contact, and found a few dozen employees who work for ES&S.

I felt cowardly about calling them. What would I say? "Hey, let me see a manual?" So I stalled by convincing myself that I should find as many names as possible. I got some from Sequoia. Then I entered "Global Election Systems" and found some old documents with e-mails ending in "gesn.com."

On page 15 of Google, looking for anything with "gesn" in it, I found a Web page. (You can still find this page at www.archive.org for GESN.com. The FTP link still appears.)



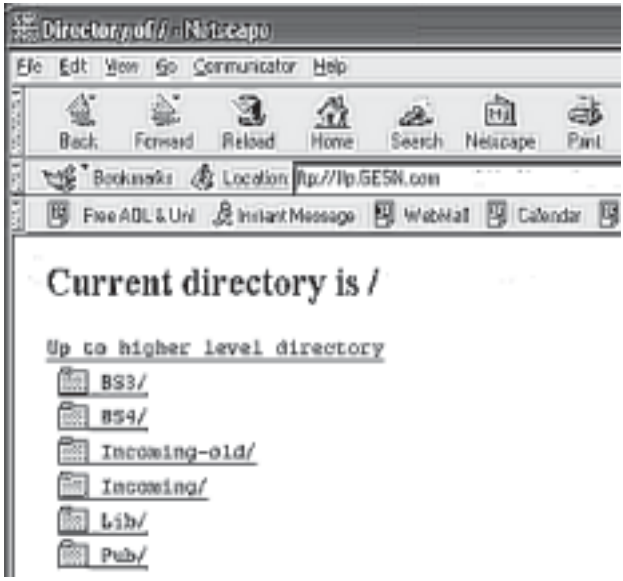
I clicked "press releases" to see what kind of claims this company was making. Then I clicked all the links. I clicked the link called "FTP" and it took me to a page full of files.

I called my publisher, David Allen.

"What am I looking at?"

He took one look at the page and snorted incredulously. "Incredible stupidity."

"Click 'Pub'" he suggested. We did, and began wandering through the files. What follows is the first detailed look — ever — into a secret voting system.



Noun or verb?

What do you do when you find 40,000 secret files on an unprotected file transfer site on the Internet? Probably just look and go away. But what if you have pledged allegiance to the United States, and to the republic for which it stands?

What if you knew that the devil went down to Georgia on Nov. 5, 2002, and handed that state an election with six upsets, tossing triple-amputee war veteran Max Cleland out of the U.S. senate in favor of a candidate who ran ads calling Cleland unpatriotic? Suppose you knew that in Georgia, the first Republican governor in 134 years had been elected despite being behind in every poll, and that African American candidates fared poorly even in their own districts? Knowing this, suppose you saw a file called "rob-georgia," looked inside, and found instructions to replace the Georgia voting program files with something unknown.

I don't know about you, but I'm a 52-year old grandma and I never expected to have to make a choice like this. I wanted someone else to take care of it. *We need investigators like Woodward and Bernstein*, I thought, so I called the *Washington Post*. Of course, Carl Bernstein isn't there any more, but I left a spicy message on Bob Woodward's voicemail. Never heard from anyone. I learned that *Washington Post* reporter Dan Keating was doing a story on voting machines, so I called him.

"So, will you call Diebold and find out what 'rob-georgia' is?" I asked.

"No."

"Why not?"

"Because I don't think 'rob-georgia' could possibly mean rob Georgia," he said.

I left a somewhat more agitated message on Bob Woodward's voicemail and submitted my experience to a Web site called *Media Whores Online*.

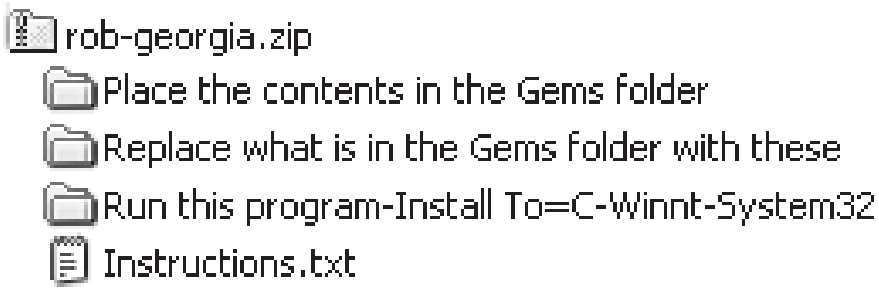
These files might contain evidence. These files might go away. I called people in various places around the world and urged them to go look at rob-georgia. I thought long and hard. And then I downloaded the files, all 40,000 of them. It took 44 hours nonstop. I gave them to someone I trust, who put them in a safe deposit box, and there they sit to this day.

Why in the world would an ATM manufacturer like Diebold leave sensitive files hanging out there on an unprotected Internet site? I made a few phone calls, which confirmed that Diebold *knew* the site was unprotected, and found out that the site had been there for years. (See appendix for interviews with Guy Lancaster, Josh Gardner and Kerry Martin.)

I kept asking if anyone knew who Rob was. Everyone told me there was no employee named Rob in Georgia.

Perhaps rob was a verb?

"rob-georgia" is a zip file with whole bunch more files inside it. It seems to be some sort of a program modification, which is a great way to slip any damn thing you want into a voting machine without anybody noticing. Here's what I saw when I clicked it:



Why did they replace voting machine stuff? *Did* they replace voting machine files? Googling around with various "Georgia, voting machine, Diebold" search words, here's what popped out:

> ***16 Sep 2002*** **Memo** from Chris Riggall (press secretary for Georgia Secretary of State Cathy Cox): "Diebold programmers developed a patch which was applied to the units deployed in Hall and Marion counties, and we were pleased that not one freeze was reported among the tens of thousands of votes cast there. Unfortunately, we simply did not have the time to apply the patch to the demo units, but that is now occurring to all units in all counties and the last increment of shipments from Diebold had this fix loaded before leaving the factory."[6]

A program modification was needed because the touch screens were freezing up, crashing the machines. Makes sense. The problem must be a big one to justify modifying the progam on all 22,000 voting machines in Georgia. But wait a minute —

"*Before being considered for acquisition in Georgia,*" states the Media Backgrounder put out by the Georgia Secretary of State Press Office, [7] "*...software is examined for reliability and hardware is subjected to a variety of 'torture tests.' The state testing examines both hardware and software for accuracy and reliability, and mock elections are conducted on the equipment, witnessed by county election officials.*" The document names Wyle Laboratories and Ciber, Inc., citing their "extensive experience in NASA-related testing."

So how did these NASA-testing labs miss something so obvious that all 22,000 voting machines had to have a program modification to keep them from crashing?

"*It is Diebold Election Systems, Inc. policy that the only acceptable level of conformance is Zero Defects,*"[8] Diebold wrote to certifier Wyle Laboratories in its latest touch-screen certification documents. Okay, we all know that 'zero defects' is one of those terms that sounds good and doesn't happen. But we ought to at least hold Diebold to this: *"The manufacturing test location, test date, and inspector initials will be recorded on a label on every voting machine."*

Whose initials, from the factory, are on the Georgia machines? Anyone's?

In its RFP soliciting purchase by the state of Georgia, Diebold submitted the following in its "Schedule for Deployment": [9]

"*Prior to our GEMS™ hardware installation at each Georgia county, the hardware will be staged in McKinney, Texas for software integration and testing.*"

1. Hardware testing: Wyle Labs
2. Software testing: Ciber Inc.
3. Every machine tested at Diebold factories
4. Rigorous testing on arrival at the Georgia warehouse
5. Testing when delivered to each of Georgia's 159 counties

As part of the installation process, Diebold promised that all software and drivers (small programs which "drive" specific pieces of hardware such as printers, touch-screens, modems) would be loaded prior to being shipped to Georgia. and according to the Georgia Secretary of State Media Backgrounder:

"*Before leaving the factory, <u>each</u> touch screen terminal receives a diagnostic test.*"

If they "staged the hardware" and did software integration and testing and loaded everything and then tested each voting machine before shipping it to Georgia, why did every one of the machines need modifications, in order not to crash, *after* they reached Georgia?

The machines were shipped to Georgia in June 2002. And once they arrived, we are told, there was more testing:

"*Upon arrival at Diebold's central warehouse in Atlanta, each unit was put through a diagnostic sequence to test a variety of functions, including the card reader, serial port, printer, the internal clock and the calibration of the touch screen itself. These tests were audited by experts from Kennesaw State University's Center for Election Systems.*" This statement, on Georgia Secretary of State letterhead, remains posted on the state's Web site as of the writing of this book.

"*After shipment to each of Georgia's 159 counties, county acceptance testing (which consists of the same types of diagnostic procedures) was performed by KSU staff on each voting terminal.*"

Was this testing rigorous? Yes, rigorous, they promised. According to the Media Backgrounder: "*Georgia's multi-tiered election equipment testing program, among the most rigorous in the nation.*"

Could someone take a moment to do the math with me? If this testing is "rigorous," might we expect them to invest, say, 10 minutes per machine?

The testing described by Diebold and Secretary of State documents adds up to every touch screen unit being tested three times *before* it gets to the renowned "logic and accuracy" test.

> **22,000** machines x **10** minutes = **220,000** minutes
>
> **220,000** minutes x **3** times = **660,000** minutes.
>
> Divide by **60** minutes = **11,000** hours.
>
> Divide by **40**-hour work week = **275** work weeks, or **68** months
>
> **68** months divided by **12** = **5.7** years
>
> Amount of time available for acceptance testing: **4** months
>
> **NOW ADD PEOPLE:**
>
> **68** months divided by **4** = **17** people working **40** hours per week for **4** months doing nothing but rigorous testing.

Do you believe they did all the testing they claim to have done? Call me a skeptic. I want to see the payroll records on that.

What does all that modifying at the last minute do to security? Wait — don't program modifications need to be recertified? How many people had to get access to these machines to do this? Was this legal?

And what exactly was in rob-georgia.zip?

With so many unanswered questions, we decided to ask the public officials responsible for voting systems in the state of Georgia about these program modifications.

Feb. 11 2003: Interview with Michael Barnes, Assistant Director of Elections for the state of Georgia:[10]

Harris: "I want to ask you about the program update that was done on all the machines shortly before the election."

Barnes: "All right."

Harris: "Was that patch certified?"

Barnes: "Yes."

Harris: "By whom?"

Barnes: "Before we put anything on our equipment we run through state certification labs, and then, in addition to that, we forwarded the patch to Wyle labs in Huntsville ... Wyle said it did not affect the certification elements. So it did not need to be certified."

Harris: "Where's the written report from Wyle on that? Can I have a copy?"

Barnes: "I'd have to look for it I don't know if there was ever a written report by Wyle. It might have been by phone. Also, in Georgia we test independently at Kennesaw University — a state university."

Harris: "Can I see that report?"

Barnes: "You'd have to talk to Dr. Williams, and he's out of town. He's in Lincoln. Dr. Williams is on the National Association of State Election Directors (NASED) certification, and I think he's also at Kennesaw University. He does the certification for the State of Georgia."

Harris: "Was this new patch tested with a Logic and Accuracy test, or was it tested by looking at the code line by line?"

Barnes: "Logic and Accuracy, and also they verify that our version is identical and also any software is tested through Ciber and Wyle."

Harris: "But Wyle decided not to test the patch, you say. Was this patch put on all the machines or just some of the machines?"

Barnes: “All the machines.”

Harris: “So every machine in Georgia got this program update.”

Barnes: “Yes, every one of the machines used on election day in November. If it had been sent out to counties prior already, Diebold and their technicians went out and manually touched every machine. Some of the machines were still at the manufacturer, they did the patches on those.”

Harris: “How long did it take to do patches on — what was it, around 22,000 machines?”

Barnes: “It took about a month to go back out and touch the systems.”

Harris: “Can you tell me about the procedure used to install the patches?”

Barnes: “The actual installation was a matter of putting in a new memory card. [memory card: like a floppy disk, but shaped like a credit card. Sometimes called PCMCIA card.] It took about one and a half minutes to boot up... [discussion of slots and memory cards]. They take the PCMCIA card, install it, and in the booting-up process the upgrade is installed.”

Harris: “Where did the actual cards come from?”

Barnes: “Diebold gave a physical card — one card that activates each machine. There were about 20 teams of technicians. They line the machines up, install the card, turn on, boot up, take that card out, move on, then test the machine.”

Harris: “Were people driving around the state putting the patches on the machines?”

Barnes: “Yes.”

Harris: “What comment do you have on the unprotected FTP site?”

Barnes: “That FTP site did not affect us in any way shape or form because we did not do any file transferring from it. None of the servers ever connected so no one could have trans-

ferred files from it. No files were transferred relating to state elections."

Harris: "How do you know that no one pulled files from the FTP site?"

Barnes: "One voting machine calls the servers and uploads the info. We don't allow the counties to hook up their servers to a network line."

Harris: "I notice that one of the things the network builder put on the [county] machines was a modem."

Barnes: "The only time you use the modem is on election night. That is the only time the unit was used, was election night when they plug it into the phone...[details on preparation of vote databases]"

Harris: "Having the screens freeze up is a pretty severe error — how did 5% of the machines get out of the factory with that? How did they get through Wyle testing labs?"

Barnes: "All I know is that the machines were repaired."

Harris: "How do you know that the software in the machines is what was certified at the labs?"

Barnes: "There is a build date and a version number that you can verify. Kennesaw University did an extensive audit of the signature feature — Dr. Williams and his team went out and tested every machine afterwards to make sure nothing was installed on them that shouldn't have been."

Harris: "They tested every one of 22,000 machines?"

Barnes: "They did a random sampling."

Feb. 12 2003: Interview with Dr. Britain Williams, Kennesaw Election Center, an organization funded by the Georgia Secretary of State.[11]

Harris: "I have questions regarding your certification of the machines used in Georgia during the last election."

Dr. Williams: "For the state of Georgia — I don't do certifica-

tion. The law gives the Secretary of State the authority to say what systems are certified and what are not. What I do is an evaluation of the system...[details on certification]"

Harris: "What was your involvement in certifying the program patch that was put on? Did you actually certify the patch, or did you determine that it was not necessary?"

Dr. Williams: "Part of our testing program is when these machines are delivered, we look at the machines and see that they comply. And in the process of doing that — representatives of Kennesaw University did this — we found about 4-5 percent of the machines were rejected, not all because of screen freezes, but that was one of the problems."

Harris: "It was the screen freezes that caused them to issue a program patch?"

Dr. Williams: "Yes. The vendor [Diebold] created a patch addressing the screen freezing. It made it better but didn't completely alleviate the problem."

Harris: "Did you do a line-by-line examination of the original source code?"

Dr. Williams: "For the original — no. We don't look at the source code anyway; that's something done by the federal ITAs."

Harris: "Did you do a line-by-line examination of the patch?"

Dr. Williams: "The patch was to the operating system, not to the program *per se*."

Harris: "It only changed Windows files? Do you know that it didn't change anything in the other program? Did you examine that?"

Dr. Williams: "We were assured by the vendor that the patch did not impact any of the things that we had previously tested on the machine."

Harris: "Did anyone look at what was contained in the replacement files?"

Dr. Williams: “We don’t look at source code on the operating system anyway. On our level we don’t look at the source code; that’s the federal certification labs that do that.”

Harris: “Did you issue a written report to the Secretary of State indicating that it was not necessary to look at the patch?”

Dr. Williams: “It was informal — not a report — we were in the heat of trying to get an election off the ground. A lot was done by e-mails.”

Harris: “What month did you install that program patch?”

Dr. Williams: “When we took delivery, we were seeing that the patch was on there.”

Harris: “I have a memo from the Secretary of State’s office that is dated in August [Sept. 16, actually], and it says that due to a problem with the screens freezing, a patch was going to be put on all the machines in Georgia. It references a Rebecca Mercuri report..[Dr. Williams discusses Dr. Mercuri]”

Harris: “...Apparently, someone had already taken delivery on these machines and they had already been shipped out around the state before the patch was applied, is that right?”

Dr. Williams: “The patches were done while we were doing acceptance testing. One of the things we looked for during acceptance testing was to make sure the patch was put in.”

Harris: “But as I understand it, a team of people went around the state putting these patches on.”

Dr. Williams: “By the time they put the patches in, the majority of the machines had been delivered. Actually, it was going on at the same time. When they started putting the patches in around the state, we tested the machines where they did that [put the patches in] at the factory.”

Harris: “When I spoke with Michael Barnes, he said that you tested all the machines, or a random sampling of the machines, after the patch was put on.”

Dr. Williams: “We had five or six teams of people with a test

script that they ran on each machine —"

Harris: "The test script did what?"

Dr. Williams: "The test script was generic. It was in two parts. One part tested the functionality of the machine. It was a hardware diagnostic; it primarily tested that the printer worked, that the serial port worked, that the card reader worked, tested the date and time in the machine, and to an extent checked calibration of the machine. Then if it passed all of those, it tested the election. We loaded a small sample election in, the same as the one used during certification testing, and we ran a pattern of votes on there."

Harris: "You mean a Logic and Accuracy test?"

Dr. Williams: "Yes. A little miniature election. If the machine passed, we wrote it up and sent the report back to the office. If it failed — if it froze up or there were other failures, and there were some of those, like the card reader was broken or the case was broken — then we didn't pass it."

Harris: "Can you tell me about the digital signature?" [A digital signature is used to show that no changes in the software were done.]

Dr. Williams: "That's part of the test that involves looking at the software — putting the patch on wouldn't change the digital signature."

Harris: "But if you put in a program patch, wouldn't that show that a change has been made?"

Dr. Williams: "No, because the patch was only in the Windows portion — there was no digital signature check on the operating system..."

[discussion of how a digital signature works]

Dr. Williams: "They write the source code and the source code is submitted to the federal lab. When it passes the lab they freeze the source code; at that point it's archived. Any change after that is subject to retesting."

Harris: "What was the security around the creation of the

cards used to implement the patch?"

Dr. Williams: "That's a real good question. Like I say, we were in the heat of the election. Some of the things we did, we probably compromised security a little bit. Let me emphasize, we've gone back since the election and done extensive testing on all this."

Harris: "Based on your knowledge of what that patch did, would it have been needed for all the machines of same make, model and program? Including machines sold to Maryland and Kansas that were built and shipped around the same time?"

Dr. Williams: "Yeah, but now the key phrase is with the 'same system.' Maryland ran a similar version with a different version of Windows and did not have this problem."

Harris: "So the program was certified by the federal labs even when it ran on different versions of the operating system?"

Dr. Williams: "Yes, they don't go into the operating system."

Harris: "There was an unprotected FTP site which contained software and hardware specifications, some source code and lots of files. One file on that site was called "rob-georgia" and this file contained files with instructions to 'replace GEMS files with these' and 'replace Windows files with these and run program.' Does this concern you?"

Dr. Williams: "I'm not familiar with that FTP site."

Harris: "Is there a utility which reports the signature? Who checks this, and how close to Election Day?"

Dr. Williams "We do that when we do acceptance testing. That would be before election testing."

Harris: "What way would there be to make sure nothing had changed between the time that you took delivery and the election?"

Dr. Williams: "Well there wouldn't — there's no way that you can be absolutely sure that nothing has changed."

Harris: "Wouldn't it help to check that digital signature, or checksum, or whatever, right before the election?"

Dr. Williams: "Well, that is outside of the scope of what some of the people there can do. I can't think of any way anyone could come in and replace those files before the election —"

Harris: "Since no one at the state level looks at the source code, if the federal lab doesn't examine the source code line by line, we have a problem, wouldn't you agree?"

Dr. Williams: "Yes. But wait a minute — I feel you are going to write a conspiracy article."

Harris: "What I'm looking at is the security of the system itself — specifically, what procedures are in place to make sure an insider cannot insert malicious code into the system."

Dr. Williams: "There are external procedures involved that prevent that."

Harris: "This is exactly what I want to know. If you know what procedures would prevent that, could you explain them to me?"

Dr. Williams "We have the source code. How can they prevent us from reviewing it? I have copies of source code that I've certified."

Harris: "But you said you do not examine the source code."

Dr. Williams: "Yes, but the ITA did it. The ITA, when they finish certifying the system, I get it from the ITA — someone would have to tamper with the source code before it goes to the ITA and the ITA would have to not catch it."

Of course, they just told us that the ITA never examined the program modifications made to 22,000 machines in Georgia.

Let's consider a few points here:

1. Tiny programs can be added to any program modification. The file "Setup.exe" launches many of these, some of which are ".dll" files, which stands for "dynamic link libary." These are small files that hide inside executable programs and can launch various functions (whatever the programmer tells them to do.) They can be set up to delay their launch until a triggering event occurs. There is nothing wrong with .dll files, but there is something very wrong with putting new.dll files into a voting machine if no one has examined them.

Other files, such as "nk.bin," also contain executables that can literally rewrite the way the system works. The nk.bin file is sort of like a mini-Windows operating system. If a programmer from Diebold modifies the nk.bin file and these modified files are put on the voting machine without being examined, the truth is, we have no idea what that machine is doing.

Also, any time you do a program modification, you can introduce a small trojan horse or virus that can corrupt the election.

(Hey! What's *this*?)

ClockFix.zip

2. The rob-georgia.zip folder includes a file called "setup.exe" that was never examined by certifiers. It contains many .dll files. The "clockfix" zip file is an nk.bin file. Someone should have looked at these.

3. Windows operating system: In order to use "COTS" software (Commercial Off The Shelf) without having certifiers examine it, the commercial software must be used "as is", with no modifications. If the patches that Barnes and Williams referred to were Windows patches, the moment Diebold modified them they became subject to certification. They did not come from Microsoft. They came directly from Diebold. Therefore, they were not "as is, off the shelf." Someone should have looked at these, too.

4. The rob-georgia.zip file contains two folders full of files that are not for Windows. GEMS is not part of the Windows operating system. You don't need to be a computer scientist to see this: Just look at the file names, which instruct the user to alter the GEMS program. Someone should have looked at these.

5. According to Dr. Williams, no one at the state level looked at these modifications, and according to Michael Barnes, no one at the national level looked at

them, either. In fact, no one has any idea what was on those Georgia voting machines on Nov. 5, 2002.

Georgia certified an illegal election. Now what?

* * * * *

As word spread about voting machine files found on an open FTP site, it became a favorite topic of conversation on internet discussion forums...

"This could make Watergate look like a game of tiddlywinks... Get a good seat. This could be quite a long ride!"

— TruthIsAll

Best disinfectant for secret vote-counting: Sunlight

Public examination of those files is the best thing that could have happened. It's the only way we can engage in an informed debate about voting machines.

I'm glad we got a look inside, but what we found was shocking. What you are about to read should divest you once and for all of the idea that we can "trust" secret voting systems created by corporations.

The Diebold FTP site contained computer files for systems marketed by Diebold Election Systems and, before that, Global Election Systems. These voting systems were used in real elections.

There is no reason to believe that other manufacturers, such as ES&S and Sequoia, are any better than Diebold — in fact, one of the founders of the original

Trust us: Here is the official statement from Diebold, issued by fax on Feb. 19, 2003:[14]

"The old Global Election Systems site has been taken down because it contained old, out-of-date material."

The facts: According to whois.sc, the site was actually owned by Diebold, and this "old" site had been taken down only days earlier, and some of its "old" files were date-stamped just three weeks before Diebold issued this statement.

ES&S system, Bob Urosevich, also oversaw development of the original software now used by Diebold Election Systems.

Because voting systems (except AccuPoll[13], which is open source) are kept secret, I am focusing on Diebold in the next several chapters only because we can't find out anything about the other vendors' systems.

"r o b - g e o r g i a . z i p ? Anonymous FTP access? LOL, unbelievable! This is beyond ridiculous, these people couldn't be trusted to secure your granny's system!"

— quimby

We do know that, according to internal memos from Diebold employees, ES&S was said to have a patent lawsuit pending against Diebold predecessor Global Election Systems at one time[13a]. That is not surprising, because ES&S founder Bob Urosevich brought technology over to Global Election Systems. If a patent lawsuit was filed, that would indicate that some part of the system was alleged to be identical. Also, Chapter 2 shows that Diebold, Sequoia and ES&S have all miscounted elections many times.

A word about "open source"

Very reputable programs, such as the Linux operating system, have been developed through "open source," letting the whole world examine the system and suggest improvements. Some advocates confuse what happened with Diebold's unprotected FTP site with open source. What Diebold did, though, is quite different.

If you never obtain public feedback to improve your software, what you have is horrific security, not an open source system. Hundreds of people have by now examined the Diebold files, but it's still not open source because no one has the slightest idea what Diebold has done to correct the flaws, if anything.

If the Diebold system had allowed everyone with expertise in security, encryption, hacking and database design to critique the software during development and then showed how it corrected the flaws, that would be open source. Such a procedure would no doubt arrive at a very simple and secure program with a voter-verified paper ballot to back it up. Australia has developed an open source voting program, and so has AccuPoll.

Instead, Diebold allowed only a small handful of programmers to look at its software. Then they put all the software (along with passwords and encryption keys) on an open Web site and left it there for several years, where crackers could download it, and people interested in elections could find out about it, but respectable experts and citizens groups were not told of its existence or allowed to examine anything.

I'm glad the files became available, but putting that kind of material on an unprotected Web site was "a major security stuff-up by anyone's reckoning."[12] That's how Thomas C. Greene, of *The Register*, describes what Diebold did, and he's right. Diebold's entire secret election system was available to any hacker with a laptop.

Did leaving these files on an unprotected Web site jeopardize elections?

Yes. If your elections officials tell you they still trust the system, give them a copy of this book. They were never made aware of the risks. Your congressperson may be equally unaware. In fact, well-meaning, election supervisors and congressmen generally know diddly about C++ programming, Microsoft Windows code or remote-access security. Even if they looked at the source code (which they are prohibited from doing), they don't have the expertise to evaluate it.

Trust us: "There's so many checks and balances in this process." — Linda H. Lamone

Maryland State Elections Board[15]

The facts: Poll-worker training won't compensate for insecure or flawed computer programs.

They trust the system because they think that someone else is minding the store — secretaries of state, for example, or state election directors. But none of that makes any difference if the innards of your voting system, including the passwords, IP information and modem configurations have been available to crackers for six years.

As you'll see, our certification system is fundamentally broken. The system is secret, relies on a few cronies and is accountable to no one. Worse, the certifiers have clearly given a passing grade to

software so flawed that it miscounts, loses votes and invites people to come in the back door to make illicit changes to anything they want. But even this inadequate certification system would be better than what we discovered is really happening:

"Are you serious? Please tell me you're not serious here?"

— DEMActivist

Diebold has been using software directly off its FTP site, without submitting it for certification at all.

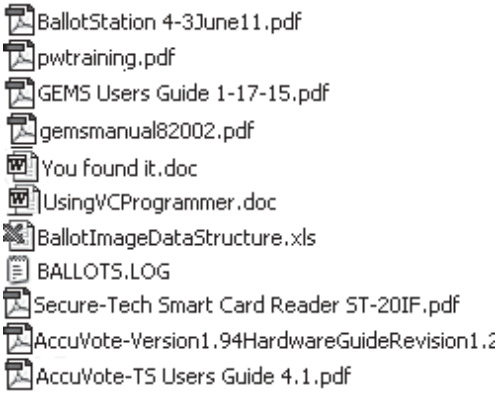
What a cracker could do with the files on the FTP site

If you want to tamper with an election through electronic voting machines, you want to play with:

Ballot configuration — Switch the position of candidates. A vote for one candidate goes to the other. This would be useful in precincts that favor one party or candidate over another.

Vote recording — Record votes electronically for the wrong candidate, or stuff the electronic ballot box.

Vote tallying — Incorrectly add up the votes, or substitute a bogus vote tally for the real one, or change the vote tally while it is being counted.



You'd want to find out as much as you could about procedures. No problem — the Web site contained the Ballot Station user manual, the Poll Worker Training Guide and at least two versions of the GEMS User Manual, along with the Voter Card Programming manual and hardware configuration manuals for the AccuVote touch screen system.

The "Technical Data Package" for the new AccuVote TSx system contains details on procedures and security measures (take with a grain of salt).

* * * * *

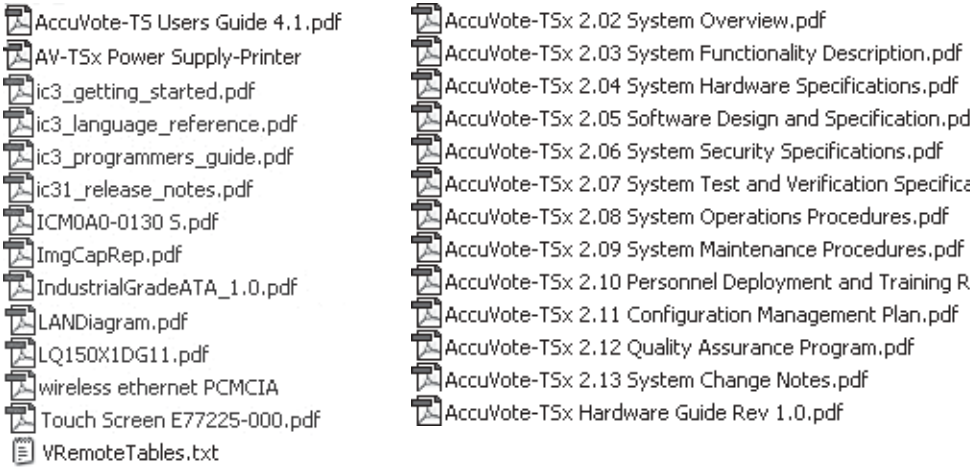
It would be helpful to play with elections in the comfort of your own home. Not a problem — full installation versions of almost all of the Diebold voting programs were on the Web site.

• **BallotStation.exe** (vote recording and precinct tallying, found in the BS folders)

• **GEMS.exe** (county-level tallying of all the precincts, found in the GEMS folders)

• **VCProgrammer.exe** (programs to sign in and validate voter cards)

Just about every version of the Diebold programs ever certified (and hundreds that were never certified) were available.



"You cannot build an idiot-proof voting system because idiots are so ingenious."

— ctdonath2

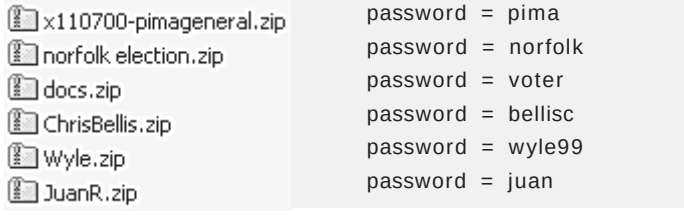
You'd want to know how to use the programs, so besides having all the installation and user manuals, all the "readme" files were available too.

It might be helpful also to know what kind of testing the voting system goes through, especially the details on the highly touted "Logic and Accuracy" testing done right before and after the election. After all, you'd want to make sure that whatever you do doesn't get caught. Not only testing procedures, but testing samples and instructions on how to do the testing were also provided on the Diebold FTP site.

You'd want to see some typical ballot configurations — or, better yet, get the data files created for actual elections. That way you'd know the positioning of the candidates on the ballot, and you could even get the candidate I.D. number used by the computers to assign votes. You could do test runs using real election files.

On the FTP site were files designated for counties in California, Maryland, Arizona, Kentucky, Colorado, Texas, Georgia, North Carolina, Kansas and Virginia. Some files, like one for San Luis Obispo County, California, were date-stamped on an election day (curiously, five hours before the polls closed).

The Diebold easy password method:



Guessing passwords is easy. Many files are named for Diebold employees, and many passwords are just employee names.

The supervisor password for voting machines at the polling place was “1111.” When I saw this in the manual, it reminded me of buying a new briefcase. It comes with a "default" combination, but of course you change the combination as soon as you start using the briefcase.

1. Insert the Manager card into the card reader.
2. Enter the password 1,1,1,1,and touch “OK”.
3. Remove card when instructed.
4. When the screen below appears, press the “End Election” button.

For some reason, Diebold’s voting machines were less secure than your briefcase. That’s because programmers hard-wired the password into the source code. That way, no one could change the password and anyone inside the polling place (the janitor, a crooked politician) could pretend to be a supervisor by entering "1111".

In case you need a fancy password, the files called “passwd” might come in handy. I don’t know if anyone found a use for the Diebold programmer passwords, but these were sitting there.

passwd

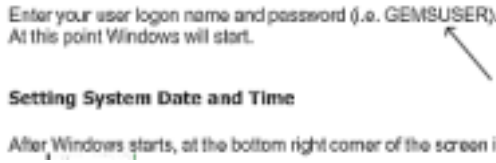
```
ken:Cx4JrK4Q4uebk
guy:APHmbSVeB5WQ6
tri:GwbsAUF5TlQ9Q
whitman:KnSetwE/DYtWM
nel:f1S7xcsCmmxBU
mike:X5oEayCP1CxN.
tomg:h8skrG2aFiuqg
bill:6bFseyII9RxVY
guest:cZm8UJv9sgzyc
```

passwd~

```
ken:Cx4JrK4Q4uebk
tri:UEGNh.UaiLRQk
dmitry:dyNCBKljMDVDU
whitman:g8PfNAeGd9Ao6
kponti:b/tlxLF5aVUVE
denisel:b/tlxLF5aVUVE
ataa:b/tlxLF5aVUVE
josh:ZHwPOhd5is3JE
```

At the county election supervisor’s office, the results from all the polling places are tabulated using a program called GEMS and the password was in the user manual.

The election supervisor can change “GEMSUSER,” but later I’ll show you how even a ten year-old could change it right back.



The password for the GEMS program is "GEMSUSER"

Supervisor access at the polling place is granted by the password 1111. Instead of allowing supervisors to control the password, it is written into the source code and printed in the manuals.

```
{
        //{{AFX_DATA_INIT(CSmartCardEmuDlg)
        m_ByAccLevel = '0';
        m_ID = _T("01234567890");
        m_Level1 = 1;
        m_Level2 = -1;
        m_Level3 = -1;
        m_Party = -1;
        m_PIN = _T("1111");
        m_Type = VOTER_CARD;
        //}}AFX_DATA_INIT
}
```

```
== ADMIN_CARD)) {
                    st = VC_NOACCESS;
              } else {
                    CVoterInfo writeVoterInfo;
                    writeVoterInfo.m_CardType = VOTER_CARD;
                    writeVoterInfo.m_Version = VCI_VERSION1;
                    writeVoterInfo.m_ElectionKey = pVCardInfo->m_ElectionId;
                    writeVoterInfo.m_VCenter = CVCenter(pVCardInfo->m_VCenterId);
                    writeVoterInfo.m_DLVersion = pVCardInfo->m_DLVersion;
                    writeVoterInfo.m_Reportunit = CDistrict(pVCardInfo->m_PrecinctId);
                    writeVoterInfo.m_Baseunit = CBaseunit(pVCardInfo->m_PortionId);
                    writeVoterInfo.m_CounterGroup = CCounterGroup(pVCardInfo->m_GroupId);
                    writeVoterInfo.m_VGroup1 = CVGroup(pVCardInfo->m_VGroup1Id);
                    writeVoterInfo.m_VGroup2 = CVGroup(pVCardInfo->m_VGroup2Id);
                    strcpy(writeVoterInfo.m_PIN, "1111");
                    strcpy(writeVoterInfo.m_Description, "");
                    writeVoterInfo.m_Flags1 = (UCHAR)((pVCardInfo->m_Flags & 0x07) |
NEWTYPE_CARD);
                    writeVoterInfo.m_Flags2 = (USHORT)(pVCardInfo->m_Flags >> 4);
                    writeVoterInfo.m_VoterSN = pVCardInfo->m_VoterId;

                    if (m_CardReader.Write(writeVoterInfo) != SMC_OK)
                          st = VC_FAILEDWRITE;
                    else
                          st = VC_OKAY;
              }
        }
        if (m_CardReader.IsOpen()) {
```

Perhaps we should run some elections.

A cracker who wants to pretend he is the county elections supervisor might start by installing one of the GEMS vote-tallying programs on his home computer. GEMS is on the central computer at the county elections office. This is the software that creates the ballots before the election, and it also tabulates the incoming votes from the polling place when the polls close. The same GEMS program handles both touch screens and optical-scan machines.

If you were to select any of the many vote databases tagged to cities or counties, you could practice tampering with elections using real software and real vote databases.

Any computer that has Windows seems to work, but meticulous people would follow the instructions left on the FTP site and put the GEMS program on a Dell PC with Windows NT 2k installed.

So many versions of the GEMS program, so little time. A good version to start with would be GEMS 1.17.17 — according to NASED documents posted on the Internet by The Election Center, that was the officially certified version of GEMS during the general election in November 2002.

A folder called “Pima Upgrade” might be a good choice for a hacker living in Tucson, and the new 1.18 series was also available. An even newer program,

version 1.19, was put on the FTP site on January 26, 2003, just three days before it was taken down.

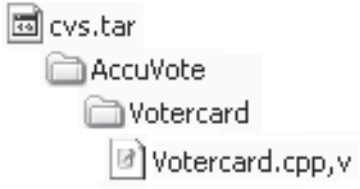
Faking your own touch screen machine

Suppose you wanted to simulate an actual touch screen voting machine. You need to activate those with a smart card, and the average desktop computer isn't set up for that. Put the word "votercard" into a text search on the Diebold files, and this pops up in a file called "votercard.cpp,v"

```
v3-10-19:1.5
v3-10-18:1.5
b1-1-3-votercard-hack:1.5.0.4
v3-10-17:1.5
v3-10-16:1.5
```

Well...what the heck is this file? What kind of file is a "cpp?"

The suffix "cpp" stands for "C++," and these files are source code. "Source code" contains the commands given to the computer that tell it how to execute the program. Many people are surprised to learn that source code files consist of English-like programming commands that people can read. After software engineers write the program, in this case in C++ language, it is then compiled to make it machine-readable.



The cvs.tar file that Diebold left on its Web site was a source code "tree" for the program used to cast votes on touch screens. The tree contains more than program commands; it includes the history of Diebold's software development process, going back all the way back to Bob Urosevich's original company, I-Mark Systems, through Global Election Systems, and including 2002 programming under Diebold Election Systems.

The Votercard.cpp,v, file is found in a directory called Votercard, in a cvs.tar directory called AccuVote.

Now, if I'm a cracker and I get the "Votercard.cpp,v" file off the Diebold Web site, and I'm running a computer that really isn't a voting machine but want to figure out how it works, here it is: a neat little program that can cancel out the card reader entirely. Diebold handed me the road map and helped me find it by naming it "votercard-hack." Any moderately skilled programmer will know how to paste it into the latest touch screen source code, recompile, install, and start playing around.

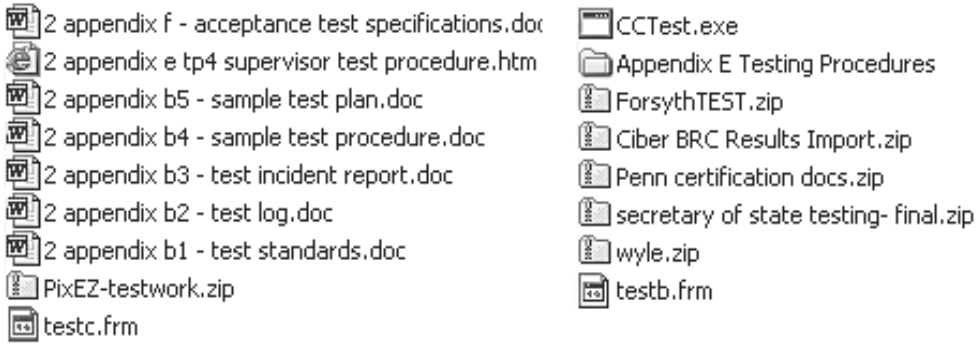
"Votercard-hack" takes you straight to the source code commands you need:

Leaving other people's pants unzipped

It's bad enough when you leave your own sensitive stuff on the Web. But Diebold exposed other people's confidential information, also. Diebold left 15,900 of Microsoft's proprietary Windows CE source code files on its public web site, ready to assemble like a set of legos.

The Microsoft Windows CE Platform Builder is a set of development tools for building a Windows CE operating system into customized gadgets. You are supposed to have a license to use it, and, according to Bill Cullinan of Venturcom Inc., a Waltham, Massachussetts-based Windows CE distributor and developer, the kit is certainly not free.

"The Platform Builder development kit for the new Windows CE .net runs about $995," he told me. "Earlier, the cost was up over $2,000."



"Stupid or evil?"
Though many companies maintain FTP sites, not many I am aware of store source code and customer files in plain sight.
— Atraides

Any cracker in the world could access the pricey Microsoft developer's platforms through the Diebold FTP site.

Despite a notice that says, "You may not copy the [Hewlett Packard] Software onto any public network,"copies of the Hewlett Packard software were on the public FTP site hosted by Diebold.

A document marked "Intel Confidential" pertaining to microprocessor development for personal PCs was on the FTP site, along with the Merlin PPC Sourcekit for personal PCs and the Intel Cotulla development kit, and board support packages for Microsoft Windows CE .NET and PocketPC 2002.

So, Diebold expects us to trust them with our vote, yet they are quite cavalier with other people's intellectual property and, as we will see in the next section, with people's personal information.

Parked on the Diebold FTP site: Private info on 310,000 Texans

Johnny May, perhaps the nation's leading expert on identity theft, has sobering information for you about the Internet and your security. Identity thieves can work anonymously from anywhere in the world and, armed with your social secu-

rity number and a few other details, can quite literally ruin your life. And all they need is your name, address and birthday to get your Social Security number.[16]

The files on the FTP site were a hodge-podge. During the writing of this chapter, I tried to take a more complete inventory.

Tucked into one folder, buried about three-deep in the directories, was a file that contained personal information for 310,000 Texans.

People have a right to privacy, even in the Internet age. Any woman who has an abusive ex-boyfriend will tell you that she doesn't want her apartment number published on an open web site. Child custody cases can get nasty. Thieves who find a database like the one left in the open by Diebold may try to sell the information.

In this file were birthdays. First, middle and last names. Street addresses. Apartment numbers. School districts. Political affiliations. Voting habits. Yes, I assume they will say it was some kind of voter registration file, but it doesn't look quite precisely like one. Each kind of information (name, zip code, etc.) is called a "field." This file had 167 fields, which included data from about three dozen elections, logged in over a period of several years by many different people. Ninety-five thousand people from Plano are in this file, and a couple hundred thousand more from Richardson, McKinney, Wylie, Dallas and surrounding areas.

Because of this file I know that Bob L. of Plano is a Republican and likes to do early voting, and that he and his wife are the same age. But does Bob know that Diebold hung his undies out the window for all to see?

Yes, I know. Someone will explain to me that you can buy voter registration files for a nominal fee. But that doesn't mean you can buy those lists and stick them on the Internet (and what was Diebold doing with this information anyway?).

And does Bob Urosevich, the President of Diebold Election Systems, know that his wife and daughter had their private information on that web site too?

And what do Diebold and the other guardians of our vote have to say about this?

"We protect the Bill of Rights, the Constitution and the Declaration of Independence. We protect the Hope Diamond. Now, we protect the most sacred treasure we have, our secret ballot."[17]

— Diebold CEO Wally O'Dell

"For 144 years, Diebold has been synonymous with security, and we take security very seriously in all of our products and services."

— Diebold web site

"Sometimes our customers use the FTP site to transfer their own files. It has been up quite some years. People go there from counties, cities, sometimes there is stuff there for state certification boards, federal certification, a lot of test material gets passed around."[18]

— Guy Lancaster
Diebold contractor, 2/03

...the current group of computer 'wizards" who are so shrilly attacking ... are no longer behaving like constructive critics but rather as irresponsible alarmists and it's getting a little old.

— Dan Burk
Registrar of Voters
Washoe County, NV
(from Diebold web site)

"They're talking about what they could do if they had access to the [computer program] code...But they're not going to get access to that code. Even if they did, we'd detect it." [19]

— Dr. Britain Williams

"Our ongoing investigation has found no merit to the insinuations of security breaches in our election solutions." [20]

Joe Richardson
Diebold spokesman
Feb 2003

Harris: (follow up question) "So if there were 20,000 files including hardware, software specs, testing protocols, source code, you do not feel that is a security breach?"

Richardson: *[shuffling papers]* "Our ongoing investigation has found no merit to the insinuations of security breaches in our election solutions." [20]

"The scientists are undermining people's confidence in democracy," Townsend said. "None of the critics is giving any credence to the extensive system of checks and balances that we employ internally."

Mischelle Townsend
Registrar of Voters
Riverside County, CA
Associated Press 8/17/03

"It is all fine and well to upload results over the internet, but we don't exactly have a lot of experience in internet security in this company, and government computers are crackers favorite targets."

Barry Herron
Diebold Regional Manager
Diebold internal E-mail - 2/3/99

Chapter 8 footnotes

1 – "If You Want To Win An Election, Just Control The Voting Machines" by Thom Hartmann: http://www.commondreams.org/views03/0131-01.htm. Thom Hartmann is the author of *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (www.unequalprotection.com)

2 – PUBLIC RECORD ACT REQUEST: Responding Agency: Alameda County Registrar of Voters filed by Jim March on July 29, 2003. http://www.equalccw.com/voteprar.html

3 – PUBLIC RECORD ACT REPLY: Responding Agency: Alameda County Registrar of Voters filed Aug. 8, 2003. http://www.equalccw.com/alamedafollowup.pdf

4 – *The Palm Beach Post:* 17 Sept. 2002; "Reno consults electronic voting foe"

5 – Unpublished interview of three experts on electronic voting, by William Rivers Pitt, author of *The Greatest Sedition is Silence*. Excerpted on Democratic Underground Aug. 1, 2003. Pitt also wrote *War in Iraq* and *Our Flag Too: The Paradox of Patriotism*.

6 – *The Risks Digest,* Vol. 22: Issue 25. Monday 23 September 2002: Memo from Chris Riggal, press secretary for Cathy Cox, Georgia Secretary of State.

7 – Georgia Secretary of State Press Office; Media Backgrounder: *Multilevel Equipment Testing Program Designed to Assure Accuracy & Reliability of Touch Screen Voting System*

8 – Diebold AccuTouch Technical Data Package TSx, final certification; *Appendix D: Quality Control Manual* and *Appendix E: Testing Procedures*, submitted to Wyle Laboratories for certification in Jan. 2003.

9 – RFP Sec 3.28, "Schedule for Deployment,"[#] submitted by Diebold Election Systems to the state of Georgia in March 2002.

10 – Feb. 11 2002: Interview of Michael Barnes, Assistant Director of Elections for the state of Georgia, by Bev Harris. Full unabridged interview can be found in the library at www.blackboxvoting.org

11 – Feb. 12 2002: Interview of Dr. Britain Williams, NASED certfication board, official voting machine certifier for the states of Georgia, Maryland

and Virginia, by Bev Harris. Full unabridged interview can be found in the library at www.blackboxvoting.org

12 – *The Register*, February 2003, republished Aug. 2 2003; "Computer ballot outfit perverts Senate race, theorist says" by Thomas C. Greene. http://www.theregister.co.uk/content/55/29247.html and (read also) http://www.theregister.co.uk/content/35/29262.html.

13 – AccuPoll voting system: http://www.accupoll.com/Products/Top10/index.html; "Non-proprietary hardware and open source software significantly reduce both initial acquisition and ongoing maintenance costs."

13a – Diebold internal Email, 4 April, 1999. From Ian Piper to Talbot Iredale.

14 – *The Baltimore City Paper*, 19 February 2003; "Ballot Check: Computerized Voting Comes Under Fire in Georgia and California" by Van Smith, and Salon.com, 20 February 2003; "Hacking Democracy" http://www.salon.com/tech/feature/2003/02/20/voting_machines/

15 – *The Baltimore Sun*, 25 July 2003; "New Study Says Maryland's Voting Machines Are Vulnerable to Hackers

16 – *The Guide to Identity Theft Prevention*, by Johnny May, CPP.Statistics on identity theft are available from the Federal Trade Commission Identity Theft Data Clearinghouse: "Figures and Trends on Identity Theft in Texas"http://www.consumer.gov/idtheft/statemap/texas.pdf (2001) and http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf (2002).

17 – *Cleveland Plain Dealer*, May 2002, interview with Wally O'Dell. Sent out as a company press release in Sept. 2003.

18 – Interview with Guy Lancaster, 4 Feb 2003; According to Lancaster's web site, he was in charge of the site for Global Election Systems; Lancaster has a small computer consulting firm and was under contract to Global Election Systems. When Diebold bought Global in Jan. 2002, they transferred responsibilities for the site to a full time Diebold employee, but kept Lancaster on under a new contract.

19 – *Washington Post*, 28 March 2003; "New Voting Systems Assailed; Computer Experts Cite Fraud Potential "

20 – Interview with Joe Richardson, Diebold spokesman by Bev Harris, Feb 2003.