Florida Fair Elections Coalition Inc.
112 W. New York Ave., Suite 201, P.O. Box 317
Deland, Florida 32721
386-736-8086
www.FloridaFairElections.org

May 31, 2006

Attorney General Charles Crist
Office of the Attorney General
The Capitol PL-01
Tallahassee, FL 32399-1050

Re: Attached Complaint concerning Diebold Election Systems' delivery of uncertified voting machines to Volusia and three other counties, in violation of Florida law

Dear Mr. Crist:

For more than a year, members of the Volusia County Council were told that they could not buy the disabled-accessible AutoMark ballot-markers favored by the county's citizens, *because the AutoMark was not certified by the state*. Now, in an amazing turn of affairs, David Drury, head of the Bureau of Voting System Certification, has authorized the delivery of *uncertified* Diebold voting machines to Volusia and other counties. Compounding the violations of state laws, Diebold issued an "Affidavit of Certification" to Volusia County officials for the uncertified equipment.

Volusia County elections personnel discovered during routine acceptance testing that the equipment they recently received from Diebold was not the certified machines they had contracted to receive but uncertified Model D units. The other three affected counties—Putnam, Glades, and Polk—apparently learned of the problem from newspaper reporters. Had Volusia County's conscientious elections staff not discovered the problem, the counties would have been obligated to pay Diebold a full eighty percent of the purchase price of the equipment at the conclusion of the acceptance testing.

Appended to the Complaint is Mr. Drury's letter to Diebold (Exhibit C) advising that it could deliver the uncertified equipment instead of the certified machines that the counties had contracted to receive. In his letter, Mr. Drury states that the delivery is acceptable because the equipment will not be "used" in an election until it is certified. The Florida Division of Elections flatly rejected this argument when Volusia County wanted to buy the uncertified AutoMark. Further, Mr. Drury does not say in the letter by what authority he is able to permit violations of state law or to allow a vendor to violate its contractual obligations with Florida counties.

Modifications or Upgrades Require Certification

In this case, there is no question of whether the equipment is certified—everyone admits that it is not. A spokesperson from the secretary of state's office, however, has suggested that the changes were merely "modifications." The changes to the Model D are, in fact, significant, but even if they weren't, any modifications, including upgrades, require certification since any change to a system can affect reliability and security. If any component of a system is not certified, then the system is not certified. Everything must be *identical*, not similar, not nearly the same, but exactly the same.

According to Mr. Drury's correspondence with Leon County, the TSx Model D differs from the certified equipment in the following ways: new liquid-crystal display, a new inverter to power the LCD, alterations to the motherboard to accommodate a graphics processor, flash memory, voltage regulators, fuses to modem outputs to improve phone line faults, and changes to the operating system. Although Mr. Drury asserts that there are no software changes, it is clear that upgrades to the software would be required to accommodate the listed hardware changes.

Mr. Drury also acknowledges in his letter to Leon County that the WinCE operating system has been "custom configured" for the new TSx model. For previous certifications, Diebold had asserted that the operating system was "commercial off the shelf" (COTS) and thus did not need to be certified. Now that Mr. Drury has acknowledged that the WinCE operating system is custom configured, it is clear that it must be certified not only for the new Model D, but also for all previously certified Diebold models. Mr. Drury states that the system has been reviewed by Wyle Laboratories, an Independent Testing Authority (ITA), but Wyle Laboratories only reviews hardware. There is most certainly a corresponding report from the ITAs responsible for software certification.

Voting Systems Must Be Certified to the Current Standards

Mr. Drury has justified this delivery by stating that he plans to certify the equipment imminently, even though he had not yet received the report from the Independent Testing Authority nor had he begun testing the machines himself. This claim is in itself distressing since it seems to suggest that the certification is a foregone conclusion.

The new TSx model, however, must now meet the requirements of new state laws that have gone into effect since the previous models were certified. Specifically, these machines must be tested to meet the provisions of Florida Statutes §§ 101.56062 and 101.573. The earlier TSx models were tested in accordance with the requirements of § 101.56062 and failed to meet those requirements. They were granted certification anyway because the new provisions were not yet in effect. If vendors were allowed to make alterations to systems without comprehensive certification testing, then they could avoid having their systems tested to meet the requirements of new state laws.

We believe the Model D would fail if tested to meet the requirements of Florida Statutes § 101.56062, since its predecessors could not meet these new standards. The difference is that Mr. Drury could no longer certify failed equipment since the higher standards apply. In fact, a letter from Maria Matthews, attorney at the Florida Division of Elections (attached), states that *all* voting systems used in the next election must meet the requirements of Florida Statutes § 101.56062. It should be noted that the ITA's do not test for Florida law, and there was a change involving the display.

New Security Concerns Should be Investigated Before Certification

Disturbing new information has come to light since the earlier TSx models were certified in March 2005. A series of security tests conducted by computer scientists in Utah have revealed that the TSx voting system has the capability of altering election results without detection. Their findings have since been confirmed by computer scientists around the country who are recognized as national experts in electronic voting systems. The problem has been written about in the *New York Times*, *Newsweek* and other credible mainstream publications (articles attached). Not only could election results be altered without detection, but an informed attacker with only minutes' access to a TSx voting machine could contaminate the entire voting system, effectively controlling the results of not only the current election but also all future elections, all without detection. There is no way to test to determine if a voting system has been contaminated, and once it is contaminated there is no way to get rid of the contamination.

Taken in their entirety, the attached reports on the recently discovered security vulnerabilities are serious and disturbing. The vulnerabilities they describe have been called a "major national security risk" and the "worst flaw ever discovered in a voting system." Following is one paragraph from the *Diebold TSx Evaluation -- SECURITY ALERT: May 11, 2006 --Critical Security Issues with Diebold TSx*:

> It is important to understand that these attacks are permanent in nature, surviving through the election cycles. Therefore, the contamination can happen at any point of the device's life cycle and remain active and undetected from the point of contamination on through multiple election cycles and even software upgrade cycles.

Earlier tests in Leon County, Florida revealed that the Diebold optical scan system also contains a major security vulnerability capable of altering election results without detection. This security hole is only

ameliorated by being able to hand count the paper ballots to confirm the machine counts. Hand counting paper ballots is not, of course, even an option with the "paperless" TSX touch-screen machines, and a new state law passed in 2005 prohibits the manual recount of paper ballots. This presents a dire picture for Florida elections, which are neither verifiable nor auditable.

Computer scientists, commissioned by the California Secretary of State's office to conduct an independent study, confirmed the Leon County findings and also found 16 additional security "bugs," all of which can alter election results without detection. The California scientists also concluded that manual audits (hand recounts) of the paper trail are the only way to determine if the machines are counting votes accurately.

In response to the report issued by the California scientists, the Florida Division of Elections took the extraordinary step of issuing a Technical Advisory that instructs the supervisors of elections to beef up security measures concerning the chain of custody for memory cards and other electronic media. The Florida Technical Advisory, however, only addresses short-term mitigation strategies for use in a local election. It does not address the long-term mitigation strategies recommended by the California scientists. Their report states that, in order for Diebold systems to be used in any *statewide* election, extraordinary measures must be taken including re-writing the entire Diebold AccuBasic programming language. This is similar to stating that a skyscraper is perfectly safe as long as the foundation is removed and rebuilt.

It is Mr. Drury's responsibility to safeguard Florida's elections by certifying all voting systems according to state law and state regulations and by thoroughly addressing problems with those systems as they are made known to him. He does not have the right or authority to allow certain vendors or equipment to bypass the certification process. He also does not have the right or authority to allow some vendors or equipment to meet lower standards for certification than those required for others.

Diebold certainly knew better—in 2004 it was fined $2.6 million for delivering uncertified equipment to Alameda County, California, and was found to have delivered uncertified equipment to 16 other California counties as well.

If Volusia's diligent elections staff hadn't discovered the problem, would it ever have been revealed? Would Mr. Drury have quietly and hastily certified the equipment so that no one would know before the certification had been completed? Would he do so by abbreviating the certification process? Would he even have required certification at all? His letter to Diebold implies he would not. Were Mr. Drury and Diebold hoping to avoid having to test the TSx voting system to meet the requirements of new state laws? Were they hoping to avoid confronting the new, huge security vulnerabilities that have been exposed in the Diebold voting system?

We are looking to you, Mr. Crist, to properly and thoroughly investigate this matter, which has huge ramifications for every voter and every candidate in this election year. The reliability and accuracy of our voting systems and confidence in our elections process is at stake.

Respectfully,

Susan R. Pynchon

Susan R. Pynchon
Executive Director
Florida Fair Elections Coalition

Attachments

ATTACHMENTS TO COVER LETTER

1. Letter from Maria Matthews, Assistant General Counsel, Florida Dept. of State

2. *Newsweek* Column, May 29, 2006, "Will Your Vote Count in 2006?"

3. *New York Times* Article, May 11, 2006, "New Fears of Security Risks in Electronic Voting Systems"

From:	"Matthews, Maria I." <MIMatthews@dos.state.fl.us> View Contact Details Add Mobile Alert
To:	"'Susan Pynchon'" <susanpynchon@yahoo.com>
Subject:	FW: Volusia County Purchase from ES&S
Date:	Thu, 15 Dec 2005 17:31:48 -0500

Per your public records request today.

Maria I. Matthews

Assistant General Counsel
Florida Department of State
R.A. Gray Building
500 S. Bronough Street
Tallahassee, Florida 32399
850.245.6536 (w)
850.245.6127 (f)

From: Matthews, Maria I.
Sent: Thursday, December 15, 2005 5:29 PM
To: 'Frederick Karl'
Cc: Alicia Hawkins; Carol Dill; Daniel Eckert
Subject: RE: Volusia County Purchase from ES&S

Mr. Karl:

Per our discussion, under section 101.294, Florida Statutes, no governing body may purchase or cause to be purchased any voting system that is not certified for use in this state.

Therefore, any contract that a governing body enters into by January 1, 2006, must provide for the purchase of a voting system that is currently certified in Florida and that is compliant with the disability requirements of section 101.56062, Florida Statutes. This is also consistent with the provisions of the Voting Systems Assistance Grant Agreement which dispensed HAVA (Help America Vote Act) monies (appropriated through the Florida Legislature) to be disbursed to certain counties to assist with the purchase of accessible voting systems. These compliant systems must be in place by the next election held in that jurisdiction following the January 1, 2006 deadline.

Provided the contract clearly states that it is for the purchase of a currently Florida-certified voting system, nothing precludes the contract from also containing a provision that in the event another specified voting system becomes certified by a future date certain, that the board may, in substitution, purchase that voting system once certified.

Respectfully,

Maria I. Matthews
Assistant General Counsel
Florida Department of State
R.A. Gray Building
500 S. Bronough Street
Tallahassee, Florida 32399
850.245.6536 (w)
850.245.6127 (f)

MSNBC.com
Newsweek

Will Your Vote Count in 2006?

'When you're using a paperless voting system, there is no security,' says Stanford's David Dill.

By Steven Levy
Newsweek

May 29, 2006 issue - Just when you thought it was safe to go back into the voting booth, here comes more disturbing news about the trustworthiness of electronic touchscreen ballot machines. Earlier this month a report by Finnish security expert Harri Hursti analyzed Diebold voting machines for an organization called Black Box Voting. Hursti found unheralded vulnerabilities in the machines that are currently entrusted to faithfully record the votes of millions of Americans.

How bad are the problems? Experts are calling them the most serious voting-machine flaws ever documented. Basically the trouble stems from the ease with which the machine's software can be altered. It requires only a few minutes of pre-election access to a Diebold machine to open the machine and insert a PC card that, if it contained malicious code, could reprogram the machine to give control to the violator. The machine could go dead on Election Day or throw votes to the wrong candidate. Worse, it's even possible for such ballot-tampering software to trick authorized technicians into thinking that everything is working fine, an illusion you couldn't pull off with pre-electronic systems. "If Diebold had set out to build a system as insecure as they possibly could, this would be it," says Avi Rubin, a Johns Hopkins University computer-science professor and elections-security expert.

Diebold Election Systems spokesperson David Bear says Hursti's findings do not represent a fatal vulnerability in Diebold technology, but simply note the presence of a feature that allows access to authorized technicians to periodically update the software. If it so happens that someone not supposed to use the machine—or an election official who wants to put his or her thumb on the scale of democracy—takes advantage of this fast track to fraud, that's not Diebold's problem. "[Our critics are] throwing out a 'what if' that's premised on a basis of an evil, nefarious person breaking the law," says Bear.

Those familiar with the actual election process—by and large run by honest people but historically subject to partisan politicking, dirty tricks and sloppy practices—are less sanguine. "It gives me a bit of alarm that the voting systems are subject to tampering and errors," says Democratic Rep. William Lacy Clay, who worries that machines in his own St. Louis district might be affected by this vulnerability. (In Maryland and Georgia, all the machines are Diebold's.)

The Diebold security gap is only the most vivid example of the reality that no electronic voting system can be 100 percent safe or reliable. That's the reason behind an initiative to augment these systems, adding a paper receipt that voters can check to make sure it conforms with their choices. The receipt is retained at the polling place so a physical count can be conducted. "When you're using a paperless voting system, there is no security," says David Dill, a Stanford professor who founded the election-reform organization Verified Voting.

To their credit, 26 states have taken action to implement paper trails. But the U.S. Congress has yet to pass legislation introduced last year by Rep. Rush Holt, Democrat of New Jersey, that would extend this protection nationwide. Holt says his bill is slowly gaining support. "The voters are saying that every vote should count, and the only way to do this is by verified audit trails," he says. But even an optimistic scenario for passage would challenge his goal of mandatory paper receipts for November's elections. In other words, it's unlikely that every voter using an electronic voting device in 2006 will know for sure that his or her vote will be reflected in the actual totals. Six years after the 2000 electoral debacle, how can this be?

URL: http://msnbc.msn.com/id/12888600/site/newsweek/

NATIONAL DESK

New Fears of Security Risks In Electronic Voting Systems

By MONICA DAVEY; GRETCHEN RUETHLING CONTRIBUTED REPORTING FROM CHICAGO FOR THIS ARTICLE, AND JOHN SCHWARTZ FROM NEW YORK. (NYT)
788 words
Published: May 12, 2006

CHICAGO, May 11 - With primary election dates fast approaching in many states, officials in Pennsylvania and California issued urgent directives in recent days about a potential security risk in their Diebold Election Systems touch-screen voting machines, while other states with similar equipment hurried to assess the seriousness of the problem.

"It's the most severe security flaw ever discovered in a voting system," said Michael I. Shamos, a professor of computer science at Carnegie Mellon University who is an examiner of electronic voting systems for Pennsylvania, where the primary is to take place on Tuesday.

Officials from Diebold and from elections' offices in numerous states minimized the significance of the risk and emphasized that there were no signs that any touch-screen machines had been tampered with. But computer scientists said the problem might allow someone to tamper with a machine's software, some saying they preferred not to discuss the flaw at all for fear of offering a roadmap to a hacker.

"This is the barn door being wide open, while people were arguing over the lock on the front door," said Douglas W. Jones, a professor of computer science at the University of Iowa, a state where the primary is June 6.

The latest concern about the touch-screen machines was only the newest chapter in an

emerging political and legal fight around the country over voting machines. While some voting officials defend the ease of touch-screens (similar to A.T.M.'s), some advocacy groups argue that optical scan machines, using paper ballots, are far more secure.

The wave of high-tech voting machines was prompted by the 2000 election in Florida, which spotlighted the problems of old-fashioned punch card ballots. But the machines that soon followed have spurred division. Here in Chicago, where voters used both touch-screen and optical-scan systems in a March primary, it took officials a week to tally all the votes because of technical problems and human errors, touching off a flurry of criticism over the Sequoia Voting Systems equipment.

In Maryland this spring, the State House of Delegates passed a bill that would have scrapped touch-screen machines, but the Senate last month took no action on the bill, effectively killing the idea.

This week, Voter Action, a nonprofit group, assisted voters in Arizona in filing for a legal injunction to try to block the state from buying touch-screen electronic voting systems. The suit is among several the group says it has pursued, in states including California, New York and New Mexico.

The new concerns about Diebold's equipment were discovered by Harri Hursti, a Finnish computer expert who was working at the request of Black Box Voting Inc., a nonprofit group that has been critical of electronic voting in the past. The group issued a report on the findings on Thursday.

Computer scientists who have studied the vulnerability say the flaw might allow someone with brief access to a voting machine and with knowledge of computer code to tamper with the machine's software, and even, potentially, to spread malicious code to other parts of the voting system.

As word of Mr. Hursti's findings spread, Diebold issued a warning to recipients of thousands of its machines, saying that it had found a "theoretical security vulnerability" that "could potentially allow unauthorized software to be loaded onto the system."

The company's letter went on: "The probability for exploiting this vulnerability to install unauthorized software that could affect an election is considered low."

David Bear, a spokesman for Diebold Election Systems, said the potential risk existed

because the company's technicians had intentionally built the machines in such a way that election officials would be able to update their systems in years ahead.

"For there to be a problem here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software," he said. "I don't believe these evil elections people exist."

Still, he said, the company will in the coming months solve the vulnerability, but not before most primary elections occur.

In places where the machines are used, most election officials said they were not worried.

"We're prepared for those types of problems," said Deborah Hench, the registrar of voters in San Joaquin County, Calif. "There are always activists that are anti-electronic voting, and they're constantly trying to put pressure on us to change our system."

Aviel Rubin, a professor of computer science at Johns Hopkins University, did the first in-depth analysis of the security flaws in the source code for Diebold touch-screen machines in 2003. After studying the latest problem, he said: "I almost had a heart attack. The implications of this are pretty astounding."

Photo: Retrieving votes from an electronic machine in Cleveland on May 3. (Photo by Jamie-Andrea Yanak/Associated Press)