



ILLINOIS BALLOT INTEGRITY PROJECT SUBURBAN COOK COUNTY CHAPTER

635 Chicago Ave • Suite 127 • Evanston • IL • 60202

Phone: (847) 644-2654 • FAX: (847) 556-0363 • email: wilson@ballot-integrity.org

www.ballot-integrity.org

Robert A. Wilson
Chairperson

Via Electronic Transmission

9 January 2006

Honorable Jesse R. Smart, Chairman
Illinois State Board of Elections
1020 S. Spring St.
Springfield, IL 62701

Dear Chairman Smart:

At the December 20, 2005 meeting of the Illinois State Board of Elections, the Board voted 6-2 with certain qualifications to certify the Diebold AccuVote TSx DRE terminal as equipped with the AccuView Printer.

At issue was the Board's "First Set of Questions and Requests for Diebold" which had been sent under cover of Executive Director Daniel White to Mr. Bill Barnett of Diebold on December 1, 2005, to which Diebold had yet to reply. The Board's conditional approval of the Diebold was given contingent on a satisfactory reply being received from Diebold before year-end. Diebold replied with responses to the 16 Questions and Requests and added a 17th response.

The Illinois Ballot Integrity Project has reviewed both the Board Requests and Diebold Responses and herewith submits its commentary, attached hereto. We respectfully request that this document be made a part of the record at the Board's next meeting.

We believe that after careful consideration of our prior submission and this commentary on Diebold's response to the Board's letter, that the Board will deem it in the public interest to withdraw the conditional interim certification granted on December 20, 2005.

Our purpose continues to be to assist the Board in providing the best election systems for the voters and taxpayers of Illinois. We adhere to the principle that ensuring fair, accurate, and completely transparent elections is paramount to the securing of American democracy. We trust that this letter and the attached document is in furtherance of that objective. Again, we wish to thank you and all Members of the Illinois State Board of Elections for your efforts on behalf of the voters of Illinois.

Respectfully submitted,

Attachment

Copies w/attachment to:

Wanda L. Rednour, Vice Chair – SBOE
(via USPS Priority Mail)
John R. Keith, Member – SBOE
William M. McGuffage, Member – SBOE
Patrick A. Brady, Member – SBOE
Robert J. Walters, Member - SBOE

Albert Porter, Member – SBOE
Brian A. Schneider, Member – SBOE
Daniel White, Executive Director – SBOE
Dianne Felts, Director, VS&S - SBOE
Mr. Charles R. Owen - DESI
Executive Committee – IBIP



ILLINOIS BALLOT INTEGRITY PROJECT

www.ballot-integrity.org

COMMENTARY ON THE
"16 QUESTIONS AND REQUESTS"
PROPOUNDED BY THE
ILLINOIS STATE BOARD OF ELECTIONS
TO DIEBOLD ELECTION SYSTEMS, INC.

January 9, 2006

For further information concerning this document, please contact:

Laurence J. Quick
Chairperson
Illinois Ballot Integrity Project
PMB 191 – 2112 Galena Blvd
Aurora IL 60506
(630) 460-0857
quickinfo@qnc.us

Robert A. Wilson
Chairperson, Suburban Cook County Chapter
Illinois Ballot Integrity Project
635 Chicago Ave – Suite 127
Evanston IL 60202
(847) 644-2654
wilson@ballot-integrity.org

COMMENTARY OF ILLINOIS BALLOT INTEGRITY PROJECT ON THE DIEBOLD RESPONSE TO THE "16 QUESTIONS" PROPOUNDED BY THE ILLINOIS STATE BOARD OF ELECTIONS

INTRODUCTION

On December 1, 2005, Executive Director, Daniel White sent a letter to Diebold Election Systems with an attachment thereto, "FIRST SET OF QUESTIONS AND REQUESTS FOR DIEBOLD." As of December 20, 2005, the Board had yet to receive a reply from Diebold. As a result, the interim certification granted to the Diebold AccuVote-TSX and AccuView printer system was made contingent on such a response.

This document examines the questions and requests and sets forth some commentary on both the questions and Diebold's responses.

Board Request

1. List each date since January 1, 2000 on which there have been election problems regarding Diebold equipment stating for each date the following:
 - a. The date(s) of each election relative to which there was a problem;
 - b. The nature of each said problem;
 - c. A description of all steps taken by Diebold to correct the problem;
 - d. The date on which the problem was satisfactorily corrected;
 - e. The name and mailing address of each election authority involved in the problem and/or correction process;
 - f. Any and all documentation to substantiate Diebold's theory of the cause of the problem;
 - g. Identification of the Diebold equipment involved in the problem situation.

Diebold Response

Diebold lists three "election problems," occurring in Johnson County, Kansas (April, 2003); Alameda County, California (March, 2004) and San Diego County, California (March, 2004). In the first, Diebold claims that the problem was a communications network problem," the Alameda County problem to be the result of an "anomaly," and the Alameda/San Diego County problem a "battery power issue."

IBIP Comments

Apparently, we are to conclude that in the six-year period, 2000-2005, that only three such problems involving Diebold products have occurred. This period is split evenly between years in which the company was known as Global Election Management Systems and subsequent to Diebold's acquisition in 2002, as Diebold Election Systems.

Three, however, seems an unreasonably low number of instances during a six-year period and that contention is contravened by IBIP's research which indicates that there are more than three dozen such occurrences. In its December 12, 2005 submission to the Board, "DIEBOLD SYSTEMS SHOULD NOT BE CERTIFIED BY THE ILLINOIS STATE BOARD OF ELECTIONS." The Illinois Ballot Integrity Project highlighted twelve such problems of sufficient magnitude that they are reproduced herein:

November 2000 - AccuVote OS Volusia County, Florida. Internal Diebold memos (leaked in 2003) show that the company officials knew about the 16,022 Gore votes that were subtracted, and they still don't have an explanation for why the votes were lost. Tampering may have been the cause.¹

¹ [Tulare] County votes for machines. By Roger Phelps, The Porterville Recorder; June 10, 2004. http://myopr.com/articles/2004/06/10/news/local_state/news01.txt

November 2002 - AccuVote OS Robeson County, North Carolina. Ballot tabulating machines failed to work properly in 31 of 41 precincts. Local election officials said the problem was the result of a software glitch, and ballots had to be recounted.

April 2003 AccuVote TS Johnson County, Kansas. An unexplained software error caused the voting computers to miscount the votes. Diebold investigated the problem and said in a news release issued at the time that a software error had led to the election night problem.²

December 2003 - AccuVote OS and TS California. Secretary of State discovers that Diebold installed uncertified software throughout California before the recall election, without informing county officials. "An audit of Diebold Election Systems voting machines in California has revealed that the company installed uncertified software in all 17 counties that use its electronic voting equipment. Diebold admitted wrongdoing Tuesday at a meeting of the state's Voting Systems Panel."³

December 2003 Diebold Seattle, Washington. Investigative journalist Bev Harris announced her discovery that a Diebold programmer had been convicted of stealing money by tampering with computer records. At least five convicted felons secured management positions at a subsidiary of Diebold, and included a cocaine trafficker, a man who conducted fraudulent stock transactions and a programmer jailed for falsifying computer records. The programmer, Jeffrey Dean, wrote and maintained proprietary code used to count hundreds of thousands of votes as senior vice president of Global Election Systems, or GES. Diebold purchased GES in January 2002. According to a public court document, Dean served time in a Washington state correctional facility for stealing money and tampering with computer files⁴

March, 2004 - GEMS San Diego County, California. The tabulation software switched 2,747 Democratic presidential primary votes for U.S. Sen. John Kerry to U.S. Rep. Dick Gephardt.⁵

April 2004 Diebold California. Secretary of State Kevin Shelley called on the Attorney General to bring criminal charges against voting-machine-maker Diebold Election Systems for fraud. Prior to and during the hearing [of November 10, 2003], Diebold representatives either claimed to have obtained federal qualification for the TSx system or that federal approval was imminent. Diebold subsequently failed to obtain federal qualification for the entire TSx system or even to pursue federal qualification of the firmware. Diebold not only failed to obtain federal qualification for the TSx system, but failed even to pursue federal qualification of the firmware versions the VSPD Diebold was authorized to install in the wake of the discovery that uncertified software had been installed.⁶

April 2004 - AccuVote TS and TSx California. Secretary of State Kevin Shelley decertified all electronic touch-screen voting machines in the state due to security concerns, primarily caused by Diebold.⁷

² **New voting technology is questioned: Computer systems can be tampered with, critics say.** The Kansas City Star; September 21, 2003. By Finn Bullers; <http://www.kansascity.com/mld/kansascity/news/6821316.htm>

³ **E-Voting Undermined by Sloppiness.** Wired News. December 17, 2003. By Kim Zetter http://www.wired.com/news/evote/0,2645,61637,00.html?tw=wn_tophead_2

⁴ **Con Job at Diebold Subsidiary.** Wired News. December 17, 2003. by AP. http://www.wired.com/news/evote/0,2645,61640,00.html?tw=wn_tophead_3

⁵ **Diebold reports multiple problems: Registrar wants reason for e-voting.** TriValley Herald. April 13, 2004. By Ian Hoffman, Staff Writer. <http://www.votersunite.org/article.asp?id=2390>

⁶ **California Bans E-Vote Machines.** Wired News. April 30, 2004. By Kim Zetter. <http://www.wired.com/news/evote/0,2645,63298,00.html>

⁷ **Ibid and Staff Report On the Investigation of Diebold Election Systems, Inc.** April 20, 2004. Presented to Secretary of State Kevin Shelley and the Voting Systems and Procedures Panel.

September 2004 - AccuVote TS and modems Prince George's County, Maryland. The modem at the central facility malfunctioned, and voters in one precinct weren't able to vote the Democratic ticket on the paperless machines, so they wrote their choices on pieces of paper.⁸

November 2004 – AccuVote TS Maryland. On election day, TrueVoteMD registered 383 reports involving 531 incidents of problems encountered by voters. Many voters reported votes switching on the screens.⁹

March 2005 - AccuVote Touch screen Montgomery County, Maryland. The IT report to the County Elections Board reveals widespread problems with the electronic voting machines on election day. From Help Desk tickets and GEMS reports, 189 voting units (7%) of units deployed failed on Election Day. An additional 122 voting units (or 5%) were suspect based on number of votes captured.¹⁰

Also appended to IBIP's December 12, 2005 submission to the Board was a list, compiled by Voters Unite (<http://www.votersunite.org>) runs to some 22 pages and is available here: <http://www.votersunite.org/info/Dieboldinthenews.pdf> This list of more than three dozen news articles concerning failures specifically related to Diebold systems was attached as Appendix A to that document.

The Diebold response, however, does not fully explain what happened in San Diego County in March, 2004. John Pilch, a retired insurance agent who worked as a polling place inspector in San Carlos, said that when polls closed at 8 p.m. Tuesday, the number of people who signed the voter log differed from the number of ballots counted by computers.

"We lost 10 votes, and the Diebold technician who was there had no explanation," said Pilch, who registered complaints with elections officials, his county supervisor and several others. "She kept looking at the tapes."¹¹

Multiple additional problems occurred, among them:

Poll workers saw unfamiliar Windows screens, frozen screens, strange error messages and login boxes none of which they'd been trained to expect. A report released Monday by Diebold Election Systems shows that 186 of 763 devices known as votercard encoders failed on election day because of hardware or software problems or both, with only a minority of problems attributable to poll worker training.

Diebold's post-mortem of the March 2 election said it was "disappointed" in the encoder failures and that it values its ties to local elections officials. But the McKinney, Texas-based firm offered no fundamental explanation of how and why the company delivered faulty voting equipment to Alameda and San Diego counties its two largest West Coast customers on the eve of the 2004 presidential primary.¹²

Further, the explanation to the Board regarding the absentee ballots in Alameda County, stating "The input from this many optical scanners caused an anomaly to occur," is directly contradicted by Diebold's own statements to Alameda County on April 26, 2004, "DESI determined that these conditions are contributing factors [large number of ballot positions, multiple scanners] of the anomaly, not its cause.

Rather, the cause is a problem with the GEMS 1.18.18 program. [emphasis added]

⁸ **Johnson Aide Wins Democratic Primary.** Washington Post. September 15, 2004. By Ovetta Wiggins, staff writer. <http://www.washingtonpost.com/wpdyn/articles/A22014-2004Sep14.html>

⁹ **When the Right to Vote Goes Wrong.** TrueVoteMD. November, 2004. http://www.truevotemd.org/Election_Report.pdf

¹⁰ **IT Report to the Montgomery County Election Board.** Page 11. http://www.truevotemd.org/Resources/Lessons_Learned.pdf

¹¹ **Poll workers, voters cite tied-up hotline, poor training, confusion.** Union Tribune; March 7, 2004; By Jeff McDonald and Luis Monteagudo Jr. <http://www.signonsandiego.com/news/politics/20040307-9999-1n7vote.html>

¹² **Report of Assurances to Alameda County.** April 26, 2004. By Diebold Election Systems, Inc. Pages 2,3. http://www.truevotemd.org/ebold_rpt_alameda.pdf

Board Request

2. List the name and address of each executive officer and director of Diebold, Inc. for all times subsequent to December 1, 2000 and for each person so listed list all partisan political activities by that person since that time.
3. Did Walden O'Dell state at any time prior to January 1, 2004 the following (or substantially the following) "I am committed to helping Ohio deliver its electoral votes to the President next year"? If so, please explain the reason for same and all actions taken by Walden O'Dell to so provide for the delivery of said votes.
4. Provide a copy of each letter sent by Walden O'Dell indicating his support for President Bush subsequent to December 1, 2001.

Diebold Response

Diebold replies that these three requests are outside the scope of certification and we tend to agree.

IBIP Comments

Mark Radke of Diebold has described the Waldon O'Dell statement as "unfortunate," and that's probably accurate. As a non-partisan, public interest association, the Illinois Ballot Integrity Project believes that individuals are entitled to engage in legal political activity, regardless of their views and opinions, corporate affiliation notwithstanding.

We will address the issue of political organizations and contributions at a subsequent point in this document.

Board Request

5. Please provide copies of all documents containing charges by the State of California relative to problems with Diebold equipment during the March, 2004 primary, identification of the equipment involved, Diebold's theory as to why the equipment malfunctioned, the steps taken to rectify the problem(s), the reason for the decertification of any Diebold equipment and the steps taken by Diebold to remedy the equipment.

Diebold Response

Diebold has responded by referring the Board to its April 26, 2004, "Response To VSPP (Voting Systems and Procedures Panel) Recommendations Submitted By Diebold Election Systems, Inc.," a 28 page document posted on Diebold's website: <http://www.diebold.com/dieboldes/vsppresponse.pdf> . We reproduce the conclusions of Diebold's response here:

DESI recognizes that there has been a significant loss of trust between (i) the VSPP and the Secretary of State and (ii) DESI and its representatives. The frustration of the VSPP and the Secretary of State is understood by DESI.

However, the VSPP Staff Report does not present a fair and balanced record. Moreover, the absence of due process and the failure to provide DESI advance notice of the Staff Report and a reasonable opportunity to respond underscores the degree to which DESI has alienated the VSPP and the SOS. DESI hopes to never be in that situation again. Despite the difficult circumstances, it is crucial that the issues and the full record be dispassionately considered. No other vendor is being put through such a process.

DESI recognizes that the very fact that it believes there is much more that should be considered by the VSPP and the Secretary of State may further inflame the situation. That is not DESI's intent. With all of this being said, DESI hopes, if it is the decision of the Secretary of State, that he will (i) temper the recommendations of the VSPP and the Staff Report, and **(ii) simply withdraw the conditional certification of the TSx as configured for the March 2, 2004 election.** [emphasis added]

IBIP Comments

This answer, while presenting Diebold's side of the controversy, fails to include the document to which it was responding, Staff Report On The Investigation Of Diebold Election Systems, Inc. ,April 20, 2004, Presented To Secretary Of State Kevin Shelley And The Voting Systems And Procedures Panel, which may be found here: http://www.ss.ca.gov/elections/ks_dre_papers/diebold_report_april20_final.pdf. That of course is not the end of the story.

In April, 2004 California Secretary of State Kevin Shelley called on the State's Attorney General to bring criminal charges against voting-machine-maker Diebold Election Systems for fraud. Prior to and during the hearing [of November 10, 2003], Diebold representatives either claimed to have obtained federal qualification for the TSx system or that federal approval was imminent. Diebold subsequently failed to obtain federal qualification for the entire TSx system or even to pursue federal qualification of the firmware. Diebold not only failed to obtain federal qualification for the TSx system, but failed even to pursue federal qualification of the firmware versions the VSPP Diebold was authorized to install in the wake of the discovery that uncertified software had been installed.

In September 2004, California Attorney General Bill Lockyer dropped the state's criminal investigation of Diebold and joined with Alameda County and two voting integrity activists, Bev Harris and Jim March, suing the company in a False Claims Act.

Their False Claims Act suit, filed under seal and in the name of state and local taxpayers, alleged that Diebold sold nearly \$13 million touch-screen system to Alameda County by misrepresenting its accuracy, security and government approval. As state and county attorneys weighed the case, state and local elections officials found that Diebold had installed unapproved software in Alameda County's touch-screens, that its system was vulnerable to hacking and that its central vote-tabulating program gave thousands of absentee votes to the wrong candidates.

"We received assurances when they sold a voting system to us, and those assurances have not been met," said Alameda County Counsel Richard Winnie.

Secretary of State Kevin Shelley blasted Diebold for what he called a "culture of deceit" and referred the company to the state attorney general for criminal investigation.

Lowell Finley, an Oakland-based elections lawyer who filed the original suit on behalf of Harris and March, said his clients will watch to ensure the state and county to pursue the case with vigor. "Now that the state's attorney general has waded into this controversial issue, it is going to be important for him and the people of the state that he delivers something substantial, either in terms of a verdict or a very favorable settlement for California taxpayers," Finley said. "I don't think he would have made the decision to intervene if he didn't think that was possible."

In November, 2004, Diebold agreed to pay \$2.6 million to settle the lawsuit alleging that the electronic voting machine company sold the state and several counties shoddy voting equipment.

"There is no more fundamental right in our democracy than the right to vote and have your vote counted," California Attorney General Bill Lockyer said in a statement. "In making false claims about its equipment, Diebold treated that right, and the taxpayers who bought its machines, cavalierly."

Board Request

6. List all criminal investigations relative to Diebold voting equipment subsequent to January 1, 2000 including for each said investigation:
 - a. The jurisdiction in which the investigation was undertaken;
 - b. The name and address of the principal investigating agency;
 - c. The present status of said investigation;
 - d. Copies of all documents supplied by Diebold in response to said investigation; and
 - e. Copies of all documents received by Diebold relative to said investigation.

Diebold Response

Diebold responds that the matter was settled by civil litigation.

IBIP Comments

See comments relating to Board Request No. 5, *supra*.

Board Request

7. Please explain the existence of the software and/or information that was found in a folder titled "Rob-Georgia.zip." relative to voting machines supplied by Diebold including the name and address of each person having knowledge of the creation, content and present status of said software.

Diebold Response

Diebold responds by stating that the file "contained ADA audio voice guidance files that are used to provide unassisted voting for people with disabilities."

Diebold also states, "Georgia has conducted over 750 elections using their Diebold systems and have conducted many recounts which have confirmed the accuracy of the system."

IBIP Comments

"Rob" refers to Rob Behler, a contract technician (not an employee of Diebold as they state in their Reponse) working for Diebold, for whom the file was intended. It would appear that the file rob-georgia.zip (indicating a compressed file using the WinZip utility) actually contained something considerably different than ADA audio files. The file was a compilation of four files, containing at least three "patches" to election software, specifically the GEMS tabulating software and fixes relating to problems Behler and his team were having getting the touch screen machines ready for the November, 2002 election.. (This fix was probably written by Talbot Iredale, a programmer who worked for Diebold).

An extensive interview by Bev Harris of Black Box Voting with Rob Behler gives us more information. It makes interesting reading and certainly gives some insight into election related problems not mentioned in Diebold's response to Board Request No. 1 of this request. The entire interview (approximately seven typewritten pages) can be read here:

<http://www.scoop.co.nz/stories/HL0307/S00078.htm> We reproduce a few of the more telling exchanges below:

Harris: What was the FTP site for?

Behler: One of problems we had was an issue with the GEMS database. They had to do an update to it, so they just post the update to the web site.

Harris: What was rob-georgia?

Behler: I believe what that file was for, I did a -- well, there were a ton of holes with the programs on those machines. When they all came into the warehouse, I did a quality check, this was something I did on a Saturday. I found that 25% of the machines on the floor would fail KSU testing --

Harris: "What kind of problems were you seeing?"

Behler: "...One of the things we had wrong was the date wasn't sticking in the Windows CE. The real time clock would go to check the time on the motherboard, and it would have an invalid year in it, like 1974 or something, and basically the machine would continue to keep checking. Every time it checked, it saw that the date was not right and this put it into a loop.

"They had to do an update in CE to fix all those dates. So the way we did that in the warehouse was, they would post whatever the update was on the FTP site. James would go get the file and put it on the [memory] cards. Because you load everything through the PCMCIA cards. You boot it up using the card and it loads the new software.

Harris: "What about the rob-georgia file?"

Behler: "I think they put it out there for me when we were doing the Dekalb thing, but I was busy managing the whole crew so, I had my laptop out, and one of the engineers used my laptop -- or maybe it was James -- one of them had to go in and get it from the FTP, put it on a card, make copies of the cards and then we used them to update the machines."

Harris: "So one of the people downloaded the patch and then made copies of it?"

Behler: "They use[d] my laptop. It was not secure, either. They just used the laptop to repro the cards. Diebold never gave us anything with a PCMCIA slot, then they'd tell us, 'Go download this,' so we'd have to get out our own laptop to do it."

Harris: "What do you know about the ROM chip, or whatever?"

Behler: "There's the eeprom, or the flash as they call it. A lot of the fixes they did they could do in the flash memory. If they said they tested it I'm going to tell you right now the software that I installed on the machine myself, they found out that that was never tested."

"It was the software, not the hardware, that's where the problem was. "If they're telling you they tested that, well they did NOT test the fixes that they did to the windows CE software."

Harris: "Do you know who was writing the fixes?"

Behler: "He had a weird name. He came out of Canada."

Harris: "Guy Lancaster? Josh ... Talbot Iredale?"

Behler: "That's it! Talbot Iredale would actually fix it and say, 'Oh, here's the problem,' and stick it on the FTP site we'd grab it stick it on the card and make a bunch of copies and use it."

Harris: "So you took the patches right off the FTP site and installed them on the machines?"

Behler: "That's what we did, he'd FTP it, and tell us to grab it, we'd put it on a laptop, copy it and when you boot the machine -- it's just like a computer that looks at the "A" drive -- these machines look at the card and then erase the flash, reprogram with whatever they said needed to be fixed -- I say, erase it and reprogram it -- and then the whole thing would start all over again.

Based on the foregoing, it would appear that rob-georgia.zip actually contained a series of untested, uncertified patches that were used in the November, 2002 Georgia election, contrary to Georgia statutes, and contrary to Diebold's contention that the files on the FTP site were "... old software which was never used in an actual election . . ." (See Diebold Response to Board Request No. 12)

Further, Diebold's statement regarding the "many recounts" simply has no real basis within the generally understood meaning of the term. Georgia did not use touch screen machines with a verified paper audit trail (VVPAT), thus there has been nothing to recount. The "recount" consists of running the original

machine count again, with of course the same results. There's nothing with which to compare the original vote count – except itself. Hardly a meaningful recount, a situation which thoroughly frustrated any attempt to examine the 2002 Georgia results which brought a nearly complete Republican sweep in Georgia, contrary to both pre-election polling and exit polling results.

Board Request

8. List each election jurisdiction to which Diebold has provided copies of its computer source code used in election systems stating the name and address of the person who has control over said computer source code.

Diebold Response

Diebold responds with a listing o escrow accounts.

IBIP Comments

The Illinois Ballot Integrity Project supports open-source election software than can be readily examined by competent experts as to its reliability, functionality and security.

Board Request

9. Please provide all documentation supplied by Diebold since January 1, 2001 to any election authority in Illinois addressing problems Diebold has had with its equipment in elections in any state, including, but not limited to, the State of California, the State of Maryland, the State of Georgia and the State of Ohio identifying each such authority, the date the authority was so notified, the specific items of the documentation which were supplied to the authority and the name and present address of the person to whom the items were supplied for that authority.

Diebold Response

Diebold responds by quoting Fidler, "There has never been any official correspondence . . ."

IBIP Comments

Diebold has neatly sidestepped the problem by allowing Fidler to state that they have never had any official correspondence, etc. Essentially this is non-responsive to the Board Request. IBIP, however, has no documents regarding previous correspondence between Diebold and state or local election officials in Illinois.

Board Request

10. List each and every political action committee, State, Federal and/or Local, in which Diebold officers or directors regularly participated, including participation on behalf of Diebold or through funds which were reimbursed by Diebold.

Diebold Response

Diebold responds by quoting its ethics policy, Section 10:

Political Activities and Contributions

Board directors, officers and employees may participate in the political process, including voluntary contributions to candidates or parties and issues or causes of their choice.

However, in recognition of the necessity for strict neutrality concerning political candidates and issues, the chief executive officer, president, and chief financial officer of Diebold, Incorporated and those Diebold, Incorporated executives identified by the Company as responsible for the oversight of its election systems companies, as well as all employees of those companies, **may not make contributions to, directly or indirectly, any political candidate, party, election issue or cause, or participate in any political activities, except for voting.** This prohibition regarding political activities and contributions applies to U.S. and Canadian election systems businesses, and only to the extent permitted under applicable law. [emphasis added]

Also, no contributions from Company funds, or use of Company facilities or equipment, are to be made to or permitted for use by, directly or indirectly, any political candidates, organizations or causes unless permissible under applicable law and approved by the Company's Contributions Committee and by the Company's Legal Department.

IBIP Comments

It should come as no surprise that as the CEO of a multi-billion dollar corporation headquartered in Ohio, that Walden O'Dell, (resigned December 12, 2005) was a Republican supporter. In a widely circulated 2003 fundraising letter for a September 26, 2003. \$1,000 a couple dinner at his Upper Arlington (a Columbus, Ohio suburb) mansion, Diebold CEO O'Dell promised to deliver Ohio's 2004 electoral votes—and thus the election—to Bush. O'Dell is one of Ohio's 30 GOP Bush Pioneer/Ranger high money donors. O'Dell's fund-raising letter followed on the heels of a visit to President Bush's Crawford Texas ranch by "Pioneers and Rangers," the designation for people who had raised \$100,000 or more for Bush's re-election.

Mr. O'Dell's letter was mailed one day before Secretary of State J. Kenneth Blackwell was expected to name Diebold as one of three firms eligible to sell voting machines to Ohio counties, which subsequently occurred.

Matt Damschroder, the executive director of the Franklin County (Columbus, Ohio) Board of Elections, acknowledged that in 2004 he had accepted a \$10,000 check for the county GOP from a Diebold consultant who was seeking county business. The transaction took place in Mr. Damschroder's county office and he was fined a month's pay for accepting this payment.

Some specific contributions by Walden O'Dell:

O' Dell, Walden W. Mr.
6/12/2003 \$4,000.00
Diebold Inc./Chairman -[Contribution]
Canton, OH 44708
BUSH-CHENEY '04 INC

O'DELL, WALDEN W
6/25/2003 \$1,500.00
NORTH CANTON, OH 44720
DIEBOLD INC -[Contribution]
VOINOVICH FOR SENATE COMMITTEE

O' Dell, Walden W. Mr.
8/8/2003 \$2,000.00
Canton, OH 44708
Diebold Inc./Chairman -[Contribution]
BUSH-CHENEY '04 INC

Other Diebold contributors:

Bucci, David Mr.
6/26/2003 \$2,000.00
Hudson, OH 44236
Diebold Inc./Senior Vice President -[Contribution]
BUSH-CHENEY '04 INC

O'DELL, WALDEN W
6/25/2003 \$500.00
NORTH CANTON, OH 44720
DIEBOLD INC -[Contribution]
VOINOVICH FOR SENATE COMMITTEE

BUCCI, DAVID
6/29/2003 \$1,000.00
HUDSON, OH 44236
DIEBOLD -[Contribution]
VOINOVICH FOR SENATE COMMITTEE

Geswein, Gregory T. Mr.
6/26/2003 \$2,000.00
Bentleyville, OH 44022
Diebold Inc./Chief Financial Office -[Contribution]
BUSH-CHENEY '04 INC

Crowther, John Michael Mr.
8/27/2003 \$2,000.00
Canton, OH 44708
Diebold Inc. -[Contribution]
BUSH-CHENEY '04 INC

D' Amico, Thomas R. Mr.
9/3/2003 \$2,000.00
Canton, OH 44718
Diebold Inc. -[Contribution]
BUSH-CHENEY '04 INC

D'AMICO, THOMAS R
6/21/2003 \$500.00
CANTON, OH 44718
DIEBOLD INC -[Contribution]
VOINOVICH FOR SENATE COMMITTEE

Frazzitta, Bart Mr.
9/29/2003 \$1,000.00
Akron, OH 44333
Diebold Inc. -[Contribution]
BUSH-CHENEY '04 INC

Hillock, Jennifer L Mrs.
8/27/2003 \$2,000.00
Massillon, OH 44646
Diebold Inc. -[Contribution]
BUSH-CHENEY '04 INC

Hillock, Michael James Mr.
6/26/2003 \$2,000.00
Massillon, OH 44646
Diebold International Inc./Presiden -[Contribution]
BUSH-CHENEY '04 INC

Ingram, Larry Dean Mr.
9/15/2003 \$1,000.00
Massillon, OH 44646
Diebold Inc. -[Contribution]
BUSH-CHENEY '04 INC

Ingram, Larry Dean Mr.
6/26/2003 \$1,000.00
Massillon, OH 44646
Diebold Inc./Vice President Of Glob -[Contribution]
BUSH-CHENEY '04 INC

Mahoney, Robert
11/30/2003 \$250.00
Canton, OH 44718
Diebold/Chairman Emeritus -[Contribution]
CARE POLITICAL ACTION COMMITTEE (CARE
PAC)

It would appear that a number of officers of Diebold, including Chairman O'Dell, violated Section 10 of Diebold's ethics policy. While O'Dell has defended his actions, telling the Cleveland Plain Dealer "I'm not doing anything wrong or complicated."

And, when it comes to the Diebold board room, O'Dell is hardly alone in his generous support of the GOP. One of the longest-serving Diebold directors is W.R. "Tim" Timken. Like O'Dell, Timken is a Republican loyalist and a major contributor to GOP candidates. Since 1991 the Timken Company and members of the Timken family have contributed more than a million dollars to the Republican Party and to GOP presidential candidates such as George W. Bush. Between 2000 and 2002 alone, Timken's Canton-based bearing and steel company gave more than \$350,000 to Republican causes, while Timken himself gave more than \$120,000.

Board Request

11. List all activities involving Diebold and any investigations regarding election systems in the State of Ohio including, but not limited to, matters involving Governor Bob Taft and the Secretary of State Kenneth Blackwell.

Diebold Response

Diebold states that it is not a party to any criminal investigation, but is responding to a subpoena received from the Inspector General for the State of Ohio.

IBIP Comment

Much of the following commentary consists of the reporting of allegations, generally in the form of indictments, but also includes some speculation and "connecting of the dots." It will probably be some time before the various investigations are played out, so we'd advise a skeptical approach. Clearly, we can not at this time allege any wrongdoing by Diebold or any Diebold employee.

A close associate of key Republicans from George H.W. Bush to George W. Bush to Ohio Senator George Voinovich to Ohio Governor Robert Taft and many, many more, Tom Noe has long been known as northwest Ohio's "Mr. Republican." He has also been at the heart of speculation on how huge numbers of votes in the Toledo area may have wrongly found their way into the Bush column, helping the GOP again take the presidency in 2004, and the linchpin of the money laundering investigation which now touches Diebold, if only tangentially.

While media attention focuses on Noe's financial scams ("Coingate"), he spent many years as Chair of the Board of Elections in Lucas County. He was deeply involved in procurement deals that brought Diebold optical scanners into inner city Toledo precincts. Many of those machines suspiciously malfunctioned at key times on election day. Sworn testimony in hearings conducted after the election confirm that thousands of inner city voters were disenfranchised due to Noe's decisions.

The federal indictments against Noe include charges of conspiring to violate the Federal Election Campaign Act through the use of two dozen "conduit donors" who slipped the Bush-Cheney campaign some \$45,400 in 2003. Charges also claim Noe caused the Bush-Cheney campaign to file false reports with the Federal Election Commission. Noe faces penalties on the three counts up to \$950,00 in fines and up to a total of fifteen years in prison.

At the core of latest charges are assertions that Noe illegally avoided the \$2,000 federal campaign donation limit by giving his own money to 24 associates and having them funnel it to the Bush-Cheney campaign. Noe had promised to raise \$50,000 for the GOP presidential effort. Noel Hillman, chief of the U.S. Justice Department's Public Integrity Section, brands the case against Noe as "one of the most blatant and excessive campaign-finance criminal schemes we have encountered" in recent years.

Key aides to Governor Robert Taft, including Brian Hicks and James Conrad, have been forced to resign, with Hicks being convicted for failing to report a stay at Noe's Florida home. Bush Pioneer, former House Speaker Larry Householder, is under federal grand jury investigation for alleged skimming of campaign funds. Another Taft aide, Cherie Carroll, is charged with taking some \$500 in free dinners from Noe.

Ohio Gov. Robert Taft has also been convicted of three misdemeanor ethics violations, at least one of which involves a golf outing with Noe, during which Noe claims he told Taft about the secret Coingate investment/slush fund.

Noe's fortune came in part from charging the Bureau of Worker's Compensation (BWC) \$12.6 million in coin-fund related expenses for managing the \$50 million investment between 1998 and 2004. Federal and state officials are now investigating these expenses. A "Ponzi scheme" is what Ohio's Republican Attorney General Jim Petro calls the method by which Noe may have stolen millions of dollars from the state of Ohio's Bureau of Worker's Compensation (BWC).

Petro says that on May 31, 1998, Noe received the first of two \$25 million payments approved from then-Governor Voinovich's BWC. Noe promptly laundered \$1.375 million into his personal or business account. Rolling in public money, Noe then asked to run a bizarre rare coin investment scheme on behalf of the BWC.

While there's much speculation, at this point there are too few facts to connect Diebold or any of its former or present management to the current indictments.

Board Request

12. State the number of occurrences Diebold is aware of, where hackers had invaded any of its election systems, listing for each said occurrence:
- a. The date of said occurrence;
 - b. The jurisdiction where the occurrence occurred;
 - c. Identification of the equipment involved in the occurrence;
 - d. The extent of the knowledge of the hacking;
 - e. The steps taken to correct it and by whom each step was taken;
 - f. The name and address of the hacker(s);
 - g. The name and address of any independent authority verifying that said problem has been corrected together with a copy of said documentation.

Diebold Response

Diebold responds that they have “. . .not had our election systems hacked when used in an actual election environment.” This may or may not be accurate because as election activists claim, a successful hack will leave no trace.

Diebold claims that “Old software which was never used in an actual election, residing on a Diebold Internet site, has been presented by activists as hackable.

IBIP Comments

We would dispute this claim as to the “never used in an actual election” as be contradicted by the rob-georgia.zip file which came from this same site and was undoubtedly used in the November, 2002 elections in Georgia. (See discussion of Board Request No. 7)

However, the problem (unmentioned in the response to Board Request No. 1) remains concerning Volusia County, Florida in 2000. Internal Diebold memos (leaked in 2003) show that the company officials knew about the 16,022 Gore votes that were subtracted, and they still don't have an explanation for why the votes were lost. Tampering may have been the cause.

The memos show that more than a year ago, Diebold knew of a problem with the Florida 2000 election - where a memory card inexplicably subtracted 16,022 votes from a total previously recorded for Vice President Al Gore.

Tampering was one of four possible causes Diebold couldn't rule out at the time, the memos show. A year later, Diebold's latest official position on Florida's Volusia County vote count still does not rule out tampering. Company spokesman Bear said recently only that he was not familiar with the aberrant vote count in Volusia County.

"The problem precinct had two memory cards uploaded," wrote Diebold tech Tab Iredale in one of the memos among Diebold employees. "There is always the possibility that 'the second memory card' came from an unauthorized source."¹³

During the discussion on December 20, 2005,, Mr. Radke also alluded to “misinformation” and also brought up the issue of last week’s successful penetration of a Diebold product, overstating the level of access that was given by the Leon County, Florida election supervisor to the experimenters. Contrary to Mr. Radke’s statement, the access given was only that that might be provided to a poll worker on election day.

¹³ **[Tulare] County votes for machines.** By Roger Phelps, The Porterville Recorder; June 10, 2004. http://myopr.com/articles/2004/06/10/news/local_state/news01.txt

Finnish security expert Harri Hursti conducted the exploit with observers from Black Box Voting, Florida Fair Elections Coalition Director Susan Pynchon, and security expert Dr. Herbert Thompson. This exercise demonstrated that Diebold claims that votes can not be changed on the "memory card" (the credit-card-sized ballot box used by computerized voting machines.) to be incorrect.

A test election was run in Leon County on Tuesday, December 13, 2005, with a total of eight ballots. Six ballots voted "no" on a ballot question as to whether Diebold voting machines can be hacked or not. Two ballots, cast by Dr. Herbert Thompson and by Harri Hursti voted "yes" indicating a belief that the Diebold machines could be hacked.

At the beginning of the test election the memory card programmed by Harri Hursti was inserted into an Optical Scan Diebold voting machine. A "zero report" was run indicating zero votes on the memory card. In fact, however, Hursti had pre-loaded the memory card with plus and minus votes.

The eight ballots were run through the optical scan machine. The standard Diebold-supplied "ender card" was run through as is normal procedure ending the election. A results tape was run from the voting machine.

Correct results should have been: Yes:2 - No:6
However, just as Hursti had planned, the results tape read: Yes:7 - No:1

The results were then uploaded from the optical scan voting machine into the GEMS central tabulator, a step cited by Diebold as a protection against memory card hacking. The central tabulator is the device that pulls in all votes from voting machines. However, the GEMS central tabulator failed to notice that the voting machines had been hacked. The results in the central tabulator read: Yes:7 ; No:1

The Hursti Hack requires a moderate level of inside access. It is, however, accomplished without being given any password and with the same level of access given thousands of poll workers across the USA. It is a particularly dangerous exploit, because it changes votes in a one-step process that will not be detected in any normal canvassing procedure, it requires only a single a credit-card sized memory card, any single individual with access to the memory cards can do it, and it requires only a small piece of equipment which can be purchased off the Internet for a few hundred dollars.

To demonstrate that the hack did not require a "hands-on" approach, Hursti was in another room when the memory card was inserted into the Diebold AccuVote OS scanner.

According to the *Tallahassee Democrat*, on December 13th, supervisor Ion Sancho got approval from county commissioners to switch to optical-scan voting machines made by Election Systems and Software (ES&S). The machines will be used in conjunction with the AutoMARK devices. This action followed Diebold's refusal to permit the use of its AccuVote OS optical scanner with the AutoMARK, adopting an "all or nothing" approach to Leon County's system. (The new Leon County setup is the same type of configuration suggested by the Illinois Ballot Integrity Project White Paper, December 12, 2005)

This hack followed that of May, 2005, when Herbert Thompson, a computer-science professor and strategist at Security Innovation, which tests software for companies such as Google and Microsoft. Thompson couldn't hack into the system from the outside. So he was given access to the central machine that tabulates votes and to the last school election at Leon County High.

Thompson told *The [Miami] Herald* he was "shocked" at how easy it was to get in, make the loser the winner and leave without a trace. The machine asked for a user name and password, but didn't require it, he said. That meant it had not just a "front door, but a back door as big as a garage," Thompson said. From there, Thompson said, he typed five lines of computer code -- and switched 5,000 votes from one candidate to another. "I am positive an eighth grader could do this," Thompson said.

After Sancho announced the results, Diebold's senior lawyer, Michael Lindroos, wrote Sancho, Leon County and the state of Florida questioning the results and calling the test "a very foolish and irresponsible act" that may have violated licensing agreements.

It would appear to us that if in fact, the insertion of a "rogue" memory card can be used to alter the vote count at the scanner level, then an entire precinct can be compromised. The level of access is such that any one of hundreds of thousands of poll workers could accomplish this and may very well explain the possible actual election hack in Volusia County in 2000, when Diebold employees speculated that a second memory card was inserted into the optical scanner.

Both of these demonstrations were predictable. More recently, on July 4, 2005, Black Box Voting (www.blackboxvoting.org) issued a "Security Alert. - *Critical Security Issues with Diebold Optical Scan Design.*" Here are some excerpts from the Executive Summary:

"The findings of this study indicate that the architecture of the Diebold Precinct-Based Optical Scan 1.94w voting system inherently supports the alteration of its basic functionality, and thus the alteration of the produced results each time an election is prepared."

"The fundamental design of the Diebold Precinct-Based Optical Scan 1.94w system (AV OS) includes the optical scan machine, with an embedded system containing firmware, and the removable media (memory card), which should contain only the ballot box, the ballot design and the race definitions, but also contains a living thing – an executable program which acts on the vote data. . . .The system won't work without this program on the memory card."

"With this architecture, every time an election is conducted it is necessary to reinstall part of the functionality into the Optical Scan system via memory card, making it possible to introduce program functions (either authorized or unauthorized), either wholesale or in a targeted manner, with no way to verify that the certified or even standard functionality is maintained from one voting machine to the next."

In the report author's opinion the greatest problem in the system under review is the very design and architecture itself. Incorporated into the foundation of the Diebold Precinct-Based Optical Scan 1.94w system is the mother of security holes, and no apparent cure will produce infertility, or system safety.

This design would not appropriately be characterized as "a house with the door open." The design of the Diebold Precinct-Based Optical Scan 1.94w system is, in the report author's own view, more akin to "a house with an unlockable revolving door."

David Jefferson, a computer scientist at Lawrence Livermore National Laboratory and a member of the California secretary of state's voting systems panel, agreed that election procedures could help prevent or detect changes in votes, but said that election officials and poll workers do not always follow procedures. Therefore, election observers need to know about the vulnerabilities so they can help reduce the risk that someone could use them to rig an election.

Jefferson added that he doesn't believe that the vulnerabilities show deliberate malice on Diebold's part to aid fraud, but those vulnerabilities do show a lack of awareness or competence and indicate that Diebold programmers simply don't know how to design a secure system.

Frankly, the Illinois Ballot Integrity Project is less concerned about hacking individual machines, whether they be the touch screen terminals or the optical scanners. While both appear vulnerable, there are significant defenses, often referred to as "perimeter defenses" which can be applied in the procedures used by election officials to insure security of the machines, just as they would ballot boxes, lever machines or punch cards.

This does not mean that vendors ought not to provide layers of security for these devices, but strategically, we believe that they are at less risk for tampering than central count systems. It is here that a significantly smaller number of people could do significantly larger damage to election integrity.

Hacking individual terminals is simply too much effort for too little gain. While the above hacks make for good press and interesting reading, they are largely academic exercises. The real threats to voting systems lie elsewhere, particularly in the GEMS central tabulating software.

Diebold has published a "rebuttal" to certain types of security breaches that we have discussed above. <http://www.diebold.com/dieboldes/pdf/rebuttal.pdf> This rebuttal relies primarily on the so-called "perimeter defense" which requires that election officials maintain perfect control of all passwords and access to GEMS.

In our December 12, 2005 white paper, we discussed the "GEMS Defect" at some length. (See pp 6-8) and how it specifically affects certain types of ballots. Mail-in votes are at exceptional risk because they are counted on a system that lacks protective features found on polling place machines. While the precinct-based optical scan machines made by Diebold produce a results tape, the same machines, when counting mail-in ballots, use a different program and do not store vote tallies on a memory card, nor do they produce an independent results tape. Therefore the defective GEMS program holds the only record for absentee vote totals.

The GEMS program is run on an ordinary PC, using the Windows operating system. Vote totals from each precinct, along with mail-in votes, are uploaded to the GEMS computer. GEMS tallies all votes and produces final election results.

Changing the candidate identifier number in GEMS provides one-step adjustment that takes only seconds, and can be implemented any time during the absentee vote-counting process to flip results. As demonstrated in the Leon County, Florida elections office on May 2, 2005 by Dr. Herbert Thompson and Black Box Voting, this kind of GEMS manipulation does not require opening the GEMS program, does not require a GEMS password, and does not show up in any audit log.

The standard safeguard for this known risk is to compare results reports from voting machines with GEMS results reports. However, Black Box Voting has learned that Diebold's mail-in vote-counting system does not produce a voting machine report. In November, 2005, Jim March of Black Box Voting examined the Diebold voting system in San Joaquin County, Calif. and learned that the voting machine results tape -- the telltale sign and the key safeguard for GEMS tabulator hacking -- *does not exist for mail-in votes.*

A Scenario

Suspend for a moment the image of the 19 year-old hacker, or the geek with six pens in a pocket protector, or even a university professor. Imagine the Minister of State Security for a significant oil-producing nation, the CEO of a multinational corporation or the head of an international crime syndicate. How much would you have to gain by influencing elections in the United States? Think for a moment of the resources at your disposal to effect such influence.

Now imagine a rogue programmer working for a large voting machine corporation. How much money, time or effort could be expended to "turn" such a person? And what if you succeeded?

Now imagine, what if this rogue programmer was the one who constructed the patches that were in the rob-georgia.zip file. What if there were malicious code in these patches that was installed in every one of the 22,000 voting terminals used in the November, 2002 election in Georgia? Untested, uncertified code? And what if that election produced six nearly inexplicable upsets, including the first Republican Governor since the Civil War?

Michael Wertheimer, a systems-security consultant at Columbia, Md.-based RABA Technologies, the firm charged with advising Maryland on its voting says the biggest risk of tampering with electronic voting machines is from insiders—either elections staff or vendors. "If you have five minutes with a server, you can load a CD and change everything," he says. The risks to ballot integrity grow the farther upstream you go.

Compromising a single machine might involve 150 votes, the average number of votes counted by a single machine, according to Wertheimer. Cracking a server at the county level in Maryland might mean access to tens of thousands of votes, with more than three million votes at stake at the state level.

"If malicious changes to the software are made before it is distributed to the individual machines, there is no way to defend against it," Dr. David Dill of Stanford says. "It can easily be hidden so that it is very unlikely to be detected by any amount of inspection or testing."

Speaking in favor of a Verified paper Audit Trail (VVPAT) Wertheimer says, "Name an electronic transaction that doesn't ask if you want a paper receipt—at the bank, the gas pump, Amazon."

Indeed, Dill suggests that voting systems need tighter security, since voters' names aren't inscribed on ballots. "Compare that with banks, [which] have paper audit trails all over the place, all transactions have the names of the participants on them—and they are still subject to insider fraud," he says. "It's a cost of doing business."

It's from such a confluence of events, opinions and information that conspiracy theories are born. We don't subscribe to them, but we realize that the possibility of high-level penetration exists. American democracy is too precious to trust to corporations that have demonstrated so little regard for the security of our elections. Transparency – open and fair elections are something we can't ever take for granted Trust . . . but verify.

Board Request

13. Specify in detail the reason that the Maryland vote counts were delayed during the primary election of 2004 including for each instance of same, the length of same, the reason for same and the name and present address of the election authority experiencing same and the equipment involved in same.

Diebold Response

Diebold places the responsibility for the slow count on precinct workers and the manual transportation of memory cards to the central tabulating location rather than transmitting results over the telephone network.

IBIP Comment

Prince George's County, Maryland - The Board of Elections had technical difficulties last night [September 14, 2004] compiling results. Election workers said the main modem to receive results from the polls had malfunctioned.

Election officials said there were no major problems at polls throughout the day. The only known glitch was at Mount Rainier Elementary School. When polls opened yesterday, nearly a dozen voters were told the machines were not pulling up the Democratic slate. Linda Couch, a Mount Rainier resident, said poll workers told the voters that because the machines weren't operating properly, they could write down their choice on a piece of paper. Couch said some voters left, saying they would try to come back. Others, like her, wrote their selections down on the paper.¹⁴

However, there are also some reports of problems in the November, 2004 election: Voters and poll watchers reported some 531 incidents to TrueVoteMD. Some 201 of these were incidents involving machine malfunctions of various types. The other 330 involved human and organizational failures, including lack of privacy, denials of provisional ballots or the right to vote at all, long lines, and insufficient help from election workers.

¹⁴ **Johnson Aide Wins Democratic Primary - Newcomer Nets a Third of the Vote.** By Ovetta Wiggins Washington Post Staff Writer, Wednesday, September 15, 2004; Page B04 - <http://www.washingtonpost.com/wp-dyn/articles/A22014-2004Sep14.html>

TrueVoteMD only covered 6% of Maryland's precincts. Among the 201 machine failures reported were:

Battery/Electrical Problem 3	Screen Malfunction 30
Late Opening due to Machine Problem 4	Vote Switching 17
Machine Crash 42	Voter Access Card/Encoder Problem 37
Replacement Machine 11	Write-in Vote Problem 9
Review Screen Incorrect 2	Technician Accessing Machine 8

TrueVoteMD says that "Incomplete Electronic Ballots have been reported in many states and every time Diebold machines have been used in Maryland. In the 2004 March Primary, Senator Barbara Mikulski was reported to have been missing from some ballots in three counties. In the November General Election, voters reported candidate Cummings, Ruppertsberger, Wynn, Van Hollen as well as Mikulski as missing from their ballots."¹⁵

Extrapolating only the 163 listed malfunctions from 108 precincts (the other 38 may have been human error) over all of Maryland's 1,787 precincts would indicate that there were approximately 2,700 machine failures statewide.

Board Request

14. Specify in detail the reason(s) that the San Diego County experienced malfunctions of Diebold equipment in the primary election of 2004 including each instance of same, the length of same, the reason for same, the name and present address of the election authority experiencing same and the equipment involved in same.

Diebold Response

Diebold contends that its more than 10,000 touch screens functioned well during the 2004 primary election in Alameda/San Diego County. It quotes extensively from a May 27, 2004 San Diego County Grand Jury Report which is favorable to touch screen machines.

Diebold also says, "Unrelated to the performance of the touch screen systems, these two jurisdictions did experience a battery power issue with an electronic poll book product during the March 2004 primary. This product, which had nothing to do with the actual casting of ballots and the tabulation of votes, has been modified to eliminate the previous issue."

IBIP Comment

One might question the terminology "nothing to do with the actual casting of ballots" inasmuch as 573 of 1,611 polling places, or 36 percent, opened after 7 a.m., and an unknown number of voters were turned away.¹⁶

Diebold also states, "Some of the electronic poll books . . . were in **car trunks** and not recharged before the election . . ." [emphasis added] This of course relates in some part to the issue of security: What were those " . . . computer encoders used to program voter cards to call up electronic ballots on the touch screens . . ." ¹⁷ doing in **car trunks**? And what other Diebold Voting System components were in those same (or other) car trunks?

¹⁵ *When The Right To Vote Goes Wrong: Maryland Citizens Tell the Story of Election Day 2004*, TrueVoteMD, <http://www.votersunite.org/info/content/newmessup-09.asp>

¹⁶ *Grand jury report backs touch-screen voter devices*, By Helen Gao UNION-TRIBUNE STAFF WRITER May 28, 2004, <http://www.signonsandiego.com/news/metro/20040528-9999-1m28voting.html>

¹⁷ *Ibid*

We have previously discussed the issue of absentee ballots, when the GEMS software used to count the scanned ballots malfunctioned, causing 2,821 votes to be miscounted in the Democratic presidential and Senate Republican primaries.

"It is no small irony that the optical scan option that the Secretary of State recommends for use in November is the only component that actually had a failure in the vote tabulation for the 2004 Primary Election," the Grand Jury report said. Of course, that's not the case at all as Diebold has admitted that the problem was not with the optical units, but with GEMS. It is no small irony that this is the software that actually had a failure and that same software tabulates the votes cast on the "flawlessly performing" touch screens.

Board Request

15. List each and every independent testing authority that has tested the Diebold Election equipment for all times subsequent to December 1, 2001 identifying the following for each such authority:
 - a. The equipment tested;
 - b. The name and address of the testing authority; and
 - c. A copy of the results of each said test.

Diebold Response

Diebold correctly identifies Wyle Laboratories and Ciber, Inc. as the ITA's it pays to certify its products.

IBIP Comment

None

Board Request

16. List all insurance policies or security bonds, if any, existing to provide coverage for any hardware malfunction, security malfunction, software malfunction or other malfunction in Diebold equipment used in elections in the State of Illinois specifying for each said policy/bond the name of the issuing company, the number of the policy, the limits of the policy, a brief description of the coverage of the policy and a copy of same.

Diebold Response

Diebold identifies its errors & omissions policy and its carrier.

IBIP Comment

None

Diebold Response No. 17

Diebold has further extended its response by adding Response No. 17 containing "corrections to misinformation" concerning the U.S. General Accountability Office (GAO) report: "Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed" (GAO-05-956). While Diebold claims that "The attached analysis summarizes the findings of the report and distinguishes them from the misinformation contained in the erroneous press reports," this is not the case. Rather than citing a single "erroneous press report," Diebold directly attacks the findings of the GAO report itself, setting up a number of straw men which it tries to knock over with varying degrees of success, or lack thereof.

Diebold also attacks the Illinois Ballot Integrity Project and Dr. Aviel Rubin, while offering its version of an endorsement from a division of NFB, the National Federation of the Blind in Computer Science, attaching a letter from Mr. Curtis Chung.

Diebold devotes nearly five pages to its defense relating to the GAO Report. The report itself, draws relatively broad conclusions throughout its more than 100 pages, seldom if ever mentioning a vendor by name. Diebold's distinguishing of GAO statements "from the misinformation contained in the erroneous press reports" consists primarily of two approaches: 1) We don't do it that way, and 2) The famous "SODDIT Defense." (Some Other Dude Did It), their favorite is Unilect, though ES&S gets a mention. From this we can easily determine that Diebold is neither Unilect nor ES&S. What this adds to the discussion or how it's responsive to the Board's Requests is not readily apparent.

One item, however, did attract our attention. Diebold selects a comment from the GAO report as follows:

Weak Security Management Practices by Voting Machine Vendors, including the failure to conduct background checks on programmers and system developers. The lack of internal security protocols during software development, and the failure to establish clear chain of custody procedures for handling and transporting software.

Diebold Response

Incorrect: All prospective Diebold employees must successfully submit to a complete and thorough background (criminal, financial, substance abuse, etc) review prior to being offered employment. Additionally, all employees must successfully complete a probation period of up to 90 days before gaining permanent employment.

IBIP Comment

Diebold in its response addresses only the first part of this issue pertaining to employee background check, choosing not to address the issue of internal security protocols or the chain of custody procedures for handling and transporting software. And for good reason. A company that leaves 40 **thousand** files on an unprotected FTP site for several years, including files containing code actually used in real elections, source code, internal memoranda, e-mails, probably doesn't have a lot to say about security protocols and chain of custody.

On Feb. 4, 2003, employees of Diebold Election Systems admitted that they had been using an insecure FTP server to exchange and update some part of Diebold's software. Bev Harris had discovered the server by doing a Google search, and she wrote it up in the on-line journal Scoop. This FTP server was taken offline on Jan 29, 2003 and it is alleged to have contained files with names like "rob-georgia.zip", large parts of GEMS (the Global Election Management System), and unknown other software.

We have already discussed the issue of rob-georgia.zip above, but it's interesting to note that this internal security lapse has (and continues) to fuel much of the discussion about Diebold's practices and procedures as well as the actual substance (at least in the developmental stages) of its software. This unguarded FTP site was the reason that Diebold source code was made available to computer experts and researchers during the early part of 2003. Diebold's approach to security was to chase the cat after it was not only out of the bag, but had fostered many offspring. Their approach was to send threatening letters to more than a dozen academic institutions threatening legal action.

One thing the FTP site confirmed was that Microsoft Access was at the heart of their system. Questions about the appropriateness of using Microsoft products, in general, or about the appropriateness of using Microsoft Office components in an application that has critical security issues are very appropriate here.. It has been clear for a decade that use of Access, Office and Windows are inappropriate in critical or high-security applications.

The discussion of security issues with respect to Diebold is often difficult. While Diebold and its supporters blandly state that "Diebold has not had our elections hacked when used in an actual election environment," they offer no proof that such is the case. Instead, Diebold insists that critics should prove that such attacks have occurred. One problem appears to be that Diebold is incapable of providing such proof as the source code language is obsolete from the standpoint that it's not one that would be selected in today's development environment, but rather dates to more than a decade ago.

This is not to say that the software has not been updated, but merely that the language used is vulnerable to memory-corruption and type-confusion attacks. Modern languages such as C#, Java, Modula-3 and others can defend against such attacks. In short, while critics are not in a position to prove such exploits, Diebold can't prove the absence of any such exploits either. If Diebold had written its software in a modern programming language, like Java, which is used in many secure transaction environments, such as banking and securities, the proof would be available for demonstration.

Diebold's security issues go deeper than the unsecured FTP site. Just a few months after the FTP site was shut down, a hacker has come forward with evidence that he broke the security of a private Web server operated by Diebold and made off with Diebold's internal discussion-list archives, a software bug database and more software.

The unidentified attacker provided *Wired News* with an archive containing 1.8 GB of files apparently taken March 2 from a site referred to by the Ohio-based company as its "staff website."

Director of Communications, John Kristoff, said the stolen files contained "sensitive" information, but he said Diebold is confident that the company's electronic voting system software has not been tampered with.¹⁸

While Diebold does set forth a strong (in words) personnel policy, we remind the Board that two key members of the Global Election Systems management team who became part of Diebold's management were Jeffrey Dean and John Elder.

Somehow Diebold let the prison record (<http://bbvdocs.org/dean.pdf>) of programmer and primary stockholder Jeffrey Dean get by them, and also forgot to look at the record of John Elder who they put in charge of their ballot printing facility.

Jeffrey Dean was convicted on 23 counts of felony embezzlement (theft in the first degree) by rigging a computer system to steal. He later became the programmer for Diebold who created the 1.96 optical scan system. Dean was incarcerated by the State of Washington from late 1991 through early 1995 and was also required to pay \$385,227.05 (plus interest) in restitution.

John Elder ran the Diebold ballot printing plant until shortly before the Nov. 2004 election. He is a convicted narcotics trafficker. Here are his prison records: <http://www.bbvdocs.org/elder.pdf> Elder was convicted of Violation of the Uniform Controlled Substance Act, Delivery of a Controlled Substance, to wit: Cocaine. Elder was incarcerated by the State of Washington from late 1991 through early 1996, and spent about nine months with Jeffrey Dean at the Washington State Cedar Creek Correctional facility in 1994-95. Both were assigned to the DNR/Fire Crew according to Correctional Department records.

We suggest that Diebold's "thorough background review" was just about as effective in preventing the employment of convicted felons as its ethics policy was in preventing the overt political activity of its CEO and other senior management employees.

¹⁸ ***New Security Woes for E-Vote Firm*** - By Brian McWilliams, *Wired News*, August 7, 2003, <http://www.wired.com/news/privacy/0,1848,59925,00.html>

Conflict of Interest

Dr. Aviel Rubin and VoteHere

In their response, Diebold raises the issue of conflict of interest, specifically citing the document quoted by the Illinois Ballot Integrity Project in its 12 December 2005 submission to the Board. Specifically, Diebold states:

The document presented by the Illinois Ballot Integrity Project references a report completed by Johns Hopkins and authored by Avi Rubin, which highlights security issues in electronic voting and **strongly promotes a method so voters can verify their selections**. Shortly after the publishing of this report, it was discovered that Mr. Rubin had stock options in a company that provided a verification system for voting systems. His disclosure of owning the stock options providing a conflict of interest can be found in the following document: [emphasis added]

http://www.jhu.edu/news_info/news/home03/aug03/votehere.html

The report, "Analysis of an Electronic Voting System," was authored not only by Dr. Aviel Rubin, but three other professors from Johns Hopkins, University of California at San Diego and Rice Universities, and is dated February 27, 2004. <http://avirubin.com/vote.pdf> The URL provided by Diebold leads to a press release by Dr. Rubin of August 17, 2003, shortly after the report was issued as a Johns Hopkins' document, "Johns Hopkins University Information Security Institute Technical Report TR-2003-19," July 23, 2003. In his statement, Dr. Rubin says:

I am on the advisory board of VoteHere Inc. Had I considered my relationship with VoteHere, I would have disclosed it at the time that the report on the Diebold software was released. However, I had not had any contact with VoteHere since I signed on to their board over two years ago, and I simply did not remember nor think about it. In hindsight, that is very unfortunate. I should mention that my research on the Diebold code was not funded by any corporate support, and to the extent that it was funded at all, it was internal Johns Hopkins funding.

Effective immediately, I am resigning from the technical advisory board of VoteHere, and I am returning all stock options. They have never been exercised and are not entirely vested. I have never profited in any way from my affiliation with VoteHere, and by returning my stock options in their entirety, it is assured that I never will.

The report gained general circulation after its May, 2004 publication by the IEEE when it appeared in the *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004, long after Dr. Rubin had severed his rather insignificant ties with VoteHere, Inc.

An examination of the 23-page report reveals that the method "strongly" promoted is mentioned in two places: One sentence in the abstract:

We suggest that the best solutions are voting systems having a "voter-verifiable audit trail," where a computerized voting system might print a paper ballot that can be read and verified by the voter.

And in one paragraph in the conclusion:

Alternatively, security models such as the voter-verified audit trail allow for electronic voting systems that produce a paper trail that can be seen and verified by a voter. In such a system, the correctness burden on the voting terminal's code is significantly less as voters can see and verify a physical object that describes their vote. Even if, for whatever reason, the machines cannot name the winner of an election, then the paper ballots can be recounted, either mechanically or manually, to gain progressively more accurate election results. Voter-verifiable audit trails are required in some U.S. states, and major DRE vendors have made public statements that they would support such features if their customers required it. The EVM [Electronic Voting Machine] project is an ambitious attempt to create an open-source voting system with a voter-verifiable audit trail—a laudable goal.

Interestingly enough, in its response, Diebold does not dispute the factual basis for the analysis nor the conclusions reached regarding the serious security issues with respect Diebold source code.

We will leave it to the Board's discretion to determine if the suggestion of a voter-verified audit trail as an alternative to open-source code, without mentioning any product or company, constitutes a "conflict of interest" when the paper receives formal publication some months after one of the four authors has severed ties with a company he had little or no contact with and none in the two years prior to publication.

Further, we would bring to the Board's attention that three additional reports, subsequent to the publication of "Analysis of an Electronic Voting System," have come to the same conclusions and support the findings of the group which authored this paper.

The first of these, "Risk Assessment Report Diebold AccuVote-TS Voting System and Processes," September 2, 2003, was prepared by Science Applications International Corporation (SAIC) for the State of Maryland:

http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf

It states:

In the course of this Risk Assessment, we reviewed the statements that were made by Aviel. D. Rubin, professor at Johns Hopkins University, in his report dated July 23, 2003. In general, SAIC made many of the same observations, *when considering only the source code*.

This Risk Assessment has identified several high-risk vulnerabilities in the implementation of the managerial, operational, and technical controls for AccuVote-TS voting system. If these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results.

In November, 2003, Compuware completed a report for the Ohio Secretary of State, Kenneth Blackwell, "Direct Recording Electronic (DRE) Technical Security Assessment Report." (a report Blackwell suppressed for a number of months) <http://www.sos.state.oh.us/sos/hava/compuware112103.pdf>

Commenting on Diebold (one of several systems tested), Compuware said:

During the course of our study, Compuware has identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented above. Following careful consideration of each of these security issues, we have developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack on the election process.

This was followed by the January 20, 2004 report "Trusted Agent Report Diebold AccuVote-TS Voting System," completed also for the State of Maryland by RABA Technologies.

http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf In this report we find:

The State of Maryland election system (comprising technical, operational, and procedural components), as configured at the time of this report, contains considerable security risks that can cause moderate to severe disruption in an election.

A considerable amount of press has been given to the "Hopkins report." The subsequent revelation of a conflict of interest involving one of its authors with a Diebold competitor has only served to detract from the substance of the results. The single most relevant finding in this section is that the general lack of security awareness, as reflected in the Diebold code, is a valid and troubling revelation. In

addition, it is not evident that widely accepted standards of software development, such as the Carnegie Mellon Software Engineering Institute's Capability Maturity Model® for Software and System Security Engineering (SW-CMM and SSE-CMM), were followed.

In summary, it would appear that the so-called "conflict of interest." If it indeed existed was such that the mere "suggestion" of a verified voter paper audit trail (VVPAT) was seen by Diebold as "strongly promoting" such a system. Perhaps in retrospect there might be some such perception on Diebold's part as it certainly has come to be accepted by the Illinois Legislature which through HB 1968 has added such language to the Illinois Election Code (10 ILCS 24/C-2):

This permanent paper record shall (i) be printed in a clear, readily readable format that can be easily reviewed by the voter for completeness and accuracy.

It is of course this provision of the Code that we believe Diebold seeks to satisfy (unsuccessfully) with its use of the AccuView printer in conjunction with the AccuVote TSX.

Diebold and the National Federation of the Blind

Ironically, in the next paragraph of their response, Diebold states:

The following is a letter of reference from the National Association of the Blind. Diebold has been an active partner of the NFB for over five years. The top technical person with the NFB participated on the design team of the Diebold ACCUVOTE-TSX touch screen voting station, which provides excellent accessibility for blind and disabled voters.

Diebold appends a letter, dated April 28, 2005, from Curtis Chung, President of the National Federation of the Blind in Computer Science (a division of the NFB). In this letter, Mr. Chung states:

On behalf of the National Association for the Blind in Computer Science, I wish to express our wholehearted support for the ACCUVOTE-TSX touch screen voting station and its ability to provide full access for blind voters to the secret ballot in local, state and national elections.

This "endorsement" of course extends only to the supposed advantages of the AccuVote-TSX with respect to non-sighted voters, rather than the more broadly stated "excellent accessibility for blind and disabled voters" stated in the Diebold response.

Just how well the AccuVote-TSX works for voters with disabilities compared to other devices might be inferred from this article, "Spencer Lane Report on Voting Technology Accessibility," posted online at (<http://www.verifiedvotingfoundation.org/article.php?id=6135>). On June 7, 2005, Lane visited the Annual Conference of the Florida State Association of Supervisors of Elections at which voting machines were on display.

The article had this to say about the AccuVote-TSX:

After several unsuccessful attempts to boot the system, the disabled interface was moved to the 2nd machine. My wife and I then "voted" on 202010 (sans interface) while Paton, voted on the disabled configured machine, 201267. With the screen blanked off, a synthesized voice led her through the ballot. My wife had a problem that it took 5-7 screen "pushes" before any of her actions registered. We observed that and postulated that perhaps her nails (which were slightly longer than mine) may be causing the problem. Even with her repeated pushes, her vote took just over three minutes. I had no problems and my fat fingers got a response on each touch, completing my ballot in just under three (3) minutes.

Paton's vote using the handicapped audio interface to outline the ballot through headphones took 31 minutes, much longer than I had thought it would.. The handicap interface was a "telephone keypad"

style with 12 keys to be selected than pressed. To select the appropriate key number required sightless touch-counting of the keys to locate the correct one before it could be pressed. (Think of placing a call on a telephone in the dark)

Interestingly enough, this is the same interface lauded by Mr. Chung in his letter. Another disadvantage pointed out was:

In the audio review of her ballot after it was cast on the Diebold TSX Touchscreen unit with Florida approved software, the synthesized voice says, "Your choice has been selected" without specifying just what that choice was. Without audible verification in her headset she had no way of knowing if the votes she cast were recorded correctly.

Paton Axelrod also tested the ES&S Automark system for handicapped voters, as our seriously sight-impaired voter. With the screen darkened (as was the Diebold) and going through a similar audio interface, Paton listened to the complete ballot and voted on all the choices. The voting took only 9 minutes, less than one third the 31 minutes the Diebold required. The through-put of 6 sight-impaired voters per hour on the AutoMark vs only 2 per hour on the Diebold seems extremely advantageous.

Thus it would appear that Mr. Chung hardly speaks for all non-sighted or disabled voters. And in fact, there is some substantial disagreement. And of course Mr. Chung's "wholehearted" endorsement of the Diebold AccuVote-TSX might carry more weight were it not for the more than \$1 million dollars Diebold has contributed to the NFB.

This is not to say Diebold's partnership with NFB is necessarily dubious. Though one does wonder how the AccuView printer record can be made accessible as President Marc Maurer of the National Federation of the Blind demanded on July 2, 2004:

We have not insisted that paper receipts be produced, but neither have we insisted that they be avoided. If they are produced, we want them to be accessible to us, and we insist that blind people get the right to a secret ballot along with everybody else.

The National Federation of the Blind has a venerable 65-year history of advocacy for the rights of the visually impaired and the blind. We believe, however, that as the *New York Times* suggested on June 11, 2004: "The National Federation of the Blind, for instance, has been championing controversial voting machines that do not provide a paper trail. It has attested not only to the machines' accessibility, but also to their security and accuracy--neither of which is within the federation's areas of expertise."

We have attempted to contact Mr, Chung to determine what tests might have been conducted on the Diebold AccuVote-TSX and other voting terminals. Unfortunately, we've not been successful in doing so.

As a final word, "No one votes unassisted on a computer; everyone is "assisted" by anonymous programmers." - *Mark Ortiz – candidate for US Representative, 8th District - NC*

Summary and Conclusion

Overall, we found the Diebold response to be somewhat less than responsive to the Board's Requests. This was especially true with respect to the response to Board Request No. 1 wherein it would appear that Diebold has never experienced any system or mechanical failure anywhere, anytime that weren't the fault of slow precinct workers (Maryland), or connecting too many optical scanners to the GEMS tabulation system or poll workers leaving encoders in their car trunks. (Alameda and San Diego Counties). It's always somebody else's fault. We are left with the impression that once Diebold changed the power switch on the encoder, everything was ship-shape. Dozens of other reported problems were simply swept under the rug.

Setting aside Board Requests Nos 2-4, we find that the response to Board Request No. 5 to be less than complete, providing only Diebold's rebuttal position.

The response to Board Request No. 6 is technically accurate. That to No. 7, however, regarding the file rob-georgia.zip is precisely contrary to that given by Rob Behler, the person who was its intended recipient and user. We'll leave it to the Board to judge the veracity of the parties. We really don't have much comment on either Board Request No. 8 or 9. We have no reason to believe that the response to No. 8 is anything other than as stated and No. 9 is simply not answered.

Diebold chose not to answer Board Request No. 10, choosing instead to posit an "ethics policy" which was so flagrantly disregarded by Diebold's top management as to be insulting to the Board. There is no proven (or even sufficiently alleged) nexus between Diebold and the Ohio Republican Party (other than a significant amount of money) to make either Board Request No. 11 or Diebold's response have much bearing on the certification issue. We felt Diebold's answer to Board Request No. 12 to be disingenuous at best. Sufficient information is simply not available to provide a good response to Board Request No. 13. Diebold's response to Board Request No. 14 shows considerable agility in avoiding the issue. Board Requests Nos. 15 and 16 appear to have been answered.

Unfortunately, Diebold Response No. 17 hardly lives up to its billing, failing to provide even a single example how how "The actual findings of the GAO report have unfortunately been misconstrued by several media outlets." Diebold's *ad hominen* attack on the GAO does little to advance its cause.

Similarly, the attempt to discredit Dr. Aviel Rubin and the Illinois Ballot Integrity Project falls short of the mark, especially when juxtaposed with Diebold's "endorsement" by the National Federation of the Blind in Computer Science, a division of an organization that has received more than \$1,000,000 in hard and soft contributions from Diebold. Diebold would have been better served to factually address the findings of the *Hopkins Report*. Far from "killing the messenger," Diebold hardly inflicted even a minor flesh wound.

The Illinois Ballot Integrity Project renews its statement of conclusions as set forth in its December 12, 2005, submission to the Board, to wit:

- Diebold Voting System components have a long and well-documented history of hardware, software and communications failures.
- Diebold Voting System components, particularly the AccuView printed output, fail to conform to the statutory requirements of the Illinois Election Code.
- The GEMS[®] (Global Election Management System) and the AccuVote-TSX[™] DRE pose significant security concerns and have been demonstrated to be susceptible to "hacking."
- The Diebold AccuVote-TSX[™] DRE compares unfavorably with other technology available to assist disabled voters which could be used to comply with Section 301(a) of Title III of HAVA.
- Diebold Election Systems, Inc. (DESI) has demonstrated a history of fraudulent activities in installing uncertified software in multiple jurisdictions and has made false claims about certification of equipment and systems.
- The Diebold AccuVote-TSX[™] direct record entry (DRE) terminal, AccuView[™] printer, AccuVote-OS[™] optical scan device and GEMS[®] (Global Election Management System) do not meet the criteria set forth in the Illinois Election Code requiring reliable and secure voting systems.

For these reasons, as more fully explicated in our December 12, 2005 submission, and as set forth in the foregoing commentary, we believe the Illinois Board of Elections should, in the public interest, deem the Diebold Response to the Board's Questions and Requests inadequate and decide not to make final its interim certification of the Diebold AccuVote-TSX DRE terminal and AccuView printer, by revoking its conditional certification granted on December 20, 2005.