



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

FOR IMMEDIATE RELEASE

Contact: Robert A. Wilson bobwilson@consultant.com (847) 644-2654

DIEBOLD HOUSE OF (MEMORY) CARDS COLLAPSING

Evanston IL, December 14, 2005. In a White Paper delivered to members of the Illinois State Board of Elections (SBOE) this week, the Illinois Ballot Integrity Project (IBIP) has outlined its opposition to the Board's proposed certification of electronic election systems manufactured by Diebold Election Systems, Inc, of North Canton, Ohio, a subsidiary of Diebold, Inc. (NYSE: DBD). Interim certification for Diebold system components is a scheduled agenda item for the Board's regular monthly meeting at the Thompson Center in Chicago next Tuesday, December 20th at 10:30 am.

The IBIP White Paper, "Diebold Voting Systems Should not be Certified by the Illinois State Board of Elections," contains documentation of dozens of significant failures of Diebold systems including its AccuVote-TSX[™] direct record entry (DRE) touch-screen voting terminal, AccuView[™] printer, AccuVote-OS[™] optical scan device and GEMS[®] (Global Election Management System) tabulating software. The White Paper includes an extensive 22-page compendium of news articles, "Diebold in the News," assembled by Voters Unite, an election activist group (www.votersunite.org).

"Diebold election systems have proven time and again that they are unreliable and insecure," said Laurence J. Quick, state chairperson of the Illinois Ballot Integrity Project. "This White Paper sets forth in significant detail why certifying Diebold touch screen terminals and other system components would be a real disservice to the voters and taxpayers of Illinois," he continued.

Much of the controversy has centered around Diebold's AccuVote-TSX[™] touch-screen devices and its GEMS[®] tabulating software. Leading voting system experts have shown that both the voting terminals and the software that counts the votes are particularly susceptible to "hacking" which would allow malicious changes to alter election results. In addition to lack of security, electronic voting systems, including Diebold's, have proven unreliable, often breaking down during elections, leading to election officials having to resort to the more reliable paper ballots.

In early December, a "summit" of election officials and public interest groups was held in Sacramento, California. Carnegie Mellon University computer expert Michael Shamos, told the assemblage of voting-system makers, elections officials and scientists: "I have good reason to believe that 10 percent of systems are failing on Election Day. That's an unbelievable number."

Diebold's AccuVote-TSX[™] touch-screen devices were originally designed to offer only "invisible ballots," with no paper record of votes cast. The recently revised Illinois Election Code requires that voters be able to cast ballots that can be "easily reviewed by the voter for completeness and accuracy." In an attempt to meet new standards, Diebold has retrofitted its AccuVote-TSX[™] touch-screen devices with a printer called the AccuView[™] which is supposed to print a ballot record on a thermal paper roll. Integrating a printer into the older hardware has proven to be a challenge, however. When the system was tested by Chicago and Cook County election officials, several machines produced blank paper rolls. A competitor's system was selected.

In addition, IBIP contends that Diebold AccuView[™] printer does not produce a Voter Verified Paper Audit Trail (VVPAT) immediately after a ballot is cast that includes "a permanent paper record of each ballot cast that shall be available as an official record for any recount, redundant count, or verification or re-tabulation of the vote count conducted with respect to any election in which the voting system is used," (10 ILCS 24/C-2) in that the AccuView[™] printer uses a continuous roll of degradable thermal imaging paper retained within the device. IBIP also found that the method used to "audit" or recount ballots from

the AccuVote-TSX™ touch-screen device does not use an image of the ballot, but relies on a barcode which would be read by a separate reader.

"This is hardly something that can be easily reviewed by the voter for completeness and accuracy," said Roy Lipscomb, a Chicago-based computer consultant and IBIP's director of technology. "While there are many reasons for not allowing Diebold systems to be used in Illinois, they ought to be disqualified for this reason alone," Lipscomb added.

Diebold's GEMS® (Global Election Management System) tabulating software has also come under fire for the so-called "Gems Defect." First reported by Bev Harris and Dr. Herbert Thompson of Black Box Voting www.blackboxvoting.org, and independently confirmed by the security consultant firm CompuWare on commission from the state of Ohio, the GEMS Defect concerns the central vote tabulating database that accumulates all the precinct and absentee votes for all Diebold optical scan and touch-screen voting systems. The GEMS Defect allows VBA (visual basic script) to rewrite the access database containing the vote count without a trace. According to the Aug. 18, 2004 report by CompuWare Corp., ". . . an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results."

"Votergate the Movie," available for free download at (<http://www.votergate.tv>) contains footage from a national TV broadcast of Bev Harris instructing Dr. Howard Dean how to hack GEMS and untraceably alter vote tallies in under two minutes.

Diebold has published a "rebuttal" to certain types of security breach protocols that have been previously documented by voter activists. (<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. Unfortunately, this is not always possible and Diebold itself has admitted to several instances, one specifically in Volusia County Florida, in which security may well have been breached with "a second memory card." Diebold further contends that, "During the twenty year usage of electronic voting, no validated security breach has ever been recorded. GEMS is not vulnerable . . . because the system as a whole is designed to eliminate vulnerability from a single point of attack.

Interestingly enough, the U.S. Department of Homeland Security had this to say about GEMS in Cyber Security Bulletin SB04-252, issued for the first week of September, 2004: "A vulnerability exists due to an undocumented backdoor account, which could allow a local or remote authenticated malicious user [to] modify votes. No workaround or patch available at time of publishing."

Undocumented software has been a problem for Diebold and its customers. In April, 2004 California Secretary of State Kevin Shelley called on the State's Attorney General to bring criminal charges against Diebold 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. Shelley blasted Diebold for what he called a "culture of deceit"

California Attorney General Bill Lockyer eventually 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. The suit, filed under seal and in the name of state and local taxpayers, alleged that Diebold sold a nearly \$13 million touch-screen system to Alameda County by misrepresenting its accuracy, security and government approval. 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.

"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."

In November, 2004, Diebold agreed to pay \$2.7 million to settle the lawsuit. In a "Privileged and Confidential" memorandum from Diebold's law firm, Jones Day, leaked to the *Oakland Tribune* last year, it was revealed that the company's legal fees for just one two month period in the state of California were estimated at \$535,000 - \$925,000 in addition to the settlement costs. The memo outlined fees for "legal analysis of potential criminal violations, white collar criminal law attorney pre-grand jury investigative advice" and even costs to "monitor selected web sites to gain key intelligence."

Commenting on recent developments, Bob Wilson, chairperson of the Suburban Cook County Chapter of IBIP said, "This week, Diebold hit the trifecta," referring to three days of consecutive "bad news" stories on Diebold involving the resignation of it's CEO,. A successful "hack" of the AccuVote-OS™ optical scan device in Leon County Florida and the filing of a class action suit by Diebold stockholders.

1. Diebold CEO Resigns

Reuters, http://yahoo.reuters.com/financeQuoteCompanyNewsArticle.jhtml?duid=mtfh13787_2005-12-12_21-35-36_wen6080_newsml reported Monday that Diebold's Walden W. O'Dell abruptly resigned, citing "personal reasons," his positions as chairman and chief executive officer with Thomas W. Swidarski, currently the firm's president and chief operating officer, named to take over as chief executive officer.

O'Dell was widely criticized by opponents for his August 14, 2003, fundraising letter on behalf of the Bush/Cheney campaign in which he promised to deliver Ohio for George W. Bush in 2004. O'Dell had attended a strategy pow-wow with wealthy Bush benefactors - known as Rangers and Pioneers - at the president's Crawford, Texas, ranch earlier that month - a group of individuals who had raised at least \$100,000 each for Bush/Cheney's 2004 re-election campaign.

The next week, he penned invitations to a \$1,000-a-plate fund-raiser to benefit the Ohio Republican Party's federal campaign fund - partially benefiting Bush. The letter went out the day before Ohio Secretary of State Ken Blackwell, also a Republican, was set to qualify Diebold as one of three firms eligible to sell upgraded electronic voting machines to Ohio for the 2004 election.

In the wake of the controversy concerning O'Dell's involvement with the Bush/Cheney campaign, a corporate policy was instituted to disallow involvement in political campaign by senior executives at the company. Last Thursday, however, the *Cleveland Plain Dealer* revealed that several Diebold executives continued to donate to various GOP campaigns, nationally and in Ohio even after the policy was enacted. <http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/113403461250230.xml&coll=2>

Speculation on Monday was that O'Dell's resignation, however, was also related to the significant drop in earnings and the price of Diebold shares.

2. Diebold Booted in Florida

And in Florida, just yesterday, Tuesday, December 13th, a test election was run in Leon County 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 of Black Box Voting and by Harri Hursti, widely recognized international computer voting expert, 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, the "mother ship" that pulls in all votes from voting machines. The results in the central tabulator read: Yes:7 No:1.

This "hack" was accomplished without Hursti or Thompson being given any password, using only the same level of access given thousands of poll workers across the USA, showed that the votes themselves were changed in a one-step process. This hack would not be detected in any normal canvassing procedure, and it required only a single a credit-card sized memory card of the type you can purchase at any major office supply store.

Due to contractual non-performance and security design issues, Leon County supervisor of elections Ion Sancho (<http://www.leonfl.org/elect/MeetTheSupervisor.htm>) told Black Box Voting that he will never again use Diebold in an election. He has requested funds to replace the Diebold system from the county. He will issue a formal announcement to this effect shortly.

3. Diebold Faces Class Action Suit

Again, yesterday (wasn't the 13th unlucky for Diebold?) Scott+Scott, LLC (<http://www.scott-scott.com>), representing Diebold stockholders, filed a securities fraud class action in the United States District Court for the Northern District of Ohio against Diebold Inc. and individual defendants. The suit alleges that Diebold and certain company officers violated provisions of the United States securities laws causing artificial inflation of the Company's stock price. According to the complaint the Company lacked a credible state of internal controls and corporate compliance and was unable to assure the quality and working order of its voting machine products.

Plaintiffs claim that the company's false and misleading statements concealed significant internal problems, culminating in false representations of "astonishingly low and incredibly inaccurate" restructuring charges for the 2005 fiscal year, which grossly understated the true costs faced in restructuring the company. The complaint also alleges over \$2.7 million of insider trading proceeds obtained by individual defendants.

As a result of what plaintiff's say was "shocking news and disclosures" of September 21, 2005, the price of Diebold shares plunged 15.5% on unusually high volume, falling from \$44.37 per share on September 20, 2005, to \$37.47 per share on September 21, 2005. In all, Diebold has fallen from a high of \$57.82 in April, 2005, to its close on December 9, 2005 at \$37.62, off slightly more than \$20 or about 35%.

In a related action, Stull, Stull & Brody, (<http://www.ssbny.com/filedcases/diebold.html>) representing employees, today (December 14, 2005) filed a class action law suit against Diebold, alleging virtually the same facts as the stockholders' suit by Scott+Scott, LLC. The suit is on behalf of employees who purchased company stock for their 401(k) plans.

Stull, Stull & Brody also announced that it has commenced an investigation relating to the 401(k) defined contribution plan of Diebold.. The firm is investigating whether fiduciaries of the 401(k) plan of Diebold may have violated the Employee Retirement Income Security Act of 1974 ("ERISA") by failing to disclose the company's true financial and operating condition to participants and beneficiaries of the plan and/or by offering Diebold stock as an investment option under the plan when it was not prudent to do so.

"It should be clear to the Board that Diebold is not a company that election authorities in Illinois ought to consider when purchasing election systems," said Bob Wilson. "As a self-anointed 'global leader' in election systems, Diebold has proven to be particularly inept in providing secure and reliable systems. They have compounded those deficiencies by misrepresenting their products and services to election officials throughout the United States, including in Illinois," he added.

"Election activists have been branded as "kooks" and "conspiracy nuts" by vendors and election officials who have failed to appreciate the dangers of privatizing elections in America, commented Larry Quick,

IBIP chairperson. He continued, "This week's events simply reinforce what activists have been saying all along, we're no longer a voice in the wilderness."

"Even the U.S. Government Accountability Office has come to the same conclusions as the Illinois Ballot Integrity Project, said Wilson, referring to the GAO report released in October which was highly critical of electronic voting systems. The report, entitled "ELECTIONS, Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed" (GAO 05-096) said:

"While electronic voting systems hold promise for a more accurate and efficient election process, numerous entities have raised concerns about their security and reliability, citing instances of weak security controls, system design flaws, inadequate system version control, inadequate security testing, incorrect system configuration, poor security management, and vague or incomplete voting system standards, among other issues."

In its key findings, the GAO listed some examples of voting system problems and vulnerabilities:

- Cast ballots, ballot definition files, and audit logs could be modified.
- Supervisor functions were protected with weak or easily-guessed passwords.
- Systems had easily picked locks and power switches that were exposed and unprotected.
- Local jurisdictions misconfigured electronic voting systems, leading to election day problems.
- Voting systems experienced operational failures during elections.
- Vendors installed uncertified electronic voting systems.

In addition to identifying potential vulnerabilities, GAO identified a number of cases of operational failures in real elections. These examples included:

- In California, a county presented voters with an incorrect electronic ballot, meaning they could not vote in certain races.
- In Pennsylvania, a county made a ballot error on an electronic voting system that resulted in the county's undervote percentage reaching 80% in some precincts.
- In North Carolina, electronic voting machines continued to accept votes after their memories were full, causing over 4,000 votes to be lost.
- In Florida, a county reported that touch screens took up to an hour to activate and had to be activated sequentially, resulting in long delays.

In summarizing the GAO Report, Government Reform Committee Ranking Member Henry A. Waxman (D-CA) said:

"The GAO report indicates that we need to get serious and act quickly to improve the security of electronic voting machines. The report makes clear that there is a lack of transparency and accountability in electronic voting systems - from the day that contracts are signed with manufacturers to the counting of electronic votes on Election Day. State and local officials are spending a great deal of money on machines without concrete proof that they are secure and reliable. American voters deserve better."

"The Illinois Ballot Integrity Project believes that one way the Illinois State Board of Elections could demonstrate that they are serious is to deny certification to Diebold Election Systems," concluded IBIP chairperson, Larry Quick.

The **Illinois Ballot Integrity Project** is a not-for-profit, non-partisan civic organization dedicated to the correction of election system deficiencies and ensuring fair, accurate, and completely transparent elections. IBIP believes that fundamental to election integrity is the inscribing of all votes (whether by hand or by machine) on durable paper ballots which are easily handled and verified by the individual voter. The voter's paper ballot should be the only official ballot for purposes of casting, tallying, counting, audit and recount.

The **Mission** of the **Illinois Ballot Integrity Project** is to inform and educate the public, media and government officials about important election integrity issues and to promote the adoption of legislation and policies designed to secure the democratic process.

For more information about IBIP – visit www.ballot-integrity.org

A copy of the IBIP White Paper is attached in Adobe PDF

###