



Wisconsin

Who we are

Voter Action Wisconsin is a new project of Voter Action. Voter Action is a national not-for-profit organization that provides legal, research and organizing support to ensure election integrity in the United States. Voter Action is currently a project of the International Humanities Center, a 501c3 organization. We are dedicated to protecting the democratic process, and ensuring that our elections remain in the public domain. We support the basic right of every voter to have his or her vote recorded as intended and counted accurately. Our work focuses on litigation and public education in support of these goals.

Background

In response to the 2000 election problems, the 2002 Help America Vote Act (HAVA) was enacted with the purpose to make voting in the United States more reliable and secure for all voters. Federal statutory deadlines for purchase and deployment of new voting machines mandated by HAVA have produced a sense of urgency among elections officials. Beginning in 2006, HAVA required all 50 states to provide at least one voting system in each polling place to enable people with disabilities to vote independently and privately. HAVA also provided funding to pay for these voting systems. Wisconsin has allocated \$18 million for the purchase of one accessible voting system per polling place (up to \$6000 per voting system per polling place)

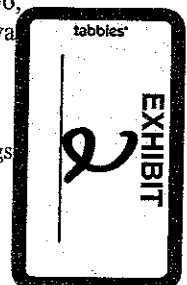
Through strong industry lobbying efforts, "Direct Record Electronic" (DRE) touch screen voting machines were promoted as the solution for the disability access mandate when in fact they do not accommodate all disabled voters and have repeatedly failed to record and store votes accurately and securely.

In New Mexico, for example, an analysis done by Dr. John Skelly¹ of the official November 2004 results revealed an unusually high rate of "undervotes" (ballots cast but no votes recorded), phantom votes (more votes than ballots counted) and vote recording and counting errors on specific electronic voting equipment in certain communities. Skelly stated that "when phantom votes are taken into consideration, the rate of undervotes rises to 2.72% (21,084 undervotes)". Presidential undervote rates as high as 37% plagued some Hispanic and Native American precincts, yet when voters from those same precincts voted on optical scan paper ballots, the undervote rate fell to less than 1%.

Based on a detailed analysis of the official 2004 New Mexico general election results, a lawsuit was filed in January 2005 requesting a permanent injunction against the use of specific voting machines and systems that consistently demonstrated gross problems and irregularities. Legal discovery in the case commenced in the fall of 2005 and revealed important documents and testimony of national significance. In December 2005, plaintiffs filed a motion for temporary restraining order supported by compelling expert testimony that prevented the Secretary of State from using federal funds to purchase hundreds more of the inaccurate and untrustworthy electronic voting machines. On January 12, 2006, Governor Richardson announced a plan to go to an all paper ballot voting system for the state that was signed into law in late February.²

¹ Affidavit of Dr. John Skelly, January 14, 2005 submitted as Plaintiff Exhibit A, New Mexico legal proceedings

² Open Letter to the State Officials of the 50 States by New Mexico Governor Bill Richardson, March 2, 2006.



On February 15th 2006, Republican Governor Robert Ehrlich of Maryland joined Democratic Governor Bill Richardson in expressing his desire to make his state, like New Mexico, an all paper ballot state due the "unreliability and tremendous costs of DRE voting systems." In a letter to the Maryland State Board of Elections, Governor Ehrlich reported cost overruns of over 1000% for maintenance of the state's touch screen voting systems³

Current Issue in Elections: HAVA and Direct Record Electronic (DRE) Voting Machines

National elections in 2002, 2004, and 2006 have shown that DRE voting systems have demonstrated significant problems. They have broken down, failed to boot up, undervoted (ballots cast but no votes recorded) and counted votes backwards. There have been high numbers of vote switching incidents (a vote switch occurs when a voter selects one candidate but another choice appears on the screen of an electronic voting machine)⁴. Vote losses were also linked to specific brands and models of voting machines, mirroring other widely reported incidents across the nation. In New Mexico approximately 12,000 votes had been lost⁵.

When electronic voting systems break down it is most often the vendors' technicians that are dispatched to fix the problems, creating even more security risk and increasing cost burdens for the counties. Machine breakdowns contribute to the creation of long lines and voter disenfranchisement. Voting on DRE voting systems also takes much longer for both disabled and non-disabled voters, exacerbating the problem.

There are other problems with DRE voting systems. Independent testing has shown that they contain illegal software code that creates a high risk of large-scale insider fraud. The voluntary federal certification process, paid for by the vendors, has failed to find or alert elections officials to the use of this illegal code. Seemingly, every week new and startling evidence is found and reported in the media.

The top 3 electronic voting systems including Sequoia Edge II, Diebold TSX, and ES&S I-Votronic have all been certified for sale in the State of Wisconsin. All have a history of serious and repeated security risks, errors, failures, disability access inadequacies and massive vote loss.

Wisconsin is one of 23 states requiring voting machines to produce a voter verified paper audit trail (VVPAT) as a means of voter verification (and a record that would enable a manual count or recount).

However, printers that have been provided as a means of verification for the electronic voting machines by the voting machine vendors certified for use in the State of Wisconsin have shown to be unreliable for verification or back up. Rather than provide more useful printers for the DRE machines, vendors have instead chosen to use narrow, continuous-roll thermal paper tapes that do not adequately accommodate meaningful recounts and audits.

Experience from recent primary elections in 2006 has shown that the printers fail to print, jam up, and don't synch up to the electronic screen. They are also impractical for auditing or recounts since they use continuous roll thermal paper that may deteriorate with handling and raises voter privacy concerns. Even if a discrepancy in the vote count could be identified, the very nature of these systems makes them ripe for election challenges where judges and not the voters will determine the outcome of elections.

³ Letter by Governor Robert Ehrlich to Maryland State Board of Elections, February 15, 2006.

⁴ Affidavit of Joyce Bartley, October 28, 2005 submitted as Plaintiff Exhibit K in New Mexico legal proceedings.

⁵ Affidavit of Attorney James Noel, December 19, 2005 submitted as Plaintiff Exhibit F in New Mexico legal proceedings.

Wisconsin has also certified 2 ballot marking devices; the Automark and the Vote Pad. As these systems employ paper ballots that can be optically scanned, they are more able to stand up to a recount and providing access in a more secure and verifiable process.

Scientific Reports Confirm Serious Security Risks With DRE Voting Machines

In 2003, Dr. Aviel Rubin, Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University, author of several widely used books on the subject of computer and network security, and chair of several of the top security research conferences analyzed the source code for the Diebold AccuVote TS direct recording electronic (DRE) voting machine and wrote a report citing many security flaws that he found.

Since his research team's 2003 study of the Diebold software code came out, seven other major studies have been released. All have identified serious security vulnerabilities in DREs.

1. September 2, 2003 - "Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes," *commission by the Governor of the State of Maryland Science Application International Corporation ("SAIC")*. The report identified 328 security flaws, 26 of them "critical" and concluded that "[t]he system, as implemented in policy, procedure, and technology, is at high risk of compromise." Diebold offered to make free software modifications for Maryland, but not for customers in other states.
2. December 2, 2003 - Ohio Secretary of State released a "DRE Technical Security Assessment" (prepared by a private firm, Compuware). The report assessed touch screen voting systems sold by Diebold and three other vendors. It found the Diebold AccuVote TS voting system had more security risks rated "high" than any other vendor. It stated that the same PIN—1111—was used on all supervisor smart cards issued nationwide, and that an unauthorized person could use it to gain access to supervisor functions on the voting terminal. The report also found that an unauthorized person could use the widely available Microsoft Access database program to change ballot definition files and election results in the Diebold GEMS software.
3. January 20, 2004, the Maryland Department of Legislative Services released a report on Diebold product security entitled "Trusted Agent Report: Diebold AccuVote-TS Voting System," prepared by RABA Technologies LLC ("RABA Report"). The RABA team, which included two prominent computer security professors and several former National Security Agency and Central Intelligence Agency computer security experts, identified numerous security vulnerabilities in the Diebold GEMS tabulation software and server and in the "smart cards" used with the Accuvote TS and TSx systems. These security vulnerabilities were confirmed and demonstrated in a single day under Election Day conditions after a single week of analysis and preparation by this small team of computer security experts. RABA, which is closely allied with the National Security Agency, concluded that a "pervasive rewrite" of Diebold's code would be required to significantly improve its security. Diebold has never done that pervasive rewrite.
4. August 2005, Ion Sancho, the elected Supervisor of Elections for Leon County, Florida, permitted computer security investigator Harri Hursti to attempt an attack on the security of the county's Diebold voting system. Hursti demonstrated that a person with access to the Diebold system's removable memory card could modify scripts (small programs written in Diebold's proprietary AccuBasic language) that are stored on the card, and also alter the vote counts stored on the card, in such a way that the tampering would affect the outcome of the election and not be detected by the post-election canvass procedures used by election officials to certify the results.

5. September 2005 - Government Accountability Office (GAO) report ("Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Underway but Key Activities Need to Be Completed") outlines severe problems with DRE voting. The GAO listed weak system security controls and design flaws in the product development stage. In the operations phase, the report found poor implementation of security procedures and system failures during elections. The GAO report also discusses vague and incomplete security provisions, inadequate requirements for vendor documentation, inadequate security testing and a lack of transparency in the testing process.
6. June 27, 2006 – Report by the Brennan Center for Justice at NYU School of Law, "The Machinery of Democracy: Protecting Elections in an Electronic World" A task force of internationally renowned government, academic and private sector scientists, voting machine experts and security professionals conducted the nation's first systematic analysis of security vulnerabilities among the three most commonly purchased electronic voting systems. They spent more than one year conducting its analysis and drafting this report. They concluded that all three systems have significant security and reliability vulnerabilities, the most troubling vulnerabilities can be substantially remedied if proper measures are implemented and few jurisdictions have implemented any of the countermeasures that could make the least difficult attacks against voting systems much more difficult to execute successfully.
7. August 2006 – Election Science Institute report, "DRE Analysis for May 2006 Primary Cuyahoga County, Ohio." This report assessed the May 2006 primary in Ohio, the first major election to use the new system. Their report reminded readers that "human administration of any system plays a role in the reliability of its results" however, they continued with a key finding of their report: "after three months of exhaustive research, empirical evidence supports the key definitive finding: the machine's four sources of vote totals – VVPAI individual ballots, VVPAT summary, election archive and memory cards – did not agree with one another."