

**STATE OF WISCONSIN
ELECTIONS BOARD**

The Complaint of Voter Action Wisconsin by Mike B. Wittenwyler,

Complainant,

against

State Elections Board,

Respondent.

VERIFIED COMPLAINT
§§ 5.37, 5.40, 5.91 AND THE WISCONSIN CONSTITUTION, ART. III, SEC. 3

On behalf of Voter Action Wisconsin, I, Mike B. Wittenwyler, primarily on information and belief allege that this complaint is under Wisconsin Constitution, Article III, Section 3, Chapter 5 of the Wisconsin Statutes, and more particularly, but not necessarily limited to, sections 5.37, 5.40 and 5.91 of the Wisconsin Statutes and that:

1. I am a citizen, a resident, and an elector of the State of Wisconsin, living at 2113 Chamberlain Avenue, Madison, Wisconsin 53726.
2. I am an attorney with the law firm of Godfrey & Kahn, S.C., and legal counsel for Voter Action Wisconsin. Voter Action Wisconsin is part of Voter Action, a national non-for profit organization dedicated to protecting the democratic process and ensuring that every voter has his or her vote recorded as intended and counted accurately.
3. I am filing this verified complaint on behalf of Voter Action Wisconsin, asking the State Elections Board (the "Board") to protect Wisconsin voters' fundamental right to vote and the integrity of Wisconsin elections by revoking the certification of certain direct recording electronic voting systems ("DREs") manufactured by Diebold Election Systems, Inc. ("Diebold"), Sequoia Voting Systems, Inc. ("Sequoia"), ES&S, and Voting Technologies International. The DRE systems subject to this complaint are limited to:
 - A. Diebold - TSX DRE Touch Screen and AccuView Printer Module, version 4.6.3
 - B. Sequoia - AVC Edge with VeriVote Printer DRE system, version 5.024
 - C. ES&S - iVotronic DRE with Real Time Audit Log, version 9.1.4.0

- D. Voting Technologies International - VotWare DRE Voting System, firmware release version 5.0.4.1

4. The Help America Vote Act of 2002 ("HAVA") contains several provisions designed to change the way Americans vote. Over the past several years, the Board attempted to comply with the HAVA requirements by certifying various voting machines including the subject DREs and requiring each polling location in Wisconsin to have at least one of the Board-certified DRE systems in operation by the September 12, 2006 primary election. Only one county, Pierce County, chose to use DRE systems exclusively at all of the County's polling locations except for those located in the city of River Falls. Voting Equipment by Municipality, State of Wisc. Elections Board, p. 82-83, August 25, 2006.¹ Based on information supplied by the Board:

- A. The following counties have begun to use the Diebold DRE systems: Calumet, Chippewa, Clark, Dodge, Door, Fond du Lac, Green, Juneau, Kenosha, Oneida, Ozaukee, Sauk, Vilas, Walworth, Washington and Winnebago.
- B. The following counties have begun to use the Sequoia DRE systems: Adams, Barron, Buffalo, Burnett, Calumet, Chippewa, Crawford, Dunn, Eau Claire, Fond du Lac, Forest, Grant, Green, Green Lake, Iowa, Iron, Jackson, Juneau, Lafayette, Langlade, Marinette, Marquette, Milwaukee, Monroe, Oconto, Outagamie, Ozaukee, Pepin, Pierce, Polk, Price, Racine, Richland, Rusk, Sawyer, Shawano, Sheboygan, St. Croix, Trempealeau, Vernon, Walworth, Waukesha, Waupaca and Waushara.
- C. Clark and Taylor Counties have begun to use the iVotronic DRE systems.
- D. Pierce County has begun to use the Voting Technologies International VotWare DRE Voting System, firmware release version 5.0.4.1.

5. It is likely that thousands of Wisconsin voters will cast their ballots in the 2006 general election using the Board-certified DRE systems.² The rates of usage may be especially high in less-populous communities where voters would not necessarily have to wait longer to the one new machine at their polling place. In the September 2006 primary, DRE machines were used by 50 to 75 percent of the voters in Washburn County, and by more than 90 percent of the voters in Spooner. Frank Zufall, *Voting Machines Widely Used*, Spooner Advocate, September 20, 2006.³ **Exhibit 3.** Even in more populous Winnebago County, where non-DRE voting stations were likely to be more plentiful, around 1200 voters used Winnebago County's Diebold

¹ Available at <http://elections.state.wi.us/docview.asp?docid=2728&locid=47>

² No statistics on the actual number of Wisconsin voters who used DREs in the September 2006 primary have been made public by any government agency.

³ Available at http://www.spooneronline.com/placed/index.php?story_id=225413&view=text.

DRE machines for the September 2006 primary. *Editorial: Touch Screen's Trial Tenuous at Best in Winnebago County*, Oshkosh Northwestern, September 14, 2006.⁴ **Exhibit 4.**

6. The Board has the obligation to "revoke its approval of any ballot, device, equipment or materials at any time for cause." Wis. Stat. § 5.91.

7. On behalf of Voter Action Wisconsin, I request that the Board revoke the certification of these DRE systems based on the following:

- A. The subject DRE systems are inherently unreliable.
- B. The subject DRE systems are open to possible tampering.
- C. The subject DRE systems are particularly susceptible to human error, which is exacerbated by insufficient training of and guidance for poll workers.
- D. The subject DRE systems violate the Wisconsin Constitution and Wisconsin's statutory requirements that electronic voting systems be secure, reliable, accurate, verifiable, private, and accessible to all Wisconsin voters. Wis. Const. Art. III, Sec. 3, Wis. Stat. §§ 5.37, 5.40, & 5.91.

THE SUBJECT DRE SYSTEMS ARE INHERENTLY UNRELIABLE.

8. The subject DRE systems have been certified by the Board for use in the 2006 election and thereafter.

9. The subject DRE systems are not reliable. In fact, numerous studies have concluded that there are significant risks with electronic voting machines due to concerns with the reliability of the systems. Rubin, Aviel D., et. al., *Analysis of an Electronic Voting System*, Johns Hopkins University Information Security Institute Technical Report TR 200319, July 23, 2003. **Exhibit 5.**

10. States across the country have commissioned reports on the security risks and inherent deficiencies of the subject DRE systems.

- A. In April 2006, Cuyahoga County Commissioners hired the Election Science Institute ("ESI") to conduct a study on its use of Diebold touch-screen voting machines during the May 2006 primary election. *See* Election Science Institute, *DRE Analysis for May 2006 Primary*, Cuyahoga County, Ohio (Aug. 2006), **Exhibit 6.** The study found that relying on the County's current election system "should be viewed as a calculated risk in which the outcome may be an acceptable election, but there is a heightened risk of unacceptable cost." *Id.* at ii-iii. Specifically, ESI found that Diebold's four sources of vote totals – voter verified paper

⁴ Available at <http://www.thenorthwestern.com/apps/pbcs.dll/article?AID=/20060914/OSH06/609140339/1190>.

audit trail (VVPAT) individual ballots, VVPAT summary, election archive, and memory cards – consistently did not agree with one another. *Id.* at 2.

- B. On September 13, 2006, Princeton University released a comprehensive analysis of the Diebold AccuVote-TS voting machine. See Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**. The study and subsequent live demonstration (**Exhibit 8 – Video File on CD**) highlighted Diebold's inherent security vulnerabilities. The machines proved to be highly susceptible to large-scale virus attacks, which are virtually undetectable by election officials: "AccuVote-TS machines are susceptible to voting-machine viruses – computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity." *Id.* at 2. The study concluded that only wholesale changes in the software and security procedures would prevent corruption. See also, Refuting Diebold's Response, **Exhibit 9**.

11. DRE systems proved to be unreliable in Waukesha County in the September 2006 primary. The Milwaukee Journal Sentinel reported that the Sequoia DRE systems failed due to "[c]omputer glitches, inoperable equipment and other problems." See Scott Williams, *Waukesha County Voting Bedeviled*, Milwaukee Journal Sentinel, September 13, 2006.⁵ **Exhibit 10**. County Clerk Kathy Nickolaus "resorted to correcting the city's results manually – a process that continued until 1 a.m." *Id.* Similar delays occurred in Winnebago County, where DRE vote totals also had to be entered manually. *Editorial: Touch Screen's Trial Tenuous at Best in Winnebago County*, Oshkosh Northwestern, September 14, 2006. **Exhibit 4**.

12. The subject DRE systems have also proven unreliable and inefficient in other states, causing voter disenfranchisement.

- A. DREs failed in a variety of ways throughout the State of Florida this year. A "computer glitch" with Sequoia DRE machines in Palm Beach County prevented local election officials from releasing accurate information on how many precincts had actually reported, which in turn prevented voters and certain local candidates from knowing who won until two days after the September 5, 2006 primary. Elsewhere, Sequoia machines in Hillsborough County indicated that 100 percent of precincts had reported after only the County's absentee ballots had been tallied. See Kimberly Miller, *Voters Assured of Count Remedy*, Palm Beach Post, September 8, 2006.⁶ **Exhibit 11**.

⁵ Available at: <http://www.jsonline.com/story/index.aspx?id=497728&format=print>.

⁶ Available at http://www.palmbeachpost.com/pbcwest/content/local_news/epaper/2006/09/08/s1a_PRECINCT_0908.html.

In Pinellas County, one candidate watched as his vote, intended for himself, was automatically switched by a Sequoia touch-screen machine to a vote for his opponent. See Anne Lindberg, *Incumbents Return in a Big Way*, St. Petersburg Times, March 8, 2006. **Exhibit 12.**⁷

Elsewhere, a Sequoia server designed to tabulate vote totals crashed twice on election night, despite the intervention of a Sequoia technician. See Will Van Sant, *Group Calls for Audit of March 7 Elections*, St. Petersburg Times, March 14, 2006.⁸ **Exhibit 13.**

- B. Throughout Cook County, Illinois, thousands of votes cast on Sequoia machines in over 500 precincts went uncounted, leading to a lengthy delay in results, in part because of equipment breakdowns and in part because of incompatibility between the Sequoia machines and Chicago's existing optical scan equipment. See Steve Patterson, *Vote Snafu: Some Blame New Equipment*, Chicago Sun-Times, March 23, 2006.⁹ **Exhibit 14.** See Aachary A. Goldfarb, *Machine Woes Slow Vote-Counting in Illinois*, Washington Post, March 23, 2006.¹⁰ **Exhibit 15.**
- C. One Colorado state legislative candidate was unable to get his Sequoia DRE vote cast for himself to print. See George Merritt, *New Machines Puzzle Voters, Officials*, Denver Post, August 9, 2006.¹¹ **Exhibit 16.**
- D. In a spring election in Pequannock, New Jersey, a Sequoia DRE municipality, voters casting a vote for a particular candidate for a three year school board term followed by a valid vote in another race for a one-year term saw their initial vote vanish from the screen prompting some voters to re-select their same initial candidate and unknowingly cancel their own votes. See Margaret K. Collins, *Machine Errors Could Lead to New School Vote*, NorthJersey.com, April 20, 2006.¹² **Exhibit 17.**
- E. Maryland also experienced an array of problems with its Diebold equipment. Diebold's electronic poll-book machines caused regularly froze and rebooted on election day. One voter was informed by its touch-screen that he had already voted, and was thus barred from voting, after he took only two minutes to review his material. See Christian Davenport,

⁷ Available at http://www.sptimes.com/2006/03/08/Neighborhoodtimes/Incumbents_return_in_.shtml.

⁸ Available at http://www.sptimes.com/2006/03/14/Northpinellas/Group_calls_for_audit.shtml.

⁹ Available at http://nl.newsbank.com/nl-search/we/Archives?p_action=list&p_topdoc=21; Kari Lydersen.

¹⁰ Available at http://www.washingtonpost.com/wp-dyn/content/article/2006/03/22/AR2006032202171_pf.html.

¹¹ Available at http://www.denverpost.com/news/ci_4153438

¹² Available at <http://northjersey.com/page.php?qstr=eXJpcnk3ZjcxN2Y3dnFIZUVFeXkyJmZnYmVsN2Y3dnFIZUVFeXk2OIIxMjk1>.

Miranda S. Spivack, and Cameron W. Barr, *Worse to Come in Fall Elections, Officials Fear*, Washington Post, September 15, 2006.¹³

Exhibit 18. Elsewhere, voters throughout populous Montgomery County found that they could not vote on their municipality's Diebold machines because their polling places did not have the cards voters must use in order to activate the machines, requiring a court-mandated one-hour extension for voting. Twenty-six precincts in the Maryland suburbs of Washington also had vote-recording cards in the machines after tabulation, raising doubts as to whether the final count had omitted numerous votes. See Tom Stuckey, *Ehrlich Says Scrap Electronic Voting for General Election*, The Capital (Annapolis, Md.), September 21, 2006.¹⁴ **Exhibit 19.**

Maryland's Republican Governor Robert Ehrlich has publicly urged voters not to use the new electronic machines and to use absentee paper ballots instead. See Jon Ward, *Democratic Governor Backs Ehrlich on Balloting*, The Washington Times, September 27, 2006.¹⁵ **Exhibit 20.** And, Gilles Burger, Chairman of the Maryland State Board of Elections, has expressed disappointment in the level of support that Diebold has provided to local election officials during the primary, in part because some temporary Diebold employees had not had adequate background checks. See *Maryland Briefing*, Washington Post, September 27, 2006.¹⁶ **Exhibit 21.**

THE SUBJECT DRE SYSTEMS ARE OPEN TO POSSIBLE TAMPERING.

13. A DRE and its components are vulnerable to security breaches, or "hacking." A hacker who breaches or compromises a DRE machine's security can alter the results of an election in a manner that is not detectable to election officials. See Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**. See also Felten Demonstration **Exhibit 8**.

14. The subject DRE systems in particular have well-known, well-documented security flaws that leave the machines vulnerable to election fraud through software tampering. These problems are of a nature that could afflict any DRE model, and include the following:

- A. **Inadequate Locks:** The locks on DRE systems are woefully inadequate and easily circumvented. See Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**. See also Felten Demonstration **Exhibit 8**.
- B. **Malicious Code:** Once the lock has been circumvented, malicious code can be downloaded into the DRE system software, altering how the votes are tabulated without detection by the voter and without altering the voter verified paper audit trail ("VVAPT"). See Ariel J. Feldman, J. Alex

¹³ Available at http://www.washingtonpost.com/wp-dyn/content/article/2006/09/14/AR2006091401614_pf.html

¹⁴ Available at www.hometownannapolis.com.

¹⁵ Available at <http://washingtontimes.com/functions/print.php?StoryID=20060926-111209-3198r>.

¹⁶ Available at http://www.washingtonpost.com/wp-dyn/content/article/2006/09/26/AR2006092601648_pf.html.

Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**.

- C. **Spreading the Infection:** Once a machine is infected, the malicious code can be passed from machine to machine through the memory cards, infecting countless other machines without circumventing the lock. See Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**.
- D. **Undetectable Code:** There is no way to ensure detection of a malicious code. The GAO has concluded that malicious code can be present in a system and evade testing. GAO, Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Under Way, but Key Activities Need to Be Completed (Sept. 2005), **Exhibit 22**.

15. Over the past two years, concerns over security breaches have prompted litigation challenging DRE systems in at least five other states over the last two years, including Arizona, California, Colorado, New Mexico, and Pennsylvania, due to the DRE systems' lack of security and inaccurate ballot tabulation. See Summary of State action on DRE Systems.¹⁷

16. Investigations performed in other states and by the Federal government highlight the security concerns with the DRE systems:

- A. A group commissioned by the Republican Governor of Maryland to review the security of the Diebold DREs reported, in September 2003, that there were 328 security flaws and concluded that "the system, as implemented in policy, procedure, and technology, is at high risk of compromise." See Science Application International Corporation, Risk Assessment Report: Diebold AccuVote-TS Voting System and Process (Sept. 2, 2003), **Exhibit 23**.
- B. In December 2003, the Ohio Secretary of State released its DRE Technical Security Assessment, finding that Diebold has more security risks rated as "high" than any other vendor's system. See Election Science Institute, DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio (Aug. 2006), **Exhibit 6**.
- C. A report released in January 2004, by the Maryland Department of Legislative Services identified numerous security vulnerabilities in the Diebold GEMS tabulation software and concluded that "a pervasive rewrite" of Diebold's code would be required to significantly improve its security. See RABA Technologies, Trusted Agent Report: Diebold AccuVote-TS Voting System (Jan. 20, 2004), **Exhibit 24**.

¹⁷ See generally <http://www.voteraction.org> (describing DRE decertification efforts in several states).

17. No similar comprehensive investigation or review of DRE security deficiencies has been conducted or commissioned in Wisconsin.

THE SUBJECT DRE SYSTEMS ARE PARTICULARLY SUSCEPTIBLE TO HUMAN ERROR, WHICH IS EXACERBATED BY INSUFFICIENT TRAINING OF AND GUIDANCE FOR POLL WORKERS.

18. The security procedures set forth by the Board are merely “security recommendations,” not requirements, and are listed as such on the Board’s website. *See* Security Recommendations for Electronic Voting Systems adopted by the Wisconsin State Elections Board on June 23, 2006.¹⁸ **Exhibit 25.** Though “adopted” by the Board, these procedures do not have the force or effect of enforceable rules, meaning voters must simply hope that their municipality is following them, but have no means of assuring so.

19. The State of Wisconsin neither offers nor requires one uniform and verifiable statewide training standard for those expected to administer DRE voting systems on election day. Because the training of county and municipal officials is left to the contracting municipality and its DRE vendor, there is no consistent standard for training, nor any way for the Board to guarantee adequate training statewide. Accordingly, the subject DREs, which are known to be particularly susceptible to human error, should be decertified.

THE SUBJECT DRE SYSTEMS VIOLATE THE WISCONSIN CONSTITUTION AND WISCONSIN STATUTES.

20. Both the Wisconsin Constitution and the Wisconsin Statutes mandate that votes are cast under the privacy of a secret ballot. Wis. Const. Art. III, Sec. 3; Wis. Stat. § 5.91(1). In addition, an electronic voting system must permit the elector to privately verify the votes selected by the elector before casting his or her ballot. § 5.91(15). The paper printout used in the Diebold and Sequoia DRE systems invades voter privacy because the printout preserves the exact order in which voters have voted.

21. The Wisconsin Statutes require that the voting system generate a complete and permanent paper record of the votes cast by each elector, that is verifiable by the elector before the elector leaves the voting area, and that enables a manual recount. § 5.91(18).

- A. Voters have no means to confirm that the DRE recorded their votes correctly, nor can they have any assurance that their votes will not be electronically changed or deleted after they have cast their electronic ballots.
- B. The DRE systems do not print on ballot-quality paper. These systems instead produce printouts of the votes cast on paper that is fragile, easily alterable by handling, and that blackens when it is exposed to heat or sunlight. The DRE printouts are not capable of supporting a manual audit because they will not retain their quality during the often lengthy recount and legal challenge period.

¹⁸ Available at <http://elections.state.wi.us/docview.asp?docid=9124&locid=47>

22. Section 5.37 of the Wisconsin Statutes requires that “[v]oting machines shall be constructed to lock so they cannot be manipulated, tampered with, or show the number of votes registered for any candidate or proposition while voting is in progress” Wis. Stat. § 5.37.

- A. The subject DRE systems violate this statute because the locks are easily compromised. *See generally* Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**. *See also* Felten Demonstration **Exhibit 8**.

23. The Wisconsin Statutes require any automatic tabulating equipment authorized by the Board to include “a mechanism which makes the operator aware of whether the equipment is malfunctioning in such a way that an inaccurate tabulation of the votes could be obtained” Wis. Stat. § 5.91(13).

- A. Because no mechanism exists that can make the operator aware of malfunctions that affect the tabulation of votes, *see* Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**, use of the Diebold and Sequoia DRE systems violates this statute.

24. Wisconsin law requires the DRE system to correctly record and accurately count every vote properly cast and maintain a cumulative tally of the total votes cast. Wis. Stat. § 5.91(11).

- A. Even machines that purportedly create a VVPAT have failed to create a reliable paper trail necessary to verify both vote totals and the functionality of the machines themselves. The Election Science Institute conducted three months of exhaustive research on hundreds of Diebold DRE machines used for the spring 2006 primary in Cuyahoga County, Ohio, and found empirical evidence indicating that the paper-trail mechanism on the Diebold machines yielded vote totals that differed from those found on the memory cards. Nearly 17 percent of VVPAT tapes showed a discrepancy of 1-5 votes between the tally of ballots and the electronically-generated results report, with some showing a discrepancy of over 25 votes. This study also concluded that nearly 10 percent of the VVPAT “tapes” were either destroyed, blank, illegible, missing, taped together, or otherwise compromised. *See* Election Science Institute: Improving the American Election Process: DRE Analysis for May 2006 Primary Cuyahoga County, Ohio (Aug. 2006).¹⁹ **Exhibit 6**.
- B. Furthermore, there are no mechanisms in place for the voter to verify that the VVPAT corresponds to the actual vote recorded by the DRE. Therefore, even when the voter verifies the printout, it is impossible to know whether the official vote has been recorded correctly on the DRE’s

¹⁹ Available at http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf.

memory card. *See generally* GAO, Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Under Way, but Key Activities Need to Be Completed (Sept. 2005), **Exhibit 22**.

- C. A manual audit comparing the printout to the machine tabulation each and every time a DRE system is used is the only way to ensure accuracy. Without the audit, there is no way to ensure that the system correctly recorded or accurately counted every vote properly cast. Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (Sept. 13, 2006), **Exhibit 7**.

RELIEF SOUGHT

25. Continued use of the subject DRE systems creates an unacceptable risk of lost or miscounted votes due to computer error or intentional manipulation, and also prevents a reliable audit or recount, resulting in election uncertainty and potential incorrect election outcomes.

26. Continued use of the subject DRE systems may result in irreparable harm to Wisconsin voters' fundamental right to vote and to Wisconsin's electoral process.

27. Because of these inherent deficiencies, the Board should immediately revoke certification of the subject DRE voting systems.

28. If immediate revocation of the certification is impossible, the Board should adopt and implement the following provisional security and training measures:

- A. Develop a formal, documented, complete, and integrated set of standard policies and procedures. Apply these standard policies and procedures consistently through all jurisdictions.
- B. Create a formal system security plan.
- C. Provide state-wide, uniform security awareness training for each poll worker.
- D. Conduct a full audit following the November 2006 election.

VERIFICATION

Mike B. Wittenwyler, being first duly sworn, on oath, state that I personally read the above complaint and that the above allegations are true based on my personal knowledge and, as to those allegations stated on information and belief, I believe them to be true.

Dated October 4, 2006



Mike B. Wittenwyler

Subscribed and sworn to before me
this 4th day of October, 2006.



Notary Public, Dane County, WI

My Commission Expires: perpetual

nm29099216

Voter Action Wisconsin Exhibits

- Exhibit 1:** Mike B. Wittenwyler, Aug. 30, 2006 Letter to the State Elections Board
- Exhibit 2:** Voter Action Wisconsin, Aug. 30, 2006 Letter to the State Elections Board
- Exhibit 3:** Frank Zufall, *Voting Machines Widely Used*, Spooner Advocate, Sept. 20, 2006
- Exhibit 4:** Editorial: *Touch Screen's Trial Tenuous at Best in Winnebago County*, Oshkosh Northwestern, Sept. 14, 2006
- Exhibit 5:** Aviel D. Rubin, et. al., Analysis of an Electronic Voting System, Johns Hopkins University Information Security Institute Technical Report TR 200319, Jul. 23, 2003
- Exhibit 6:** Election Science Institute, DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio, Aug. 2006.
- Exhibit 7:** Ariel J. Feldman, J. Alex Halderman and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine, Sept. 13, 2006.
- Exhibit 8:** Felten Demonstration
- Exhibit 9:** Refuting Diebold's Response
- Exhibit 10:** Scott Williams, *Waukesha County Voting Bedeviled*, Milwaukee Journal Sentinel, Sept. 13, 2006
- Exhibit 11:** Kimberly Miller, *Voters Assured of Count Remedy*, Palm Beach Post, Sept. 8, 2006
- Exhibit 12:** Anne Lindberg, *Incumbents Return in a Big Way*, St. Petersburg Times, Mar. 8, 2006
- Exhibit 13:** Will Van Sant, *Group Calls for Audit of March 7 Elections*, St. Petersburg Times, Mar. 14, 2006
- Exhibit 14:** Steve Patterson, *Vote Snafu. Some Blame New Equipment*, Chicago Sun-Times, March 23, 2006
- Exhibit 15:** Kari Lydersen and Aachary A. Goldfarb, *Machine Woes Slow Vote-Counting in Illinois*, Washington Post, Mar. 23, 2006
- Exhibit 16:** George Merritt, *New Machines Puzzle Voters, Officials*, Denver Post, Aug. 9, 2006
- Exhibit 17:** Margaret K. Collins, *Machine Errors Could Lead to New School Vote*, NorthJersey.com, April 20, 2006
- Exhibit 18:** Christian Davenport, Miranda S. Spivack, and Cameron W. Barr, *Worse to Come in Fall Elections, Officials Fear*, Washington Post, Sept. 15, 2006,
- Exhibit 19:** Tom Stuckey, *Ehrlich Says Scrap Electronic Voting for General Election*, The Capital (Annapolis, Md.), Sept. 21, 2006
- Exhibit 20:** Jon Ward, *Democratic Governor Backs Ehrlich on Balloting*, The Washington Times, Sept. 27, 2006
- Exhibit 21:** *Maryland Briefing*, Washington Post, Sept. 27, 2006
- Exhibit 22:** GAO, Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Under Way, but Key Activities Need to Be Completed, Sept. 2005
- Exhibit 23:** Science Application International Corporation, Risk Assessment Report: Diebold AccuVote-TS Voting System and Process, Sept. 2, 2003.
- Exhibit 24:** RABA Technologies, Trusted Agent Report: Diebold AccuVote-IS Voting System
- Exhibit 25:** Security Recommendations for Electronic Voting Systems adopted by the Wisconsin State Elections Board on June 23, 2006