Confusion of Myth and Fact in Maryland

Douglas W, Jones
THE UNIVERSITY OF IOWA Department of Computer Science
July 19, 2004
http://www.cs.uiowa.edu/~jones/voting/myth-fact-md.html

In late June or early July of 2004, the Maryland State Board of Elections issued a brochure, *Maryland's Better Way to Vote -- Electronic Voting: Myth vs. Fact* [1] listing 6 "myths" about electronic voting and offering "facts" in response to each "myth." This brochure was intended to counter widespread public criticism of the voting system in use in Maryland. Clearly, skepticism about the voting system does threaten public trust in that system, and public trust in the voting system is essential if the government is to be seen as legitimate in the eyes of the electorate, so some kind of defense is appropriate.

Sadly, Maryland's *Myth versus Fact* defense contains a sufficient number of misleading assertions, straw-man arguments and outright errors that it may well do more to fuel public distrust than it does to assure the trustworthiness of the system it defends. In sum, many of the statements in this brochure would be more nearly accurate if the labels *myth* and *fact* were exchanged. A more appropriate defense might have involved squarely admitting the defects in the current system and clearly documenting, for each, the actions taken by the Board of Elections to deal with the problem.

The text of the Maryland brochure is reproduced in the following. Added comments detail errors in the presentation of "myth" and "fact", presenting evidence and suggesting alternative defensive measures:

Maryland's Better Way to Vote

Electronic Voting:
Myth vs. Fact

Maryland State Board of Elections
151 West Street, Suite 200
P.O. Box 6486
Annapolis, MD 21401
www.elections.state.md.us

Myth 1

"Electronic voting systems are inherently insecure and vulnerable to fraud."

FACTS

- Maryland's new Direct Recording Electronic (DRE) voting system has been been studied and analyzed more than any other voting system in the country.

This is true. Following the release of the Hopkins Report [2], Maryland commissioned reports by SAIC[3] and RABA Technologies [4]. In addition Ohio commissioned reports by InfoSENTRY [5] and

Compuware [6]. These studies complement each other, and all of the have found serious security flaws in Maryland's voting system. Sadly, each of these studies appears to have found at least one flaw missed by the others, and this, in turn, suggests that additional flaws may remain to be identified.

Unfortunately, only 69 pages of the 200 page report by SAIC have been released to the public. The remaining pages were wholly redacted and many of the released pages were partly redacted by the State of Maryland. It seems fair to ask, why has Maryland not released the whole report? The contents of this report are of national importance, since this voting system is widely used outside Maryland. If the problems described in the redactions have been resolved, the state should release the whole report. If the problems have not been resolved, it is even more important for us to know this.

- Not one of the security analyses conducted on Maryland's voting system showed evidence of fraud or manipulation or the ability to manipulate the voting system in a polling place, considering the procedural and human safeguards that surround an election.

The analyses were not looking for evidence of manipulation, they were looking for vulnerabilities, so the first claim above is a red herring.

The analyses did find numerous vulnerabilities, many of which involved the possibility of insider fraud or errors in carrying out these procedural safeguards. It is worth noting that the history of election fraud in the United States includes many instances of collusion between crooked politicians and election administrators! Furthermore, the SAIC study found serious flaws in Maryland's procedures[3].

Also note the use of the clause "in a polling place," because many of the vulnerabilities found were not at the polling place, but in the pathway from the polling place to the final canvass.

- The changes made as a result of the analyses improve the security of the voting system and further diminish the likelihood of fraud.

This is true, and the states of Maryland and Ohio are both to be congratulated for contracting to have several of these analyses done.

- Additionally, as noted in a recent U.S. Congressional Research Report, "there are no proven cases of tampering with the Direct Recording Electronic (DRE) or other computer-assisted voting systems in public elections."

This is true, the report cited was by Eric. A. Fisher [7].

Note, however, that "no proven cases" yet does not imply that there will never be such cases. A smart crook is unlikely to attack a controversial new technology; instead, such a crook is far more likely to attack a widely accepted but vulnerable technology. Statewide acceptance of DRE voting systems makes them more tempting targets, but only after they have been in use for a few years should we expect crooks to begin to exploit their weaknesses.

Myth 1 has not been rebutted by the facts presented, and it is almost certainly true, not merely a myth, since it is fair to state that all voting systems are inherently vulnerable to fraud, regardless of their technological foundation. What we seek, then, are voting systems that are less vulnerable than their competitors. Data presented in the Compuware Report suggests that the Diebold system, used in the State of Maryland, was the most vulnerable of the four DRE systems examined [6]. Many people have argued that hybrid technologies such as machine-counted paper ballots with precinct-count scanners offer significantly more security than DRE systems.

Myth 2

"The voting systems do not accurately record and tabulate the votes cast."

FACTS

- All of the analyses of Maryland's voting system confirmed that the system counts and tabulates votes with 100% accuracy.

Strictly speaking, no analysis of a computerized system can confirm its accuracy, so when such a statement is made, it must be taken as hyperbole. In general, the most that can be confirmed by analysis of a computer system is that, so far, it has not failed. In many cases, given sufficient safeguards, this is sufficient to allow us to use the system.

Indeed, barring the as-yet-to-be-detected fraud, and barring a variety of procedural and programming errors that have been made in various jurisdictions, DRE systems have proven to be quite good at counting the votes that they have successfully captured from voters.

On the other hand, DRE systems have an established record of confusing a significant but small fraction of the electorate, on the order of 1%, into casting votes that do not reflect their intent. This appears to be the result of badly designed screen layouts and can certainly be corrected. Research in this area is ongoing (notably by Ben Bederson at the University of Maryland [8]).

In Maryland, TrueVoteMD.org [9] has found five cases, in different races in different parts of the state, where witnesses assert that DRE machines failed to present the entire ballot. The argument that the machine counts every vote cast does not address the issue posed when a voting machine fails to allow a voter to cast a vote in some particular race.

There have been examples of electronic mis-tabulation of votes. Some attributed to running machines with low batteries, some to accumulating too many votes on a machine, and some to random events such as cosmic rays flipping single bits of memory. See *Electronic Miscounts and Malfunctions In Recent Elections* for more details [10].

- An independent testing authority tests the source code, a human-readable program written by a programmer, to ensure that the software accurately tabulates votes with 100% accuracy.

The report of the independent testing authority, or ITA is confidential, shared only with the vendor and select state officials, and the ITA is paid by the vendor and usually has a close working relationship with the vendor.

Programs, while nominally human-readable, are notoriously hard to read. The fact that one or two programmers at the ITA read the code offers very little assurance that the code is correct, although it is certainly better than having no outsiders read the code. The fact that the examiners at the ITAs have found many errors and forced the vendors to correct them does not, however, offer any guarantees that no errors remain to be found!

There have been numerous significant errors in voting systems that have escaped detection by ITAs, including major security flaws that first came to widespread public attention because of the Hopkins Report [2], and have been confirmed by the other independent reports commissioned by the states of Maryland and Ohio.

- Election officials and an independent verification firm thoroughly test each unit.

Genuinely thorough testing of any computerized system is impossible. The reason is simple: There are an infinite number of possible sequences of events the computer could respond to, and we can only afford to test a finite number of these. As a result, while testing can detect errors, testing can never certify that a computer system is error free.

A few machines of each new make and model of voting machine are tested extensively by an independent testing authority (ITA) prior to presentation to the state. This is the most thorough testing voting machines ever get, and yet, we know that flaws go undetected through these tests. The state tests a few machines during state qualification, but state testing is rarely as thorough as the ITA tests, and some states contract this testing to the ITA itself.

Every one of the thousands of voting machines delivered undergoes a very perfunctory acceptance test -- when you are receiving machines by the thousand, you cannot spend hours testing each of them! Finally, before every election, a brief pre-election test is applied to each machine. Pre-election testing for the Diebold Accuvote system used in Maryland is described in Subsection 33.10.02.15 of the *Code of Maryland Regulations* [11]. This allows the use of an automated pre-election test where the machine and the canvassing system are put through self-tests that involve processing scripted test data. Such tests give some assurance that the machine is functional as intended by the programmers, but they give no assurance that the software is honest. Given the number of machines that must be tested, what we want from this pre-election test is an assurance that the machine is set up for the correct election, that the batteries and plug-in power supply are good, that the touch screen works, and that the correct software and ballot information are loaded.

Maryland also requires a public demonstration pre-election test. Subsection 33.10.02.16 of the *Code of Maryland Regulations* says little about the substance of this test [11], but focues instead on who may observe and who must be notified in advance of this test. This test should clearly include a demonstration of the minimal testing mandated by the previous section of the regulations, but a responsible jurisdiction ought to use this opportunity to select a few voting machines at random for much more intensive pre-election tests, voting hundreds of test ballots and doing so using real touches to the screen by human fingers instead of automated test scripts. Such a test can be comparable in intensity to those used by many states for qualification, but unfortunately, the cost of such testing is high enough that it is unreasonable to expect that every voting machine used will see such tests.

Neither Maryland law nor regulations appear mention any use of parallel testing, that is, testing of randomly selected voting machines on election day during the election itself. Many opponents of voter-verified paper ballots say that such ballots are unnecessary because parallel testing can be used to achieve the same goal. For example, the League of Women Voters' *Questions and Answers on Direct Recording Electronic (DRE) Voting Systems* strongly advocates this [12], as does the Leadership Conference on Civil Rights [13]. It is noteworthy that the state of California has used parallel testing in the spring 2004 presidential primary [14].

The weakness of pre-election testing of all forms is that dishonest software could be written to detect that testing is under way so that it behaves honestly when under test and only cheats during real elections. For example, such software could examine voting patterns, the date, how long it has been turned on, or any of many other variables to distinguish between real elections and testing. Parallel testing addresses this possibility by testing randomly selected machines during the election, with test ballots cast in a manner that is as nearly indistinguishable from real ballots as is possible. Ideally, the machine to be tested is selected at the last moment, so that there is no opportunity to fix the software to behave specially.

Parallel testing is not perfect. It cannot detect fraudulent software that is enabled by a specific action by a voter or polling place official who is part of the conspiracy, and it has a low likelihood of detecting fraudulent software if only a few machines, at random, behave fraudulently, but it does defend against a wide range of potential threats. It is therefore reasonable to ask why so few states are using parallel testing for their DRE voting systems!

It is important that technically knowledgable observers be invited to observe all tests and that they be invited to ask questions about the tests. Testing in private, behind closed doors, as it is currently done at the ITAs, offers very little on which to base public confidence. Subsection 33.10.02.16 of the *Code of Maryland Regulations* does require that the nature of the pre-election demonstration be described to the observers, but it appears to give no right to observe the routine pre-election tests [11].

Myth 2 is well supported by the facts. DRE voting systems have misrecorded votes, and DRE voting systems have mistabulated votes. Furthermore, the "facts" presented by Maryland to contradict Myth 2 misrepresent what is possible in the domain of inspection and testing of computerized systems.

Myth 3

"A single person could cast multiple votes."

<u>FACTS</u>

- A voter must have an access card specifically activated for a voting unit in the polling place. Only election judges can activate voter access cards. After a voter casts a ballot, the access card cannot be used again until an election judge reactivates the card.

This correctly describes the intent of the Diebold AccuVote TS architecture. Ideally, only election judges should be able to activate voter access cards, but the red-team exercise conducted by RABA Technologies, for the state of Maryland, included the design (but not construction) of a pocket-sized device that would allow a voter to forge voter access cards [4]. They built one using a laptop computer and demonstrated that this worked.

- a combination of physical security (and visual oversight of the voting process at the precinct), software, and system features would make casting multiple votes extremely difficult and highly unlikely.

This is true. So long as the required polling place procedures are actually followed, the risks posed by this weakness in the voting system may be acceptable. Election observers should familiarize themselves with Title 10, Subtitle 3 of *Maryland Election Law* [15] and with the appropriate section of Subtitle 33.10 of the *Code of Maryland Regulations* (depending on the voting system being used) in order to assure that the required procedures are indeed being followed [11]. Unfortunately, the Maryland Regulations leave most of the details to the Judge's Manual provided to each county by the state election administrator under Regulation 33.10.03.01. Unfortunately, these manuals do not appear to be readily available.

- Throughout the day, election judges reconcile the number of voters who have checked in at the polling place against the number of votes recorded on each voting unit. Any discrepancy would be identified immediately.

This will be true if the required polling place procedures are actually followed. It is noteworthy that this reconciliation requirement is not immediately evident in either *Maryland Election Law* [15] or the *Code of Maryland Regulations* [11]. It must therefore be in the Judge's Manual provided to each county.

- It is a felony to cast multiple votes and is punishable by fines and imprisonment.

This is true, but unfortunately, there is a long history of violations of these laws. For example, Linda Lamone said that Maryland and the District of Columbia recently compared their voter databases and found 12 voters that had voted in both jurisdictions. When this was reported to the FBI, there were, apparently, no prosecutions!

Myth 3 focuses on what has been called retail vote fraud, in which individual dishonest voters attempt to cheat. Such retail fraud is a serious problem in some regions of the country, although the small number of cases found in the recent Maryland-DC comparison suggests that the magnitude of this problem may be overestimated by many. The big threat posed by DRE voting systems has always been wholesale fraud, in which dishonest election officials or other insiders with access to the machinery deliver votes, not one by one, but in bulk quantity, as in the bad old days when Chicago's dead were reputed to be regular voters.

Myth 4

"Paper receipts solve the concerns regarding electronic voting system fraud."

<u>FACTS</u>

- Maryland only uses a voting system that meets all voting system standards established by the federal government.

This oversimplifies the story. The law cited is *Maryland Election Law*, 9-102. Certification of Voting Systems, Section (2) [15]. As is the case in most states, however, not all parts of Maryland's current voting system are certified to the FEC/NASED *2002 Voting System Standards* [16]; some parts are only certified to the older 1990 Standards [17]. It takes time for vendors to bring their products into conformance with new standards, and there is a delay after that while the new equipment is tested. It is therefore somewhat unrealistic to expect, two years after the new standard was adopted, that all voting systems will have been updated to conform to the new standard.

- Until standards for printers are established and voting systems are tested and certified against these standards, it would be irresponsible to attach a printer to a voting system and would violate Maryland's election law.

This bends the truth. As of July 7, 2002, the Avante Vote Trakker voting machine [18] was certified to the *1990 Voting System Standards* [17]; this machine offers a voter-verified paper trail. Others machines offering voter-verified paper trails have since been certified to these old standards, and two, one from Avante and one from Sequoia, have been certified to the newer 2002 standards [16]. A relatively up-to-date list of certified voting systems is available from the National Association of State Election Directors [19]; this lists, for each system, the standard to which it was certified.

It is true, however, that there are no standards in place that address the specific issues raised by the addition of a paper trail to a touch-screen voting system. The state of California has proposed a draft standard to address this lack [20]. The state of Maryland, however, has taken little or no interest in encouraging the development of such a standard.

It is also noteworthy that *Maryland Election Law*, 9-102. Certification of Voting Systems, Subsection (3d) item 9 deems it a positive virtue for a voting system to offer an alternative means of verifying the tabulation

[15]. The Diebold system currently in use in Maryland offers very weak assurances in this regard, since the electronic records of the votes are all created by the same software, and no recount of some version of these records can correct for errors introduced by this software.

- Paper receipts provide a false sense of security because they do not guarantee that the results recorded in the machines are the same results printed on the receipt.

Advocates of paper generally do not refer to the pieces printed by the voting machine as receipts. Rather, they refer to them as voter-verified paper ballots. A receipt is something you take from the polling place as proof of your vote, while a ballot is something you leave behind, in a secure ballot box.

It is true that merely printing a paper ballot does not answer all of the security questions. This is why many advocates of voter-verified paper ballots prefer that the paper itself be counted -- for example, by precinct-based ballot tabulating machines, instead of allowing the possibility that the voting machine would record the vote one way while it prints something else on the paper.

Alternatively, many advocates of voter-verified paper ballots recommend routine hand reconciliation of the paper record against the electronic record. The *California Election Code* sets a model for this [21]: After each election, Section 15360 mandates that precincts representing at least one percent of the vote be selected at random in each jurisdiction for such an audit in order to check the accuracy of the vote tabulating equipment.

Myth 4, therefore, is best characterized as a straw-man argument, an easily refuted statement that misrepresents the position taken by the opponents of DRE voting systems. Sadly, some of the "facts" presented are not entirely true.

Myth 5

"Hackers could alter a voting system by introducing a `Trojan Horse' or breaking into the election management system."

<u>FACTS</u>

- A person must have physical access to the source code in order to plant a "Trojan horse" (i.e., hidden program or utility that can cause harm). Election offices do not receive source code and only receive "application" software (i.e., computer-readable program).

This is true but a bit garbled, and this only applies to Trojan horses, not other serious threats. A better definition of a Trojan horse is that it is something offered (or sold) as having one function, for example, as a beautiful sculpture, but that actually serves another function, for example, to carry invading soldiers into town. Trojan horse attacks in software must therefore come from the software developers, not from hackers.

Other forms of attack such as virus-based and worm-based attacks are more interesting threats for a hacker to exploit, and we are interested in defense not only against hackers, but against insiders, for example, programmers working for the voting system vendor, the independent testing authority or the state election office.

The form of delivery of the software is not really relevant to questions about Trojan horse attacks or attacks through worms or viruses. Delivery of easily edited source code to the local election office would allow local election officials to easily change the software, opening the door to locally administered wholesale fraud, but this is not at all the same as an attack by an outside hacker. It is worthwhile to note that many successful hacker attacks have been made on systems where there was no access to source code.

The computer industry has a long record of releasing products that contain unauthorized features that were inserted by programmers at the vendor without the authorization or approval of the vendor. Some of these are quite large, for example, the flight simulator game in Microsoft's *Excel 97* [22]. We must defend ourselves against such features in election software! Because software testing and inspection are themselves weak defenses, we must ask about the character and integrity of the software developers. Unfortunately, Diebold and its corporate predecessors involved in developing the AccuVote TS have a record of hiring convicted felons as software developers [23], including one, Jeffrey Dean, who was found guilty of computer-based embezzlement.

Ilicit software has also been inserted into applications by testing authorities! Consider the case of Ronald Harris [24], an employee of the Nevada Gaming Control Board, who was convicted in 1997 for rigging the computerized slot machines when he was supposed to be testing them for honesty. It is noteworthy that slot machines are generally subject to more intense oversight than voting machines. We must defend ourselves against such threats to our voting system.

- A person would need physical access to the main computer to break into the election management system. This computer is password protected and is located in a secure location.

This is false! There are many ways to attack a computer through network connections, including through attacks by dial-up modem. The election management systems used in Maryland run on computers that have dial-up modems, and they run versions of Microsoft Windows, an operating system that is notoriously insecure.

- The voting units and the main computers are never connected to the Internet.

We know, from the SAIC report on Maryland's voting system, that the election management systems were directly connected to the Internet[3]. We can hope that such direct connections have been eliminated, but eliminating such connections does not guarantee much.

Maryland's voting system uses modem connections, through the public dial-up telephone network, to connect from polling places to the election management system at the close of the polls. This means that a hacker could attempt to enter the election management system through the dial-up modem connection.

Also note that ATMs are not connected to the Internet, yet in late 2003 it was found that several Diebold ATMs had become infected with the "Nachi" worm [25]! All that it takes is connection, briefly, to another computer that was infected when it, in turn, was briefly connected to the Internet.

Myth 5, again, is best characterized as a straw-man argument, since Trojan horse attacks and attacks by hackers each represent only a small fraction of the attacks from which we desire defense. Here, though, the problem is compounded by false and misleading assertions among the "facts" presented as refutations.

Myth 6

"A person could intercept the electronically transmitted unofficial and incomplete election results."

FACTS

- The data on the memory cards inside the voting machine become the official results. These cards are transported to the local election office by sworn election judges.

This is correct. The best practice is to have the ballot transport done in the joint custody of two judges, representing opposing parties, so that nobody every has sole access to the ballots, whether in paper or electronic form. It is unclear whether such a procedure is required in Maryland's Judge's Manuals.

With conventional ballot boxes, putting the ballot box in the joint custody of two people was quite easy. When the ballot box is reduced to an electronic format, a PCMCIA card, the entire concept of joint custody and observability begins to collapse. The PCMCIA cards used for this purpose in Maryland are the size of a playing card, and therefore vulnerable to sleight of hand manipulation. As a result, unlike conventional ballot boxes, it is almost impossible for an observer to see that the memory card inserted in the envelope for transport to the canvassing center is indeed the one that was pulled from the machine.

- Results are only official once all memory cards have been physically uploaded directly into the elections server.

This is correct, but it is noteworthy that the memory cards used by Maryland's system are fully compatible with any laptop computer or PDA that has a PCMCIA slot; many do. If someone had the inside knowledge needed to modify the contents of the memory card, the necessary technology is commonplace. Furthermore, just as there is a risk of sleight of hand manipulation at the precinct, there is also such a risk at the canvassing center when cards are handled for uploading into the elections server.

- Final reconciliation of official and unofficial results would immediately uncover discrepancies.

This is correct, but the wording of this answer leaves open the question of whether or not this reconciliation is mandatory, and it also leaves out the question of how discrepancies, if found, are resolved.

The best practice with precinct-count electronic systems, whether they are optical mark-sense scanners or DRE voting systems, is to print the vote totals on paper immediately after the polls close, before any modem connections are made to the outside world. One copy of the printed totals should be posted, in public. A second copy should be included with the electronic record (the PCMCIA card, as used in Maryland), and only after these copies are printed should the voting system be connected to the telephone for modem transmission of the unofficial totals. This procedure is well documented in Georgia's administrative code, section 183-1-12-.02, section (5)(a)3 [26]. While there are hints of such a procedure in Subtitle 33.10 of *Code of Maryland Regulations* [11], it does not appear to be implied by Maryland Election Law, 11-202. Election judges - Procedures for vote counting [15]; if such a procedure is actually required, it must therefore be in the Judge's Manual provided to each county.

The best practice ensures that observers can make their own record of the precinct totals in order to independently confirm that they are correctly incorporated into the canvass, and it ensures that a paper record as well as an electronic record are hand-delivered to the counting center, so that any corruption of the official electronic record by counting center computers can be defended against by reconciliation against the paper record. In Miami-Dade County, this reconciliation is done routinely after every election. No such reconciliation appears to be mandated in Subtitle 33.08 of *Code of Maryland Regulations* [11], but there are hints in 33.08.01.10 that local boards have the authority (but probably not the obligation) to include such a reconciliation as part of a post-election audit.

Finally, rules are needed to handle discrepancies. It is not sufficient merely to state that, in the event of discrepancy, it shall be investigated and resolved (Regulation 33.08.01.10 does this, for example) but this is better than a statement, by fiat, that one or the other record shall govern. If a discrepancy is found between the records transmitted by modem and the records delivered by hand, both should be considered suspect, the integrity of both should be investigated, and the records that conform most closely to other evidence should be accepted. Comparison of the number of voters recorded with the pollbook and comparison with independently transmitted copies of the election totals can all be used to resolve discrepancies.

Maryland State Board of Elections
151 West Street, Suite 200
P.O. Box 6486
Annapolis, MD 21401
Phone: 401-269-2840
www.elections.state.md.us

Acknowledgements

I would like to acknowledge helpful suggestions from Avi Rubin at Johns Hopkins University, and Linda Schade, Paul Suh and Robert Ferraro of TrueVoteMD.

This material was first placed on the web on July 16, 2004 and the first public release was on July 18, 2004.

References

1] *Maryland's Better Way to Vote -- Electronic Voting: Myth vs. Fact*, http://www.cs.uiowa.edu/~jones/voting/myth-fact-md.html

2] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, Analysis of an Electronic Voting System, *IEEE Symposium on Security and Privacy*, Oakland, CA, May, 2004. http://avirubin.com/vote/analysis/index.html

3] *Risk Assessment Report -- Diebold AccuVote-TS Voting System and Processes.* Science Applications International Corporation, SAIC-6099-2003-261, September 2, 2003. (see web site 2 for a link to this)

4] *Trusted Agent Report Diebold AccuVote-TS Voting System*. RABA Technologies LLC, January 20, 2004. (see web site 2 for a link to this)

5] *Computerized Voting Systems -- Security Assessment: Summary of Findings and Recommendations, Volume 1*, InfoSENTRY Services, Inc. November 21, 2003. http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf

6] Direct Recording Electronic (DRE) Technical Security Assessment Report. Compuware Corporation Document Control Number v01 11/21/2003, November 21, 2003. http://www.sos.state.oh.us/sos/hava/files/compuware.pdf

7] Eric A. Fischer, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues.* Congressional Research Service, Order Code RL32139, November 4, 2003. http://www.epic.org/privacy/voting/crsreport.pdf

8] Ben Bederson, Electronic Voting Systems web pages. http://www.cs.umd.edu/~bederson/voting/

9] Campaign for Verifiable Voting in Maryland. http://TrueVoteMD.org/

10] *Electronic Miscounts and Malfunctions In Recent Elections*, VerifiedVoting.org, updated regularly. http://www.verifiedvoting.org/resources/documents/ElectronicsInRecentElections.pdf

11] *Code of Maryland Regulations*. Maryland Division of State Documents, effective July 18, 2004. http://www.dsd.state.md.us/comar/

12] *Questions and Answers on Direct Recording Electronic (DRE) Voting Systems*. League of Women Voters of the United States, November 24, 2003.
an updated version is posted at http://www.lwv.org/HAVA_QAonDRE.pdf
the older version is available at http://www.elections.state.md.us/pdf/lwv_dre_faq.pdf

13] *Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems*. Civilrights.org, June 29, 2004. http://www.civilrights.org/issues/voting/details.cfm?id=23781

14] *Parallel Monitoring Program Summary Report for March 2, 2004*, R&G Associates, LLC, April 19, 2004. http://www.ss.ca.gov/elections/ks_dre_papers/Parallel_Monitoring_Summary_Report.pdf

15] *Maryland Election Law*, annotated, Maryland State Board of Elections. http://www.elections.state.md.us/citizens/law/Destination/Destination-1.htm

16] *Voting System Standards*, Federal Election Commission, April 30, 2002. http://www.fec.gov/pages/vssfinal/vss.html

17] *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems*, Federal Election Commission, January 1990. http://sims.berkeley.edu/~jhall/fec_vss_1990_pdf/

18] The VOTE-TRAKKER™ EVC308 Receives NASED Certification, AI Technology Inc. Avante Press Release, July 7, 2002.
http://www.aitechnology.com/votetrakker2/nased_press_release.htm

19] *NASED Qualified Voting Systems*. National Association of State Election Directors, June 29, 2004.
http://www.nased.org/NASEDITAQualifications7.04.pdf

20] *State of California DRAFT STANDARDS For Use of Accessible Voter Verified Paper Audit Trail Systems in Direct Recording Electronic (DRE) Voting Machines*. Secretary of State, State of California, March 18, 2004.
http://ss.ca.gov/elections/ks_dre_papers/avvpat_draft_standards_3_18_04.pdf

21] *California Election Code*, Legislative Counsel, State of California, 2003.
http://www.leginfo.ca.gov/calaw.html

22] *Excel Easter Egg - Fly The Flight Simulator*. Egg Heaven 2000, April 29, 2000.
http://www.eggheaven2000.com/detailed/17.html

23] *Press Conference*, Black Box Voting, December 16, 2003.
http://www.blackboxvoting.org/Dec16-pressconf.htm

24] Steve Bourie, *The World's Greatest Slot Cheat?* American Casino Guide, 1999.
http://www.americancasinoguide.com/Tips/slot-cheat.shtml

25] *Worm Hits Diebold's Windows ATMs*. Wired News, December 9, 2003.
http://www.wired.com/news/business/0,1367,61526,00.html

26] *Georgia Election Code: Voting Machines -- Vote Recorders*. Georgia State Election Board.
http://rules.sos.state.ga.us/cgi-bin/search.cgi?d=1&query=183