

**IN THE CIRCUIT COURT
FOR ANNE ARUNDEL COUNTY**

LINDA SCHADE, ANDREW HARRIS, JUDITH BURNS,
MARK ELRICH, KWAME ABAYOMI, TERRENCE
FITZGERALD, SHARON BEARD, and PAUL SUH,

Plaintiffs,

vs.

MARYLAND STATE BOARD OF ELECTIONS,
LINDA H. LAMONE (as Administrator of Maryland's State
Board of Elections),

Defendants.

CASE NO. _____

COMPLAINT

1. This case is brought on behalf of registered Maryland voters and candidates for public office to ensure the integrity of the November 2004 elections, and to preserve public trust and confidence in the system by which Maryland voters will elect the next President of the United States. Specifically, Plaintiffs bring this action against the Maryland State Board of Elections and its Administrator, Linda H. Lamone, for improperly certifying the Diebold AccuVote-TS electronic voting machines used in Maryland, and then failing to either correct or decertify the machines -- as required by state and federal law -- once it became clear that the machines could neither preserve the security and reliability of the November 2004 election nor create a voter-verified paper audit trail. This suit is filed now, well in advance of the November 2004 election, to make sure that Maryland, which lies at the epicenter of the nationwide electronic voting machine controversy, does not become the next Florida.

2. Ironically, Maryland's embrace of electronic voting machines, has its roots in the Florida election experience in 2000. Even before the U.S. Supreme Court decided *Bush v. Gore*, resolving the disputed Presidential election, Maryland Governor Parris N. Glendening established a Special Committee to review Maryland's voting systems and election procedures. The Special Committee cautiously endorsed electronic voting machines, but insisted that such machines be secure, reliable, and "capable of creating a paper record of all votes cast in order that an audit trail is available in the event of a recount." Special Committee on Voting Systems and Election Procedures in Maryland, *Report and Recommendations*, Feb. 2001, at 41 ("Special Committee Report") (Ex. 1). The Committee explained that the "paper record" was intended to address concerns with the "bold embrace" of this new technology and was necessary to provide "instinctive security" against potential problems. *Id.* Soon thereafter, the Maryland General Assembly enacted these standards into law and authorized the State Board of Elections to move forward with the purchase of electronic voting machines.

3. The State Board of Elections set up a Procurement Review Committee to help select a vendor. But after meeting with various vendors and evaluating the maturity of this new technology, the Procurement Review Committee instead **declined** to endorse any of the vendors because of security and reliability concerns with the nascent technology. The Committee recommended that Maryland **not** move forward with the purchase of electronic voting machines. Despite this recommendation, the State Board of Elections forged ahead and signed a contract with the lowest bidder -- Diebold Election Systems, Inc. -- for the purchase of over 4,000 electronic voting machines. The State Board did so even though Diebold would not be able to produce a voter-verifiable paper audit trail as required by recently enacted state law.

4. It has since become clear that the Procurement Review Committee's initial assessment was correct and should have been followed. On July 23, 2003, two days after Maryland purchased an

additional 11,000 Diebold AccuVote-TS electronic voting machines at a cost of approximately \$55.6 million, Professor Aviel Rubin and his colleagues at Johns Hopkins University produced a widely published report severely criticizing the security of the Diebold computer source code. The Hopkins Report found “*significant and wide-reaching security vulnerabilities*”¹ with the Diebold AccuVote TS voting system used in Maryland and repeated the Special Committee’s earlier recommendation, since enacted into law, that “*currently the most viable solution for secure electronic voting machines is to introduce a voter-verifiable audit trail*” such that a recount could be conducted should any security vulnerabilities be exploited. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin & Dan S. Wallach, *Analysis of an Electronic Voting System*, Feb. 27, 2004, at 4 (“Hopkins Report”) (Ex. 2). The Hopkins Report concluded by warning that “if we do not change the process of designing out voting systems, we will have no confidence that our election results will reflect the will of the electorate.” *Id.* at 21.

5. Following the Hopkins Report, the Governor and the Maryland General Assembly ordered independent assessments of the Diebold electronic voting system. Both confirmed the seriousness of the security vulnerabilities in the electronic voting systems and reiterated the need for a voter-verified paper audit trail:

- **The Science Application International Corp. (“SAIC”) Report**, ordered by Maryland Governor Ehrlich on August 7, 2003 as an independent assessment of the security concerns raised by the Hopkins Report, found **328 security weakness** with the Diebold AccuVote-TS electronic voting system, **26 of which were deemed critical**, and as a result concluded that the Maryland elections were at “**high risk of compromise.**” Science Applications Int’l Corp., *Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes*, Sept. 2, 2003, at 10 (“SAIC Report”) (Ex. 3). SAIC recommended a series of mitigation steps to help *reduce* the potential security concerns, but could not guarantee that, even if these steps were adopted, the vote in Maryland would not be compromised.

¹ All emphasis is added unless otherwise indicated.

- **The RABA Report**, ordered by the Maryland General Assembly on November 10, 2003 as an independent assessment of the security concerns identified by the Hopkins and SAIC reports, confirmed the results of the earlier studies and noted that the State Board of Elections had failed to even address many of the mitigation steps recommended by SAIC. See RABA Technologies LLC, *Trusted Agent Report: Diebold AccuVote-TS Voting System*, Jan. 20, 2004 (“RABA Report”) (Ex. 4). In addition, RABA conducted its own “Red Team Exercise,” which revealed that the Diebold AccuVote-TS electronic voting system presented “*considerable security risks*” that could cause “*moderate to severe disruption in an election.*” *Id.* at 3. Although the RABA team felt that “a pervasive code rewrite would be necessary” to secure the systems, it questioned whether Diebold had the technical expertise to accomplish this task. *Id.* at 23. As a result, the RABA report again emphasized that “*the introduction of voter-verifiable paper receipts is absolutely necessary in some limited form*” prior to the November 2004 election. *Id.* The widely respected RABA team members subsequently explained just how easy it would be to exploit a security vulnerability in the Diebold system and alter an election: “the level of effort [needed to get into the system] was pretty low. *A high school kid could do this. Right now, the bar is maybe 8th grade.*” Stephanie Desmon, *Md. Computer Testers Cast a Vote: Election Boxes Easy to Mess With*, Baltimore Sun, Jan. 30, 2004 (Ex. 5). Indeed, they concluded that “[y]ou are more secure *buying a book from Amazon* than you are uploading your results to a Diebold server.” Nelson Hernandez, *Md. Voting Machines Vulnerable, Firm Says*, Wash. Post, Jan. 30, 2004 at B1 (Ex. 6). This was because “Diebold basically had no interest in putting actual security in this system. *It’s not like they did it wrong. It’s like they didn’t bother.*” Desmon, *supra*.

6. Surprisingly, however, the State Board of Elections has ignored the clear warnings presented in these independent studies, even going so far as proclaiming that “the findings in the SAIC and RABA reports both confirm the accuracy and security of Maryland’s voting procedures and our voting systems as they exist today,” and moved forward despite the potential consequences. State of Maryland State Board of Elections, *Response to: Department of Legislative Services Trusted Agent Report on Diebold AccuVote-TS Voting System*, Jan. 29, 2004, at 2 (“SBE Response to SAIC and RABA”) (Ex. 7). Indeed, despite an earlier public acknowledgement by Ms. Lamone that “the machines could be upgraded by November” to implement RABA’s recommendations, the State Board of Elections has **failed** to either correct or decertify the machines in violation of state and federal law. Hernandez, *supra* at B1.

7. Based on the reports commissioned by Maryland, numerous **other** states have instituted voter-verifiable paper audit trails and other security recommendations proposed by RABA and SAIC authors. Yet the Maryland State Board of Elections steadfastly refuses to fully implement the

recommendations of these taxpayer-funded reports. As a result, the voters of Maryland cannot have confidence that the November 2004 election will produce a trusted or that will accurately reflect the will of the electorate. The lessons of Florida 2000 will be lost.

JURISDICTION

8. This Court has jurisdiction over Defendants pursuant to MD Code, Courts and Judicial Proceedings § 6-102.

VENUE

9. Venue is proper in this County pursuant to MD Code, Courts and Judicial Proceedings § 6-201.

THE PARTIES AND OTHER RELEVANT PERSONS

10. Plaintiffs are a cross-partisan, diverse group of registered Maryland voters and candidates who share a profound concern for the integrity of the upcoming 2004 general election in Maryland.

11. Plaintiff Linda Schade is a resident and registered voter in Takoma Park, Maryland and is the co-founder of the Campaign for Verifiable Voting in Maryland (“CVVM”). CVVM is an organization dedicated to the security and integrity of Maryland’s voting system. Members include experts on computer software, programming and computer security, election judges, election poll watchers, candidates for elected office, and thousands of registered Maryland voters. Ms. Schade was a candidate for the House of Delegates in Maryland in 2002, plans to run for elected office in the future, and intends to vote in the November 2004 general election. Ms. Schade became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law, on April 12, 2004.

12. Plaintiff Andrew Harris is a resident and registered voter in Cockeysville, Maryland. He is the minority whip of the Maryland State Senate, representing the citizens of Baltimore and

Harford Counties. Senator Harris was co-sponsor of SR-393, the Voter Verified Paper Record. He intends to vote in the November 2004 general election. Senator Harris became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law, became known to Senator Harris on April 12, 2004.

13. Plaintiff Judith Burns is a resident and registered voter in Lexington, Maryland. Until retirement, Ms. Burns designed and programmed computer software for 35 years for entities such as the United States Department of Navy and savings and loan associations. Ms. Burns intends to vote in the November 2004 General Election. Ms. Burns became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law on April 16, 2004, after reading an article about the controversy in *The Enterprise* newspaper.

14. Plaintiff Mark Elrich is a resident and registered voter in Montgomery County, Maryland. He has been a city councilman in Takoma Park for 16 years and intends to run in the 2005 city election and the 2006 county election. He introduced a Takoma Park resolution to require a voter-verified paper audit trail. Councilman Elrich intends to vote in the November 2004 general election. Councilman Elrich became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law, on April 12, 2004.

15. Plaintiff Kwame Abayomi is a resident and registered voter in Baltimore City, Maryland. He is a Baltimore City Councilman. Councilman Abayomi intends to vote in the November 2004 general election. Councilman Abayomi became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law.

16. Plaintiff Terry Fitzgerald is a resident and registered voter in Baltimore City, Maryland and is a candidate for Baltimore City Councilman in the November 2004 elections. Mr. Fitzgerald intends to vote in the November 2004 general election. Mr. Fitzgerald became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law, on April 12, 2004.

17. Plaintiff Sharon Beard is a resident and registered voter in Pasadena, Maryland. Ms. Beard intends to vote in the November 2004 General Election. Ms. Beard became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law, on April 18, 2004.

18. Plaintiff Paul Suh is a resident and registered voter in Chevy Chase, Maryland. Mr. Suh is a security specialist for the CVVM and is a curriculum developer at Apple Computers. Mr. Suh intends to vote in the November 2004 general election. Mr. Suh became aware that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state and federal law, on April 12, 2004.

19. All Plaintiffs are registered voters in Maryland, and some plaintiffs are candidates. All Plaintiffs will suffer injury as a result of the State Board of Elections' refusal to decertify the Diebold AccuVote-TS voting systems for use in the November 2004 general election unless and until the security concerns are addressed and a voter-verifiable paper audit trail is instituted.

20. Defendant Maryland State Board of Elections ("State Board" or "SBE") manages and supervises elections conducted by the 24 local election board offices in Maryland. The State Board is tasked with ensuring compliance with the requirements of Maryland and federal election laws by all persons involved in the election process, including pertinent state law relating to the review,

certification, and decertification of voting systems. The State Board's mission is to provide all eligible Maryland citizens with appropriate access to voter registration, to provide all registered voters accessible locations in which they may exercise their right to vote, to ensure uniformity of election practices, to promote fair and equitable elections, and to maintain registration records, campaign fund reports, and other election-related data accurately and in a form that is accessible to the public.

21. Defendant Linda H. Lamone is the Administrator of the State Board of Elections. The State Administrator of Elections is the chief election official in Maryland. The State Administrator is appointed by the State Board and is responsible for supervising the operations of the local boards of election ("LBES") and for performing any other duties assigned to the Administrator by law or delegated to the Administrator by the State Board.

22. Diebold Election Systems, Inc., formerly known as Global Election Systems Inc. ("GES"), is now a subsidiary of Diebold, Inc. Diebold, Inc. acquired GES in September 2001 for \$26.2 million in cash and stock in order to enter the electronic voting machine business. Diebold, based in North Canton, Ohio, is the manufacturer of the AccuVote-TS electronic voting system used in Maryland. Diebold is a multinational corporation with representation in more than 88 countries and reported revenue of \$2.1 billion in 2003.

23. The Special Committee on Voting Systems and Election Procedures in Maryland was created by executive order of Maryland Governor Parris N. Glendening on December 4, 2000 to review Maryland's voting systems and election procedures. The Special Committee had 15 members. Secretary of State John T. Willis was designated as Chair and former State Senators Julian L. Lapidus, Esq. and F. Vernon Boozer, Esq. served as Vice Chairs. Two Maryland State Senators, Michael J. Collins and Joan Carter Conway, and two Maryland State Delegates, John S. Arnick and Robert H. Kittelman, were appointed by the respective presiding officers to represent the Maryland General Assembly. The public members were Anne Arundel County Executive Janet S. Owens, retired Court

of Special Appeals Judge Raymond G. Thieme, H. Harry Basehart, Ph.D., Frances Murphy Draper, Lt. Gen. Emmett Paige, Jr. (Ret.), and Linda Bowler Pierson. The Chair of the State Board of Elections, Helen L. Koss, and the President of the Maryland Association of Election Officers, Marvin L. Cheatham, served as ex-officio members of the Special Committee.

24. The Procurement Review Committee is a five-member panel of security and technical specialists established in 2001 that was tasked with reviewing proposals by electronic voting systems vendors and ultimately with recommending a vendor to provide Maryland's new electronic voting system.

25. Beverly Harris is the author of *Black Box Voting: Ballot-Tampering in the 21st Century*. While writing *Black Box Voting*, Ms. Harris spent over 2,000 hours researching voting machines and interviewing dozens of witnesses, including many election officials and voting machine programmers. Ms. Harris is also the author of *How to Embezzle a Fortune*, which provides tips on how to identify accounting fraud and recover embezzled funds, and she has published numerous articles on voting machine ownership, errors, and security in news publications worldwide.

26. Professor Aviel Rubin is the lead author of a technical report entitled "Analysis of an Electronic Voting System," (the "Hopkins Report") which found "significant and wide-reaching security vulnerability" with the Diebold electronic voting system. Hopkins Report, *supra* at 4. Professor Rubin is a highly regarded Professor of Computer Science at Johns Hopkins University and Technical Director of the Johns Hopkins Information Security Institute. Before joining the faculty at Johns Hopkins University, Professor Rubin worked in the Secure Systems Research Department at AT&T Labs-Research, where his primary areas of expertise were cryptography, network security, Web security, and secure Internet services. Professor Rubin holds B.S., M.S.E., and Ph.D. degrees in Computer Science from the University of Michigan.

27. Professor Douglas W. Jones is the author of a series of research papers on the security of electronic voting systems. Professor Jones is an Associate Professor of Computer Science at the University of Iowa. He has served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems since 1994 and chaired the Board from the Fall of 1999 to early 2003. Professor Jones has also been asked to testify before the U.S. Civil Rights Commission and the U.S. House of Representatives Science Committee on electronic voting issues, and he is frequently consulted by major media outlets for his views on the security of electronic voting machines. Professor Jones holds a B.S. in Computer Science from Carnegie Mellon University and an M.S. and Ph.D. in Computer Science from the University of Illinois.

28. Professor David Dill is the founder and primary public spokesman of VerifiedVoting.org, a non-partisan organization that advocates transparent, reliable, and publicly verifiable elections in the United States. Professor Dill is a Professor of Computer Science and, by courtesy, Electrical Engineering at Stanford University. Since becoming involved in the electronic voting controversy, Professor Dill has served on the California Secretary of State's Ad Hoc Task Force on Touch-Screen Voting and currently serves on the IEEE P1583 Committee, and on Santa Clara County's Citizen's DRE Oversight Board. In December of 2003, Professor Dill was one of a select group of presenters at the Symposium on Building Trust and Confidence in Voting Systems sponsored by the National Institute of Standards and Technology ("NIST"). Professor Dill holds an S.B. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology and an M.S. and Ph.D. from Carnegie Mellon University.

29. Science Application International Corp. ("SAIC") is the author of a widely publicized audit and risk assessment of Maryland's electronic voting system that was ordered by Maryland Governor Robert L. Ehrlich, Jr. Founded by Dr. J. Robert Beyster and a small group of scientists in 1969, SAIC is now a Fortune 500 company. It ranks as the largest employee-owned research and

engineering firm in the United States. SAIC and its subsidiaries have more than 43,000 employees with offices in over 150 cities worldwide. SAIC has a standing contract with the State of Maryland to provide information technology security consulting.

30. RABA Technologies LLC (“RABA”) is the author of a widely publicized analysis of the security of the Diebold AccuVote-TS electronic voting machines used in Maryland. This analysis was ordered by the Maryland General Assembly. RABA was founded by Robert Baruch in 1994 with the goal of creating a differentiated peer-based consulting company capable of tackling the most complex and intractable technology problems. With its roster of former National Security Agency and Central Intelligence Agency professionals, RABA has traditionally been a provider of technology consulting services to the Defense and Intelligence communities.

FACTUAL BACKGROUND

The 2000 Presidential Election and the Special Committee On Voting Systems and Election Procedures in Maryland

31. As a result of the constitutional crisis triggered by the 2000 presidential election, Maryland Governor Parris N. Glendening issued Executive Order 01.01.2000.25 on December 4, 2000 establishing a Special Committee to review Maryland’s voting systems and election procedures. The executive order recognized that “the ‘right to vote’ is the most important and fundamental right of the people” and that “the citizens of Maryland must have *the highest degree of confidence in the voting systems and procedures used in the election of public officials and determination of ballot issues.*” Exec. Order No. 01.01.2000.25 at 1 (Dec 4, 2000) (Ex. 8). The order stated that “Maryland’s voting systems and procedures must ensure that all votes are counted accurately.” *Id.*

32. The Special Committee had 15 members with Secretary of State John T. Willis designated as Chair and former State Senators Julian L. Lapidés, Esq. and F. Vernon Boozer, Esq. serving as Vice Chairs. Two Maryland State Senators -- Michael J. Collins and Joan Carter Conway --

and two Maryland State Delegates -- John S. Arnick and Robert H. Kittelman -- were appointed by the respective presiding officers to represent the Maryland General Assembly.

33. The Special Committee's mission was to "evaluate the voting systems and election procedures utilized in Maryland; review existing standards for recounts and contested elections to ensure conformance with the highest professional standards and best practices; recommend appropriate funding sources to provide Marylanders with accurate, convenient and reliable election systems, and recommend statutory and regulatory changes to ensure full and fair elections in Maryland." *Id.* To fulfill this mission, the Special Committee formed workgroups to focus on four areas: (1) voting systems, (2) election and recount procedures, (3) appropriate judicial and administrative remedies, and (4) appropriate funding formulas and mechanisms. *See* Special Committee Report, *supra* at 9.

34. On January 4, 2001, the Special Committee held a public hearing. At this meeting, Marie Garber, the former State Administrator of Election Laws, was invited to speak about the changes enacted as a result of her work on the Commission to Revise the Election Code. Ms. Garber emphasized that the Committee sought to strengthen the certification of electronic voting systems by mandating compliance with the Federal Election Commission ("FEC") standards and by requiring the approval of an Independent Testing Authority ("ITA") in a National Association of State Election Directors ("NASSED") program before an electronic voting system could be certified.

35. Moreover, Ms. Garber advised the Committee to take into account certain considerations in choosing a new Maryland voting system. Specifically, Ms. Garber emphasized that Maryland required "a proved system; no prototype for us" and an "audit trail, so the election can be reconstructed and recounted if necessary." *Id.* at 63. The goal was to ensure that Maryland "will not look like the next Florida when it has its next recount." *Id.* at 60.

36. Touch-screen direct recording electronic voting machines ("DREs") constitute the latest technology. *See id.* at 60-63. These machines allow a voter to enter a vote on a machine, which it then

records electronically. *See id.* The problem with this technology, however, is that the machines are not conducive to recounts. *Id.* As a result, Ms. Garber emphasized that the Committee must “explore the method for recount” of DREs. *Id.* at 60. Ms. Garber warned the Committee not to “forget the software when choosing a voting system” and raised a number of serious questions about the selection of any DRE for the State of Maryland, including “Does it count accurately? ... Has it been used in enough real elections so that the bugs have been identified and eliminated? ... Do you realize that if any user of any voting system tells you he has had no problem with his system, you are not getting a straight story?” *Id.* at 61. Ms. Gerber went on to emphasize the importance of accurate, secure, and reliable software. *See id.*

37. A subsequent public meeting was held on January 18, 2001, and public work sessions were convened on February 1 and 7, 2001. The Special Committee issued its Final Report and Recommendations later that month. Among the major findings and recommendations of the Special Committee were (1) the State Board of Elections, in consultation with the LBEs, should, as soon as possible, select and certify a uniform mandatory voting system for use in all polling places in Maryland and a uniform absentee voting system for use in all jurisdictions; (2) the preferred uniform voting system for all polling places in Maryland should be a direct recording electronic voting system; and (3) the preferred absentee ballot voting system should be an optical scan voting system with uniform procedures and standards for counting in all jurisdictions. *See id.* at 41-42. The Special Committee emphasized that “the quality of voting systems does make a difference in the accuracy of counting votes.” *Id.* at 8.

38. The Committee noted that in the 2000 Presidential election, 19 counties in Maryland used optical scan voting systems, three counties (Allegheny, Dorchester, and Prince George’s Counties) used mechanical lever voting machines, one county (Montgomery County) used the Datavote voting system, and Baltimore City used a Direct Recording Electronic Voting system. *See id.*

at 24. The Committee quickly summarized the problems with mechanical lever machines and noted that Maryland law required that all such systems be decertified as a matter of law on January 1, 2002 as a result of the problems. *See id.* at 20. Similarly, the Committee noted that the 2000 Presidential Election exposed the weaknesses of the Datavote system and warned that “a situation not dissimilar to the 2000 Florida experience could arise” if such a system was used. *Id.* at 21. It was clear to the Committee that “the disadvantages of the Datavote system outweigh any of the system’s advantages.” *Id.*

39. The Committee praised optical scan systems, however, for their ability to detect and alert the voter to overvotes and undervotes while the voter was in the booth, and because optical scanning systems have an “audit trail which is built into the system in three ways: the memory pack, the tape printout, and the voter marked paper ballot which can be manually recounted.” *Id.* at 22. The Committee also emphasized that “the experience in Maryland with optical scan voting systems has been generally positive” and that “[w]ith the use of this system, the number of uncounted ballots has dropped significantly in the State.” *Id.* at 24. Notwithstanding its praise for optical scan voting systems, the Committee nonetheless ultimately chose to endorse “the latest in sophisticated voting technology” -- touch-screen DREs. *Id.*

40. Surprisingly, the Committee never explained why the more costly DRE voting system was a better alternative for the State of Maryland than the optical scanning systems, especially considering that the Committee itself had recognized that the use of optical scanning systems in Maryland was “generally positive” and had significantly reduced the number of uncounted ballots in the State. *Id.*

41. The Committee recognized that there could be “some potential difficulties with the implementation of a Direct Recording Electronic voting system,” but it believed at the time that this could potentially be addressed through a rigorous testing regimen:

Comprehensive and thorough testing before and after the election is critical to verifying the accuracy and security of Direct Record Electronic voting system software. This testing is in addition to the testing conducted by an independent certified testing authority prior to the certification by the State Board of Elections. Testing at every stage of the election process is necessary to provide assurance to the voter, candidates, election officials, and the public of the system's ability to count votes accurately.

Id. at 26.

The Committee also noted that “[a]dditional assurances that should be made in the use of a Direct Recording Electronic voting system are outlined in the Voluntary Voting Systems Standards prepared by the Office of Election Administration of the Federal Election Commission,” which had been statutorily adopted by the State of Maryland. *Id.* These standards required a vendor “to submit to an escrow agent the source code and documentation of the voting system.” *Id.*

42. But rigorous testing was not enough. The Committee also believed that it was vitally necessary to lay out stringent criteria for the selection of any DRE for the State of Maryland. Specifically, the Committee found that the DRE should “[p]roperly record a voter’s ballot choices by preventing overvoting and unintentional undervoting ... [p]rovide the voter an opportunity to review his or her choices and, if necessary, to correct any ballot errors prior to casting the vote ... [b]e available for leasing rather than purchasing in order to take advantage of anticipated technological advances ...[and] ***[b]e capable of creating a paper record of all votes cast in order than an audit trail is available in the event of a recount.***” *Id.* at 41. The Committee noted that this last criterion -- ***the need for “a paper audit trail with a marked ballot”*** -- was designed to address concerns with its bold embrace of this new technology and referred to it as necessary to provide “instinctive security” against any problems that may arise. *Id.* at 48.

43. The Committee concluded its Report and Recommendations by emphasizing the importance of public confidence and trust in any electronic voting system. It noted that “[i]n a speech to the delegates of the Constitutional Convention in 1787 urging an end to divisiveness and in support of the proposed new governing document, Ben Franklin observed, ‘Much of the strength and efficiency

of any government, in procuring and securing happiness to the people, depends on *opinion*, on the general opinion of the goodness of that government, as well as of the wisdom and integrity of its governors.’” *Id.* at 49 (emphasis in original). Franklin’s observations ring true today. The citizens’ perception and opinion of their government and political leaders is based, in no small part, on their level of trust in fair, open, and accurate elections.

**The Maryland General Assembly Enacts the Special Committee’s
Recommendations Into Law**

44. On April 5, 2001, the Maryland Legislature passed HB 1457 into law, authorizing the State Board of Elections to select, certify, and acquire a voting system for voting in polling places, and a voting system for absentee voting that meets uniform statewide standards. The Statement of Purpose for HB 1457 is clear: the bill mandates that the conduct of elections “should inspire public confidence and trust” by assuring that all voters are treated fairly and equally, that security and integrity are maintained “in the casting of ballots, canvass of votes, and reporting of election results,” and that the prevention of fraud and corruption is “diligently pursued.” HB 1457 § 1-201(A) (2001) (Ex. 9).

45. In addition, following the Special Committee’s recommendation, the new Maryland law specifically forbids the Maryland State Board of Elections from certifying an electronic voting system unless it determined that the voting system will (1) protect secrecy; (2) protect the security of the voting process; (3) count and record all votes accurately; (4) protect all other rights of voters and candidates; and (5) be capable of creating a record of all votes cast in order that an audit trail is available.” *See Maryland Code* (2001) § 9-102(c) of the Election Law Article (hereinafter “Maryland Election Law”). Similarly, if the State Board subsequently learns that the electronic voting system was insecure, the new law requires the State Board to decertify the machines until such concerns are addressed. *Id.* § 9-103(a)(2). On May 15, 2001, the Governor signed the bill into law.

46. In conjunction with HB 1457, the State Board promulgated regulations designed to carry out the Election Bill’s mandate. Those regulations require, in pertinent part, that the voting

system “shall be capable of providing an audit trail of all ballots cast so that, in a recount, the election can be reconstructed, starting with the individual votes of all eligible voters.” Maryland Code of Regulations § 33.09.02 (2001) (Ex. 10).

The Purchase Decision

47. On July 17, 2001, the State Board issued a Request for Proposals for Direct Recording Electronic Voting Systems and Optical Scan Absentee Voting System for Four Counties. Offerers were required to comply with state and federal law and “clearly demonstrate and document” that all proposed equipment and software comply with the FEC’s voting system standards regarding DREs and optical scan equipment, and are qualified by an ITA approved by the NASED.

48. The Request for Proposal (“RFP”) also demanded that the voting systems “produce a record of each vote,” report all votes cast with 100% accuracy, alert the voter to undervotes and prohibit overvotes before the final vote is cast, and provide for safeguards against tampering, theft, or damage. Md. Bd. Of Elections, Req. for Proposals, Project No. SBE-2002-01, at 12 (“MD Bd. Elections RFP”) (July 17, 2001) (Ex. 11). In addition, the RFP required that prices for future purchases for hardware and software will meet a “lowest cost” provision, which guarantees that the Contractor will adjust its Maryland prices for all equipment and software purchased in the future to “no more than the price(s) charged to any other non-Federal customer for the same or equivalent hardware or software.” MD Bd. Elections RFP, *supra* at 7.

49. To decide which touch-screen system was best, the State Board established a “Procurement Review Committee” comprised of a five member panel of security and technical specialists. After meeting with Diebold and other vendors, however, the Panel quickly realized that the nascent DRE electronic voting technology was neither mature nor secure enough to use in actual election. Indeed, the Panel was so concerned about the lack of security and reliability of the DRE systems that it sent a letter to the State Board on Oct. 24, 2001 ***declining to endorse any of the touch-***

screen systems for use in Maryland. See Scott Shane, *Scientists Say ‘Nay’ to Computerized Voting; Group Assails Machines as ‘Inherently Subject to Programming Error,’* The Baltimore Sun, July 27, 2003 at 1A (Ex. 12).

50. But despite the clear warning of the technical committee, the State Board nonetheless announced shortly thereafter that it had selected the lowest bidder -- Global/Diebold Election Systems -- as the vendor for the new DRE voting systems in Maryland. Maryland paid approximately \$6.6 million and the four Maryland counties paid another \$6.6 million to procure 4,678 new Diebold AccuVote-TS voting systems.

51. At that same time, and again despite knowing that the Procurement Review Committee concluded that DREs were unfit for an election, Secretary of State John T. Willis -- the Chair of the Governor’s Special Committee on Voting Systems and Procedures -- publicly touted the Diebold AccuVote-TS’s “accuracy of capturing voter intent.” Press Release, Md. State Bd. of Elections, “Voting System Procurement: State Board of Elections Select Voting System Vendor” (Dec. 7, 2001) (Ex. 13). The Maryland public, however, was unaware at this time that a Committee established by the State Board itself declined to endorse the use of electronic voting machines in Maryland because of reliability and security concerns. The findings of the Procurement Review Committee were confidential, and the conclusions were not made public until the *Baltimore Sun*’s report in July 2003.

52. Secretary of State Willis also stated the goal of the Diebold purchase was to “give Marylanders the opportunity and confidence that they now use at the gas pump and the supermarket checkout.” *Id.* But Maryland voters would not receive a paper record when it elected the next President of the United States as they would at the gas pumps and supermarket checkouts to which Willis referred. This false portrayal of the accuracy and security of the electronic voting machines was the first in a long line of misrepresentations that Maryland Election officials would make to the Maryland public regarding the voting machines.

**Despite Growing Concerns, Maryland Fully Commits
to the Diebold Electronic Voting System**

53. The State Board's experience with Diebold in preparing for the September 2002 primary elections (in which the Diebold AccuVote-TS electronic voting systems were first used in four Maryland counties) vindicated the Procurement Review Committee's warnings. State Board Administrator Linda Lamone reported to the House Commerce and Government Matters Committee that implementing the Diebold system "has been a nightmare." Christopher Sherman, *Maryland Elections Fume Over Service*, The Daily Record, Oct. 9, 2002 (Ex. 14). Ms. Lamone complained that members of the Diebold staff charged with helping to implement the system "*are not responsible people.*" *Id.* In addition, she alleged that Diebold did not comply with all of its contractual requirements, and that Diebold provided an insufficient number of staff to help implement the system. *See id.* Even the staff that Diebold did provide, moreover, was "inexperienced." *See id.*

54. Indeed, the problems the State Board faced with Diebold nearly rendered the 2002 election a disaster. David Heller, Project Manager for Maryland's Board of Elections, reported to the House Commerce and Government Affairs Committee that Maryland election officials "really had to scramble to make sure [Maryland] didn't have a failed election in September" because of the problems with Diebold. *Id.* And this was only the beginning.

55. After the 2002 elections, a number of concerns with the Diebold electronic voting system began to arise. For example, in early February 2003, Beverly Harris, the author of the influential *BlackBoxVoting* book, reported that she was able to freely access an insecure file transfer protocol ("FTP") server used by Diebold programmers to exchange and update some parts of Diebold's allegedly secure software *simply by running a Google search.* Bev Harris, *Voting System Integrity Flaw Discovered at Diebold Election Systems*, Scoop, Feb. 5, 2003 and Feb. 10, 2003 (Ex. 15). The FTP server contained what Harris called "a virtual handbook for vote-tampering": diagrams

of remote communications setups, passwords, encryption keys, source code, user manuals, testing protocols and simulators, as well as files containing votes and voting machine software. *See id.*

56. The FTP was quickly taken down and employees of Diebold admitted on February 4, 2003 that they had been using an insecure server to program Diebold software. Maryland would later learn that the source code used in the Diebold machines that hosted the 2002 election contained massive security vulnerabilities and was the same source code Beverly Harris discovered on the Internet by running a Google search.

57. Yet, despite the negative experience with Diebold in the September 2002 elections and the increasingly apparent security vulnerabilities with the Diebold electronic voting system, the Maryland Board of Public Works, with the blessing of the State Board, announced on July 21, 2003, that it would nonetheless move ahead with the purchase of an additional 11,000 Diebold AccuVote-TS systems for approximately \$55.6 million.

The First Shoe Drops: The Johns Hopkins Report

58. On July 23, 2003, Professor Aviel Rubin and colleagues at Johns Hopkins University's Information Security Institute produced a technical report entitled "Analysis of an Electronic Voting System," which publicized their technical findings and security analysis that the Hopkins scientists performed on the Diebold source code discovered by Beverly Harris. The authors had not intended to publish their report at the time, but Maryland's statewide purchase of the Diebold machines prompted immediate publication.

59. "As a result of the Florida 2000 presidential election," the Hopkins Report began, "the inadequacies of widely-used punch card voting systems have become well understood by the general population." Hopkins Report *supra*, at 3. The Hopkins Report noted that there have been several computer science studies that "caution against the risks of moving too quickly to adopt electronic

voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing.” *Id.*

60. The most fundamental problem with such a voting system, according to the Hopkins Report, is the software itself:

[T]he entire election hinges on the correctness, robustness, and security of the software within the voting terminal. Should that code have security relevant flaws, they might be exploitable either by unscrupulous voters or by malicious insiders. Such insiders include election officials, the developers of the voting system, and the developers of the embedded operating system on which the voting system runs. If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters.

Id.

In essence, the authors warned that the software used in the Diebold electronic voting machines was inherently susceptible to security vulnerabilities, which would allow someone to alter the results of an election without ever being detected.

61. Despite the opposition of computer scientists, however, the Hopkins Report observed that there seemed to be “increasingly widespread adoption of ‘direct record electronic’ (DRE) voting systems.” *Id.* The Hopkins Report warned that “many government entities have adopted paperless DRE systems without appearing to have critically questioned the security claims made by the systems’ vendors.” *Id.* at 4. Until recently, the authors warned, such systems “have been dubiously ‘certified’ for use without any public release of the analyses behind these certifications, much less any release of the source code that might allow independent third parties to perform their own analyses.” *Id.*

62. Although some vendors, including Diebold, claimed that a concept known as ‘security through obscurity’ justified such refusals, the Hopkins Report noted that the security community’s “universally held belief” was that this was inadequate. Indeed, the fallacy of the vendors’ claims, the Hopkins Report noted, is evidenced by the fact that the supposedly secure source code repository for

Diebold's AccuVote-TS DRE voting system -- the same system in use in Maryland -- had recently been unwittingly made available to everyone on the Internet.

63. The authors used this glaring security lapse as a unique opportunity to analyze the source code of the widely used Diebold AccuVote-TS system and to evaluate Diebold's security claims. The results were astonishing. The Hopkins Report uncovered “*significant and wide-reaching security vulnerabilities*” with the system:

Most notably, voters can easily program their own smartcards to simulate the behavior of valid smartcards used in the election. With such homebrew cards, a voter can cast multiple ballots without leaving any trace. A voter can also perform actions that normally require administrative privileges, including viewing partial results and terminating the election early. Similar undesirable modifications could be made by malevolent poll workers (or janitorial staff) with access to the voting terminals before the start of an election. Furthermore, the protocols used when the voting terminals communicate with their home base, both to fetch election configuration information and to report final election results, do not use cryptographic techniques to authenticate either end of the connection nor do they check the integrity of the data in transit. Given that these voting terminals could potentially communicate over insecure phone lines or even wireless Internet connections, even unsophisticated attackers can perform untraceable ‘man-in-the-middle’ attacks.

We also saw no evidence of any change-control process that might restrict a developer's ability to insert arbitrary patches to the code. Absent such processes, a malevolent developer could easily make changes to the code that would create vulnerabilities to be later exploited on Election Day.

Id.

The previous computer science studies cautioning against the use of electronic voting machines had only scratched the surface. The potential for foul play created by these security vulnerabilities was almost limitless.

64. To address these concerns, the Hopkins Report concluded that -- contrary to Diebold's universally rejected security through obscurity claim -- “an open process would result in more careful development, as more scientists, software engineers, political activists, and others who value their democracy would be paying attention to the quality of the software that is used for their elections...”

Id. at 21. They noted that “[s]uch open design processes have proven successful in projects ranging from very focused efforts, such as specifying the Advanced Encryption Standard (AES) through very large and complex systems such as maintaining the Linux operating system.” *Id.*

65. The Hopkins Report also echoed the earlier recommendation of the Special Committee and noted that “**currently the most viable solution for securing electronic voting machines is to introduce a ‘voter verifiable audit trail.’**” *Id.* A voter-verified paper audit trail would provide a check against the exploitation of security vulnerabilities through a paper ballot verified by the voter before the ballot commingled with the Diebold software:

A DRE system with a printer attachment, or even a traditional optical scan system (e.g. one where a voter fills in a printer bubble next to their chosen candidates), will satisfy this requirement by having a piece of paper for voters to read and verify that their intent is correctly reflected. This paper is stored in ballot boxes and is considered to be the primary record of a voter’s intent. If, for some reason, the printed paper has some kind of error, it is considered to be a ‘spoiled ballot’ and can be mechanically destroyed, giving the voter the chance to vote again. As a result, the correctness of any voting software no longer matters; either a voting terminal prints correct ballots or it is taken out of service. If there is any discrepancy in the vote tally, the paper ballots will be available to be recounted, either mechanically or by hand.

Id. at 3-4.

These “voter-verifiable audit trails are required in some U.S. states,” the report confirmed, and “major DRE vendors have made public statements that they would support such a feature if their customers required it.” *Id.* at 21. Indeed, Diebold has stated publicly many times that such a feature is readily available.

66. The Hopkins Report concluded by emphasizing that “[t]he model where individual vendors write proprietary code to run our elections appears to be unreliable, and if we do not change the process of designing our voting systems, **we will have no confidence that our election results will reflect the will of the electorate.** We owe it to ourselves and to our future to have robust, well-designed election systems to preserve the bedrock of our democracy.” *Id.* at 21.

**The Reaction to the Hopkins Report: Diebold Spins and Attacks
as Security Concerns Grow**

67. The controversy engendered by the Hopkins Report grew exponentially when it was revealed that the source code the Hopkins team reviewed had been used in actual elections. On July 29, 2003, Beverly Harris observed that the version numbers from the code found on Diebold's FTP site corresponded to the version numbers listed as having been approved on the National Association of State Elections Directors website. Bev Harris, *Diebold Rebuttals Don't Stand Up*, Scoop, July 29, 2003 (Ex. 16). Soon thereafter, on August 4, 2003, a Diebold spokesman by the name of Mike Jacobsen confirmed in *Wired* magazine that the flawed source code analyzed by the Hopkins scientists was indeed used in the November 2002 general elections in Georgia, Maryland, and in counties in California and Kansas. Louise Witt, *More Calls to Vet Voting Machines*, Wired News, Aug. 4, 2003 (Ex. 17).

68. Two days later, on Aug. 6, 2003, Dr. Douglas Jones, a Professor in the Computer Science Department at the University of Iowa, presented a paper at the USENIX Security Symposium in Washington D.C. entitled "*The Diebold AccuVote-Ts Should Be Decertified and What This Tells Us About the Certification Process.*" Professor Jones independently verified the findings in the Hopkins Report and called for the decertification of the Diebold systems. See Douglas W. Jones, *The Diebold AccuVote-Ts Should Be Decertified and What This Tells Us About the Certification Process*, USENIX Security Symposium (August 6, 2003) ("Jones Presentation") (Ex. 18). Indeed, he noted that the Hopkins Report had found a security flaw that he had brought to Diebold's attention six years earlier. *Id.* at 3. He argued that for Diebold "[t]o allow a security flaw of this magnitude to remain uncorrected after being informed of its existence and after the flaw has been described in public exhibits a serious disregard for security!" *Id.* Finally, he observed that the Hopkins Report "represents more than just a black eye for Diebold. ... [I]t represents a black eye for the entire system of Voting System Standards promulgated by the Federal Election Commission and the National

Association of State Election Directors. Not only did the I-Mark/Global/Diebold touch-screen system pass all of the tests imposed by this standards process, but it passed them many times, and the source code auditors even gave it exceptionally high marks. Given this, should we trust the security of any of the other Direct Recording Electronic voting systems on the market?" *Id.*

69. Diebold's response turned nastier in the ensuing days, as Diebold began to spin, attack those who criticized its machines, and pull together as much support as possible from those state election officials whose vested interests were aligned with their own. At the same USENIX Security Symposium that Dr. Jones presented his paper, it was revealed that Diebold had sent letters to officials at Johns Hopkins University asking not only for the retraction of the Hopkins Report but also threatening action against the authors.

70. In addition, the Diebold admission that the code had been used in actual elections, along with and several other parts of the *Wired* article, were replaced at some point on or soon before August 11, 2003 with far more carefully worded statements from Diebold. In the revised version, Diebold's Director of Corporate Communications John Kristoff -- Mike Jacobosen's supervisor -- replaced the admission of his subordinate with a quote that flatly stated that the code "on the whole is not the same" as the code used in the previously mentioned elections. Witt, *supra* at 1.

The Second Shoe Drops: The SAIC Report

71. On August 7, 2003, the day after the USENIX Security Symposium where Dr. Jones called for the decertification of the Diebold systems based on the analysis presented in the Hopkins Report, Maryland Gov. Robert L. Ehrlich Jr. ordered an outside audit and review of the Diebold electronic voting system scheduled to be in place for the March 2004 presidential primary election by Science Application International Corp. The SAIC team was led by project manager Frank Schugar. SAIC was to complete their risk assessment in four weeks and produce findings for the Governor to review before determining whether Maryland would move forward with the \$55.6 million purchase of

the Diebold machines. The Department of Budget and Management and the State Board jointly managed the project.

72. SAIC performed a risk assessment from August 5, 2003 through August 26, 2003 using the methodology documented in National Institute of Science and Technology SP 800-30, *Risk Management Guide for Information Technology Systems*, and the State of Maryland's Certification and Accreditation Guidelines. The assessment provided "an in-depth analysis of security controls, including comprehensive personnel interviews, documentation reviews, site surveys, and evaluation of the system's hardware and software." SAIC Report, *supra* at 1-2.

73. On September 2, 2003, at the insistence of the State of Maryland, SAIC published a ***heavily redacted and condensed*** version of its 200-page Risk Assessment Report on Diebold AccuVote-TS Voting System and Processes. Only 69 pages (40 pages of the Report plus 29 pages of the Appendix), most of which were significantly redacted, were released to the public. Nonetheless, the State Board could not hide the core findings of the SAIC report, which ***confirmed*** and ***expanded upon*** the security concerns identified in the Hopkins Report.

74. SAIC found that the implementation of the Diebold AccuVote-TS system in Maryland was "***at high risk of compromise***" because SAIC had "identified several ***high-risk vulnerabilities in the implementation of the managerial, operational, and technical controls for AccuVote-TS voting system.***" *Id.* at V. In total, according to the Washington Post, SAIC found no less than ***328 security weaknesses, 26 of which were deemed critical and "high risk."*** If these vulnerabilities are exploited, the SAIC report warned that "***significant impact*** could occur on the accuracy, integrity, and availability of election results" and "damage the reputation and interests of the SBE and the LBEs." *Id.*

75. Management Controls. The SAIC report found widespread security vulnerabilities with Maryland's management and implementation controls for the Diebold AccuVote-TS electronic voting

system. Specifically, SAIC found that the Diebold AccuVote-TS voting system “is not compliant with State of Maryland Information Security Policy & Standards” and that the State Board had not “ensured the integrity of the AccuVote-TS voting system.” *Id.* at 3, 4. In addition, SAIC criticized the State Board’s failure to implement several management controls deemed to be best practices, such as a System Security Plan and system security training, and the State Board’s failure to require certain security practices, such as the secure transmission of election vote totals and the review of computer audit trails.

76. Operational Controls. The SAIC report also found significant security vulnerabilities with the operational controls for the Diebold AccuVote-TS electronic voting system in Maryland. SAIC noted that the State Board relies upon Diebold -- the vendor that Linda Lamone had previously characterized as “not responsible” -- to load the version of the Diebold software certified by the Independent Testing Authority even though this is the State Board’s primary responsibility. *See id.* at 7. Without supervision, the SAIC report noted, Diebold could easily load uncertified versions of the software onto the machines (as we have now learned Diebold had done in California). *See id.* at 8. Moreover, SAIC found that the State Board’s GEMS server is connected to the State Board intranet (and thus the Internet) even though the security controls for the system require that the system not be networked, thereby potentially exposing the system to a wealth of malicious Trojan Horses, worms, and other viruses that could be used to interfere with or even alter the election. *Id.* at 8.

77. Technical Controls. Finally, the SAIC report found that there are numerous security vulnerabilities with the technical controls for the Diebold AccuVote-TS voting system in Maryland. Audit logs are not configured properly and not reviewed and the GEMS server configuration is not compliant with State of Maryland Information Security Policy & Standards for identification and authentication, both of which makes it easier for the system to be hacked without anyone ever knowing. *Id.* at 8.

78. Notably, the above-referenced security concerns are the only control failures that were publicly disclosed in the heavily redacted SAIC report. Others are apparently so serious that redaction was necessary. To address these concerns, SAIC promulgated a list of recommended steps designed to mitigate the risks associated with Maryland's implementation of the Diebold system. *See id.* at 4-5. SAIC cautioned, however, that steps would only *reduce* the risk to the system, not eliminate them all together. *See id.*

Denial: The SAIC Report's Aftermath

79. Despite the explicit findings of the SAIC reports, the State Board remained undeterred. SAIC's findings that Maryland's implementation of the Diebold system created a "high risk of compromise" that could "damage the reputation and interests of the SBE and the LBEs" did not seem to concern Diebold or the State Board.

80. On September 23, 2003, the State Board sent a letter to James C. DiPaula, Jr., Secretary of the Department of Budget and Management, recommending that the State proceed with Phase II of the implementation of the Diebold AccuVote-TS electronic voting system in Maryland and go ahead with the \$55.6 million purchase of the Diebold machines. Steven T. Dennis & Thomas Dennison, *State Keeping Quiet on Flaws in Machines*, *The Gazette*, Oct 6, 2003 (Ex. 19). Gilles W. Burger, the Chairman of the State Board, reacted to the SAIC report by flatly stating that "we believe we are fully prepared to roll out the revised Diebold machines." Inexplicably, Secretary DiPaula concurred in this sentiment: "We remain very confident in this voting system." Tom Stuckey, *State to Go Ahead With Purchase of Touch-Screen Voting Machines*, *Associated Press*, Sept. 25, 2003 (Ex. 20).

81. This decision emboldened Diebold to spin the SAIC report beyond the realm of credibility. "After the completion of the SAIC analysis," Diebold spokesman Mark Radke proclaimed that "it's obvious that the security of our system *is very, very sound*, and voters should feel comfortable using our terminals." David Nitkin, *Voting System Found to Have Election Risks*, *Baltimore Sun*, Sept.

25, 2003. (Ex. 21) And Thomas W. Swidarski, president of Diebold Election Systems, said the SAIC study “verifies that the Diebold voting station provides an unprecedented level of election security.” Stuckey, *supra*.

82. Diebold’s denials and the State Board’s move prompted outrage amongst computer scientists and concerned Maryland voters. Aviel D. Rubin, the lead author of the Hopkins Report, expressed astonishment at how Maryland could possibly proceed with the purchase of the machines after SAIC uncovered so many security vulnerabilities: “If you commission SAIC to do a study and write a report, and they come back and say that the system is insecure, it would seem to make sense to suspend the plans to use the system until SAIC writes a report saying that it is safe to use them. It defies logic that Maryland has these plans (to proceed) given what SAIC says about the Diebold machines.” Nitkin, *supra*.

The David Dill White Paper

83. On September 26, 2003, David Dill -- a prominent and widely respected Computer Science professor at Stanford University who had served on the California Secretary of State’s Ad-Hoc Task Force on Touch-Screen Voting, posted a reply to the SAIC report lauding its conclusions regarding the security vulnerabilities, but taking issue with its solution. Indeed, Dill noted that it “is important to understand that ‘mitigating’ a risk does not necessarily reduce that risk to acceptable levels” David L. Dill, *Risk Assessment Report Diebold AccuVote-TS Voting System and Processes*, (2003) (Ex. 22). The most serious flaw in the SAIC report, according to Dill, “is the failure to consider the most obvious alternative for risk mitigation: ***Don’t use touch-screen voting machines.***” *Id.* Dill explained:

By the study’s methodology of considering what is ‘effective, least cost, and easiest implementation,’ optical scan systems are clearly the superior option: they are much more secure than DREs and cost one-third as much. However, this option is not discussed. What about the serious concerns, raised by the Johns Hopkins/Rice report as well as others, that malicious software changes could be introduced by a programmer at the manufacturer? Such changes could easily be engineered to evade

detection by any practical level of inspection or testing. The only reference to the possibility of malicious code in the public portion of report is a recommendation to ‘modify procedures for the Logic and Accuracy (L&A) testing to include testing of time-oriented exploits (e.g., Trojans).’ This is probably a reference to malicious software that uses the election date and time to determine whether votes are being cast in an actual election or during testing. Such software has the goal of appearing to work perfectly during testing, while changing votes during the actual election. This risk mitigation can be easily evaded. Dozens of checks could be used by Trojans to distinguish testing from real elections. And malicious code can be triggered manually by voters, poll workers, or technicians during an election as well.

Id.

84. In addition, Dill questioned whether the Diebold AccuVote-TS electronic voting machines should be trusted even if Maryland adopted all of the recommendations of the SAIC report:

Is it true that, as Governor Robert L. Ehrlich said yesterday, ‘Because of this report, Maryland voters will have one of the safest election environments in the nation’? ***Quite the contrary.*** Since the report ***confirms*** the presence of major security flaws in the software, it provides further evidence that the current regulatory processes are completely inadequate for ensuring the integrity of electronic voting. That applies to ALL systems, not just Diebold’s. More importantly, procedural or design changes cannot solve the most difficult problems. Electronic voting is a more challenging technical problem than other computer security problems, since ballot secrecy requires that vital information be DISCARDED by the computer system. ***Paperless electronic voting is an idea whose time has not yet come. The technology does not exist to do it safely and securely.*** Indeed, SAIC cannot assure us that these machines will be trustworthy, even if all of their recommendations are properly implemented. They say so on page 12: ‘SAIC cannot guarantee or assure that risks, vulnerabilities and threats other than those addressed in this report will not occur nor can we guarantee or assure that, even if the State of Maryland implements the recommendations we have proposed, the State’s business, facilities, computer networks and systems, software, computer hardware and other tangible equipment and assets will not be compromised, damaged or destroyed.’

Id.

85. Dill concluded by observing that “[p]erhaps the most interesting aspect of this report is what is **not** there. If the system will be adequately secure after the proposed procedural changes (as Governor Ehrlich asserts), why is it necessary to hide over two-thirds of the report for security reasons?” *Id.*

The Citizens Complaint

86. As a result of this controversy, Plaintiff Linda Schade, through CVVM, filed a formal Citizens Complaint with the State Board on November 5, 2003. The Citizens Complaint requested that the State Board decertify and stop the purchase of the Diebold electronic voting systems unless and until voters are able to verify their votes before they are cast, and confirm their vote so that a paper record can be produced for random audits and independent recounts as required by state law. Noting that California had recently halted certification of Diebold machines, the Citizens Complaint asked: “Why should voters in Maryland have a less secure and reliable vote than voters in California?” Citizens Complaint, *Electronic Voting Machines That Do Not Provide a Paper Trail Violate the Voting Rights of the People of Maryland*, MD. Board of Elections (Nov. 5, 2003) (Ex. 23).

87. The Citizens Complaint articulated eight separate concerns with the State Board’s implementation of the Diebold system in Maryland:

- The State has ceded responsibility for counting and reporting election results to a private corporation. Ensuring the integrity of the vote cannot occur if the State does not count the vote in a transparent way so interested parties can observe the count.
- The electronic votes are counted in secret, by proprietary software known only to the corporate vendor -- unknown even to election officials tasked with recounts and audits. Thus, there is no open counting or transparency to the election.
- The voting machines do not provide voters with any ability to verify that their vote was accurately recorded.
- The machines do not provide voters with a paper record they can check and then change until it is accurate for a permanent paper record of their correct vote.
- The machines do not produce anything that would allow election judges or election monitors to watch a vote count after poll closing, to ensure the computers were counting the votes accurately.
- The machines do not produce any independent paper trail that will allow local, state and county election officials to randomly audit the machines to ensure their accuracy. The so-called recount that can be done is merely a reprint of a potentially erroneous vote total as if the software has an error in it a recount will only reprint the same software error.
- The machines do not produce any independent paper trail that will allow local, state or county election officials to recount the vote if the election is close, a recount is requested by a candidate or if irregularities appear. A reprint of a potentially erroneous vote total does not an audit make.

- If intentional tampering with the electronic count occurs from insiders or from outsiders the machines will generally be unable to determine that such tampering has occurred. *Id.*

Each of these concerns, the Complaint noted, was validated by both the Hopkins Report and the SAIC Risk Assessment: “As a result of these reports in Maryland, as well as reports throughout the nation, voters cannot have confidence that the Diebold Corporation’s electronic voting machines will count their votes accurately. There are alternative machines, and the Diebold Corp. machines can be retrofitted, to satisfy the need for a paper ballot audit and recount trail as well as ensure the voting rights of Maryland voters, including the blind and disabled communities.” *Id.*

88. The Citizens Complaint concluded by noting the “the bedrock of our democracy is the right to vote. Maryland is quickly moving to put in place electronic voting machines that make it impossible to safeguard the integrity of our vote thereby threatening the very foundation of our democracy. It is essential that the Board of Elections immediately decertify the Diebold machines and stop the purchase of electronic voting machines produced by Diebold Corporation of Ohio unless and until voters are able to verify their votes before they are cast; and confirm their vote for a paper audit and recount trail.” *Id.*

89. The State Board of Elections, however, continued to implausibly deny that there were *any* security concerns with the Diebold electronic voting system. Despite the unanimous results of computer science studies and an internal state audit, as well as real world experiences, Donna Duncan, a spokesman for the Maryland State Board of Elections responded to the Citizens Complaint by flatly stating: “*I don’t know of any problems. ... We have no concerns. We are very confident in the system.*” Kara Kridler, *Campaign for Verifiable Voting in Md. Believes New Voting Machines Will Jeopardize Election Results*, The Daily Record, Nov. 6, 2003 (Ex. 24).

Diebold’s Credibility Sinks Lower

90. At the same time that the Hopkins and SAIC reports were exposing Diebold’s inadequacies and security flaws, a number of internal Diebold memos were published on the Internet

that confirmed that Diebold was aware of its software flaws and had been for years. An October 2001 memo recognized, for example, that anyone could access the audit logs of the votes and change the contents -- without a password. Email from Ken Clark to Support (Oct. 18, 2001) (Ex. 25). Another memo acknowledged that Diebold sold uncertified software that was used in elections, and that the software “really need[ed] more testing.” Email from Ken Clark, engineer for Diebold Election Systems, to Support (Jan. 7, 2000) (Ex. 26).

91. Upon resignation, another Diebold employee charged that Diebold contracted to “provide products and services which do not exist and then attempting to build these items on an unreasonable timetable with no written plan, little to no time for testing, and minimal resources.” Email from Brian Clubb to Global Elections Systems (Oct. 5, 2001) (Ex. 27). He lamented that it “also seems to be an accepted practice [within Diebold] to exaggerate our progress and functionality to our customers and ourselves [and] then make excuses at delivery time when these products and services do not meet expectations.” *Id.*

92. At that same time, a Baltimore Gazette article on December 15, 2003 reported that an internal Diebold e-mail created by “Ken,” principal engineer for Diebold election systems, recommended “**charging Maryland out the yin**” if the state required Diebold to add a voter-verifiable paper audit trail as suggested by the Hopkins Report (and required by Maryland law): “[t]here is an important point that seems to be missed by all these articles: they already bought the system. At this point they are just closing the barn door. Let’s just hope that as a company we are smart enough to charge out the yin if they try to change the rules now and legislate voter receipts.” Steven T. Dennis, *E-Mail Stolen from Diebold is a Call to Gouge Maryland*, Dec. 15, 2003 (Ex. 28). The recipient of this email asked “what does ‘out the yin’ mean?” Ken Clark responded: “**Short for ‘out the yin-yang’**. Perhaps a little too colloquial; apologies for that. In my defense, Google turns up 694 references to the

phrase. *Any after-sale changes should be prohibitively expensive.* Much more expensive than, for example, a university research grant.” Email from Ken Clark to Support (Jan. 3, 2003) (Ex. 29).

93. The Baltimore Gazette reported that State Board Administrator Linda Lamone had told the paper last month that Diebold had -- coincidentally -- given a preliminary estimate of \$1,000 to \$1,200 per machine to add a voter-verified paper audit trail, or up to \$20 million for the state’s more than 16,000 machines -- even though competitor estimates were reportedly less than half that amount. Dennis, *supra*. Notably, to protect against price gouging, Lamone had told the paper that she believed that a “most-favored nation” clause in the Diebold contract required Diebold to give Maryland the lowest hardware price of any state. *Id.* Since Diebold had already provided certain California counties with a voter-verified paper audit trail for free when election officials raised concerns, the natural implication of Lamone’s argument was that Maryland should also be able to secure a voter-verified paper audit trail without incurring any additional cost. *See Id.* Unease among Maryland voters with Maryland’s planned deployment of the Diebold systems in the 2004 elections escalated even further on December 17, 2003 when *Wired* magazine reported that at least five convicted felons secured management positions at a Diebold subsidiary. *Con Job at Diebold Subsidiary*, *Wired News*, Dec. 17, 2003 (Ex. 30). One of the convicted felons, Jeffrey Dean, wrote and maintained proprietary code used to count hundreds of thousands of votes as a Senior Vice President of Global Election Systems. According to publicly available court documents, Dean served time in a Washington state correctional facility for stealing money and *tampering with computer files in a scheme that “involved a high degree of sophistication and planning.”* *Id.* The other reported felons included a cocaine trafficker and a man convicted of engaging in fraudulent stock transactions. *See id.* This revelation further increased the widespread fears of the potential for computer programmer mischief identified by the Hopkins Report.

The Final Shoe Drops: The RABA Report

94. As a result of this rising tidal wave of criticism, the Maryland Department of Legislative Services (“DLS”) entered into an agreement with RABA Technologies, LLC (“RABA”) -- an IT security consulting firm traditionally serving the Defense and Intelligence communities -- to perform a comprehensive, independent “trusted agent” evaluation of certain aspects of the Maryland State Board of Elections’ plan to use the Diebold AccuVote-TS touch-screen DREs in the upcoming 2004 Presidential elections.

95. The DLS tasked RABA with five specific areas of inquiry: (1) examine and critique the Hopkins Report; (2) examine and critique the methodology and practices used by SAIC in its review of the Diebold equipment and the Rubin report; (3) examine and critique the conclusions reached by SAIC regarding the integrity of the Diebold voting machines and the overall security of Maryland’s election procedures, including whether Maryland made the implementations recommended by the SAIC; (4) examine and critique the Information Technology Security Certification and Accreditation Guidelines as issued by the Maryland Department of Budget and Management; and (5) assist the DLS in comparing existing State Board practices and procedures to those of the counterparts in other states. RABA Report, *supra* at 3.

96. RABA’s highly experienced Innovative Solution Cell (“Red Team”) was tapped for the assignment. This elite group was led by The Red Team Director Dr. Michael A. Werthheimer. Dr. Werthheimer brought to bear 21 years of experience as a cryptologic mathematician at the NSA, he served as Senior Technical Director for the NSA during the last three. Dr. Werthheimer’s Red Team cell also included team members with similar experience at the NSA, CIA, Booz Allen Hamilton, and the National Institute of Science and Technology. This core group was then supplemented by two highly regarded IT security consultants: Dr. William Arbaugh, an Assistant Professor of Computer Science at the University of Maryland and co-author of *Real 802.11 Security: Wi-Fi Protected Access*

and 802.11i, with ten years of experience at the NSA, and Dr. Matt Bishop, an Associate Professor of Computer Science at the University of California-Davis and author of the widely-used textbook *Computer Security: Art and Science*.

97. All Red Team members were given copies of the Diebold source code and access to both a GEMS server and six AccuVote-TS terminals during a one-week period. The results were reported to the DLS on January 20, 2004, and became public a week later when it was reported on by *The New York Times*.

98. The Hopkins Report. The Red Team's first task was to assess the security concerns raised by the Hopkins Report. Unsurprisingly, the Red Team -- like SAIC -- confirmed the findings of the Hopkins Report and applauded the authors for their "thorough, independent review of the AccuVote-TS source code." Raba Report *supra* at 11. After reviewing the source code for the Diebold AccuVote-TS terminals used in Maryland, the Red Team expressed shock at "the general lack of security awareness" in the Diebold source code and found Diebold's apparent disregard for security to be "troubling." *Id.* at 7. Indeed, the Red Team noted, Diebold neglected to even follow widely accepted standards for secure software development, such as the *Carnegie Mellon Software Engineering Institute's Capability Maturity Model for Software and System Security Engineering* in developing the source code for its election systems. *Id.*

99. The SAIC Report. The Red Team's assessment of the conclusions reached by SAIC and the State Board's subsequent mitigation efforts exposed the attempted spin by Diebold and State Board representatives after the SAIC report was released as blatantly false misrepresentations. Indeed, contrary to Diebold and the State Board's statements, the Red Team reiterated that, not only did the SAIC report expose "**a number of high-risk vulnerabilities** across all three categories (management, operational, and technical)," but it also indicated that SAIC had barely scratched the surface of the potential security vulnerabilities that could be exploited in the Diebold AccuVote TS machines. *Id.* at

11. For example, although Maryland had adopted the FEC Voting Systems Standards by statute, the SAIC report had not even attempted to assess Maryland's compliance with these stringent standards relating to the security, accuracy, non-catastrophic error recovery, integrity, audit, etc. of electronic voting systems.

100. In addition, the Red Team found that the Maryland State Board of Elections had **ignored** many of the managerial, operational, and technical concerns identified by SAIC and **failed** to make many of the necessary technical corrections suggested by SAIC to ensure the security and integrity of the March 2004 primary elections:

- **Management Controls.** The Maryland State Board of Elections represented that it met all of the 169 management baseline security guidelines, with all 35 of the security requirements that SAIC found to be in non-compliance corrected. *See id.* at 13. The Red Team, however, found this claim to be dubious. Not only was the supposed documentation of the Maryland State Board of Elections' corrective actions "scattered" but the Red Team also suggested that there was in fact reason to believe that some of the corrective actions had not been fully met. *Id.* at 13-14.
- **Operational Controls.** Similarly, contrary to the State Board's representations, the Red Team found that the State Board had **completely failed to correct 15 operational security requirements**, several of which were denoted "**high risk.**" *Id.* at 14. The Red Team emphasized that "*not only must these high risk vulnerabilities be mitigated, it is imperative that they be independently reassessed before the system is put into use. They are critical to the legitimacy of the electronic tally.*" *Id.*
- **Technical Controls.** Finally, again contrary to public representations, the Red Team found that the State Board had **failed to correct another 15 technical security requirements**. But there was even more cause for alarm. SAIC -- unlike the Red Team -- did *not* have access to the Diebold source code. This meant that even those security requirements that SAIC deemed met depended entirely on the "the presumed integrity of the Diebold software and the Microsoft operating systems (Windows CE on the touch-screen terminals, and Windows 2000 on the server)" -- which is a questionable assumption. *Id.* "Good security practice (defense-in-depth)," as explained by the Red Team, "acknowledges that systems do fail and constructs layered defenses to prevent or at least mitigate the subsequent damage." *Id.* at 14-15. But, because SAIC did not have access to the source code, "**no accounting is made for the failure of any of these systems.**" *Id.* at 14.

These findings directly contradict Diebold and the State Board's public statements after the release of the SAIC report.

101. The “Red Team” Exercise. After reviewing both the Johns Hopkins and the SAIC Reports, the Red Team determined that a “Red Team exercise” was necessary to completely test and stress the exact electronic voting system -- the Diebold AccuVote-TS -- that Maryland intended to deploy for the March 2004 primaries. A “Red Team exercise,” as explained by the Red Team, “is designed to simulate the environment of an actual event, using the same equipment and procedures of the system to be evaluated.” *Id.* at 16. The Red Team is then “free to experiment with attack scenarios without penalty” and, as a result, “a broad range of vulnerabilities may be discovered and validated in an operational environment.” *Id.* The actual “Red Team exercise” took place on January 19, 2004. *See id.* at 15-16.

102. At the outset, the Red Team noted that its “Red Team” exercise was contractually limited (in dollars) from the start, thereby hampering its ability to conduct a comprehensive security review of the Diebold AccuVote-TS machines. *See id.* Indeed, as the Red Team noted, the total Diebold software package contains over 285,000 lines of source code, only a fraction of which could be carefully studied. *See id.* To make up for this limitation, the Red Team’s narrowly focused its efforts on only a few likely vulnerabilities: smart card vulnerabilities, AccuVote-Ts terminal security, GEMS server security, and the method used to upload results following an election.

103. *Smart Cards.* Smart cards are an integral part of the Diebold AccuVote-TS system. A voter inserts a Voter Access Card into a Diebold AccuVote-TS terminal to call up the proper ballot for the individual voter. The contents of the smart card are password protected in order to preserve the security integrity of an individual vote. ***Shockingly, however, the Red Team found it was easy to gain access to the contents of the smart card.*** Not only could modern technology break the rather simplistic default password system devised by Diebold, the Red Team actually was able to ***simply guess the password and gain instant access to the card’s contents.*** *See id.* at 16-17. Indeed, the passwords used to protect both types of smart cards actually appeared in the openly published source

code that the Johns Hopkins team evaluated. As a result, the Red Team concluded that ***“[i]t must be assumed that these passwords are well known.”*** *Id.* at 16.

104. Once the Red Team gained access to the card’s contents, they were able to cause numerous disruptions: (1) they were able to duplicate them; (2) they were able to change a voter card to a supervisor card (and vice versa); and (3) they were able to reinitialize a voter card so that it could be used to vote multiple times. The team estimated that this kind of election fraud could be easily perpetrated ***with a pocket-sized PDA at a relatively minuscule cost of less than \$750.*** *See id.*

105. Finally, the Red Team noted that the Diebold smart cards are neither encrypted nor digitally signed. *See id.* at 17. For example, if a Supervisor Card is inserted into an AccuVote-TS terminal a 4-digit PIN is requested. *See id.* But this PIN can be read directly from the card if the password is known (which, as noted above, is quite likely). *Id.* Once someone knows the PIN on a Supervisor Card, however, that person has the ability to end the election, clear the vote counts, or vote multiple times. *See id.*

106. *AccuVote-TS Terminals.* The Diebold AccuVote-TS Terminals consist of a touch-screen voting terminal with two locked bays, one that contains a roll of paper tape that prints out the initial (“zero count”) vote tally and the final vote tally after the election, and the other bay that houses the on-off power switch, two PCMCIA slots, and a standard keyboard jack. *See id.* at 18. Each of the 16,000 AccuVote-TS Terminals that Maryland has ordered comes equipped with the two locking bays and two keys, for a total of 32,000 locks and keys. *See id.* at 23. The Red Team, however, was ***“surprised”*** to learn that ***“each lock is identical and can be opened by any one of the 32,000 keys.”*** *Id.* And they were easily able to have duplicate keys made at local hardware stores. *Id.* Therefore, the Red Team believed that ***“it is a reasonable scenario to assume that a working key is available to an attacker.”*** *Id.*

107. In addition, the Red Team identified a host of other security vulnerabilities associated with the AccuVote-TS Terminal, including the ability to pick the lock easily, to access the entire directory tree on the Terminal's internal memory and on the PCMCIA card, to remove the PCMCIA card, to load a PCMCIA card with an update file, to install new passwords, to jam the cardreader, to disconnect the monitor, etc. *Id.* at 18. These specific scenarios were ***just “a sampling of the vulnerabilities found as a result of poor physical security coupled with software that fails to use robust encryption and authentication.”*** *Id.* at 19. The team was “confident that physical access to the bay housing the PCMCIA cards, power switch, and keyboard jack can ultimately lead to ***devastating results*** to the particular terminal.” *Id.*

108. *GEMS Server.* The Maryland State Board of Elections uses a Dell computer server running the GEMS software to accumulate and tally votes submitted to it by the Local Board of Elections for each county, who uses the same system to accumulate and tally votes submitted to them by each precinct within the county. *See id.* To accommodate preliminary (unofficial) results, however, the GEMS servers are equipped to receive counts from precincts (in the case of LBEs) and counties (in the case of the State Board) via telephone modem transfer. *See id.* Yet, as a result of this configuration, the Red Team was able to easily access the GEMS software through their modems. *See id.* The security vulnerabilities were both widespread and startling.

109. In particular, the Red Team “verified that the current version of the GEMS software ***still contains many of the vulnerabilities widely published on the Internet***” and condemned the fact that ***“no obvious attention was paid to addressing these weaknesses.”*** *Id.* at 20. For example, the GEMS server lacked several ***critical*** security updates from Microsoft than even most home users of Microsoft operating systems would have known to install. *See id.* Using a software product known as Canvas, the Red Team was able to successfully exploit a well-known vulnerability -- the same one that had been exploited by the infamous “Blaster” worm on August 11, 2003 -- ***to gain complete control of***

the GEMS server. Id. The Red Team was able to easily upload, download, alter and execute election files with full system administrator privileges.

110. The most troubling aspect of this finding, however, is that a Microsoft security advisor previously described the precise security vulnerability that the Red Team exploited, and for which Microsoft had made a patch available nearly six months earlier. All that needed to be done to prevent this devastating attack, which could be used to completely alter the results of a Maryland election, was to update the GEMS software with this critical security update from Microsoft. In all, the Red Team Exercise identified 15 additional Microsoft security patches that had not been installed on the GEMS servers used in Maryland.

111. The Red Team also found that the GEMS server lacked even the most rudimentary security measures, such as firewalls and anti-virus programs, and that the GEMS server could be easily exposed to so-called “man-in-the-middle” attacks as a result of an incomplete implementation of the SSL security protocol. *See id.* at 22. The Red Team concluded that by flatly stating that “*the quantity and quality of the attacks described above is disturbing, especially given the short time the team had access to the system.*” *Id.*

112. Conclusions and Recommendations. The RABA Report’s final conclusion was pointed: “The State of Maryland election system (comprising technical, operational, and procedural components), as configured at the time of this report, contains *considerable security risks* that can cause *moderate to severe disruption in an election.*” *Id.* at 3. To address these security vulnerabilities, the Red Team provided a list of specific near-term mitigation recommendations -- as had the SAIC team before it -- that could be implemented in time for the March 2004 primary. *Id.* **IF and only IF** these recommendations were adopted, the Red Team believed that the system could be used in the March 2004 primary, even if significant security vulnerabilities remained. *See id.*

113. But the Red Team emphasized that the Diebold systems *should not be used* in the November elections without significant overhaul: “between the March and November elections *we strongly feel that additional actions must be taken to mitigate increasing risks incumbent on a system that will receive broad scrutiny.*” *Id.* at 3. Ideally, the Red Team believed that “a pervasive code rewrite would be necessary to instantiate the level of best practice security necessary to eliminate the risks” they had identified. *Id.* at 23. As a result, according to the Red Team, “*the introduction of voter-verifiable paper receipts is absolutely necessary in some form*” by the November 2004 election. *Id.* at 23. “The number of software vulnerabilities such receipts mitigate, the amount of savings they introduce by lowering the procedural requirements, and the trust they garner,” the Red Team reasoned, are “likely to be just as cost effective in the long run as a fully locked-down all-electronic system.” *Id.*

Denial Part II: Diebold and the State Board’s Response to the RABA Report

114. After the RABA report was made public on January 29, 2004, the response from Diebold President Bob Urosevich was predictable spin and hyperbole. Urosevich claimed inexplicably that “the findings in the SAIC and RABA reports both confirm the accuracy and security of Maryland’s voting procedures and our voting systems as they exist today. ... Touch screen voting from Diebold Election Systems has evolved to be the most secure and accurate election system in the history of our democracy.” *Maryland Security Study Validates Diebold Election Systems Equipment for March*, PR Newswire, Jan. 29, 2004 (Ex. 31). And Diebold marketing director Mark Radke echoed that the RABA researchers allegedly “found the system to be very secure.” Elise Ackerman, *Electronic Voting’s Hidden Perils*, San Jose Mercury Times, Feb. 1, 2004, at A1 (Ex. 32).

115. For her own response to the report, State Board Administrator Linda Lamone parroted Diebold’s statement *word for word*: “The findings in the SAIC and RABA reports both confirm the accuracy and security of Maryland’s voting systems as they exist today.” Linda H. Lamone, *Response to: Department of Legislative Services Trusted Agent Report on Diebold AccuVote-TS Voting System*,

Jan. 29, 2004 (Ex. 33). And at a hearing before the Maryland Senate Education, Health and Environmental Affairs Committee and the House Ways and Means Committee, Ms. Lamone specifically refused to adopt many of RABA's near-term recommendations, citing a variety of excuses and irrelevant facts.

116. Notwithstanding the rosy picture of the RABA report painted by Diebold and the State Board, the RABA team members themselves presented a far more frightening view of their report on January 29, 2004. In explaining the significance of the security concerns his team had identified to Maryland legislators and election officials, Dr. Wertheimer warned that “[y]ou are more secure buying a book from Amazon than you are uploading your results to a Diebold server.” Nelson Hernandez, *Md. Voting Machines Vulnerable, Firm Says*, Wash. Post, Jan. 30, 2004, at B1 (Ex. 34). Paul Franceus, another member of the RABA team, put it more bluntly: “Diebold basically had no interest in putting actual security in this system. It’s not like they did it wrong. It’s like they didn’t bother.” Desmon, *supra*. And Dr. William Arbaugh, an Assistant Professor of Computer Science at the University of Maryland with ten years of experience at the NSA and also a RABA team member, stated: “I can say with confidence that nobody looked at the system with an eye to security who understands security.” John Schwartz, *The 2004 Campaign: Technology; Electronic Vote Faces Big Test Of Its Security*, The New York Times, Feb. 28, 2004, at A1 (Ex. 35). Dr. Arbaugh summed up just how easy it would be to exploit a security vulnerability in the Diebold system and alter an election: “the level of effort (needed to get into the system) was pretty low. A high school kid could do this. Right now, the bar is maybe 8th grade.” Desmon, *supra*.

117. After the hearing, Linda Lamone did not disagree with RABA's conclusions, noting that “I don’t disagree with what they say -- they’re the experts.” Yet, at the same time, the denial persisted and she made it clear that she hung on to her belief that the Diebold system was “a very good system.” Hernandez, *supra* at B1. Ultimately, Lamone remarkably concluded that “[i]t’s not worth it this late in

the game to install [the] fixes [the RABA Report] recommended” in time for the March 2004 primary, but nonetheless assured Maryland voters that “the machines could be upgraded by November” for the general elections. Steven T. Dennis, *Flaws, But Hope, in Voting Report*, *The Gazette*, Jan. 30, 2004 (Ex. 36).

118. Notably, the State Board stood alone in its refusal to adopt the RABA near-term recommendations for the March 2004 primaries. Henry Fawell, a spokesman for Gov. Robert L. Ehrlich, Jr., emphasized that “[i]t is **absolutely critical** that the State Board of Elections closely monitor the machines and implement the recommendations.” Hernandez, *supra* at B1. Similarly, Karl Aro, Executive Director of the Department of Legislative Services, advised the Maryland General Assembly in a formal report that “it is **critical** to the success of the election that the State Board of Elections implement the physical security recommendations made by RABA with respect to the AccuVote-TS voting terminals and the GEMS servers” and “it is also **imperative** that SBE take steps to further train local election officials in basic security awareness with respect to the RABA findings.” Karl S. Aro, *A Review of Issues Relating to the Diebold Accuvote-TS Voting System in Maryland*, Jan. 29, 2004 (Ex. 37). As an interim measure, the DLS also endorsed the limited use of a voter-verified paper audit trail for the March 2004 primaries, noting that “it may be possible to equip only a limited number of the terminals in each precinct with the ability to provide voters receipts, check these receipts from randomly selected terminals against the electronic results, and be assured that the overall counts for a precinct are accurate.” *Id.* at 33. The primary objective was “voter confidence in the election system.” *Id.*

119. Similarly, the Campaign for Verifiable Voting in Maryland (“CVVM”) published a white paper on February 4, 2004 entitled “You Can’t Trust Maryland’s Paperless Voting Machines,” which emphasized that the three formal reviews (i.e. SAIC, RABA, and the DLS reports) commissioned by the state of Maryland had all given Maryland’s electronic voting system failing

grades -- but that the State Board had repeatedly and inexplicably ignored the key findings of these voter-funded reports altogether. For example, the CVVM white paper emphasized that both the RABA and DLS reports had noted that the State Board “still has not implemented” the mitigation strategies recommended by SAIC despite public pronouncements to the contrary. Campaign for Verifiable Voting in Maryland, *You Can't Trust Maryland's Paperless Voting Machines*, Feb. 4, 2004 at 4 (Ex. 38).

120. The CVVM white paper also emphasized that the RABA report and subsequent DLS report barely scratched the surface of potential security vulnerabilities with the Diebold electronic voting system. Most notably, the RABA and DLS reports -- unlike the Hopkins Report -- failed to examine the potential for an inside error or inside attack (i.e. by Diebold programmers, developers of the embedded operating system, or possibly even partisan election officials) on the Diebold system. *Id.* at 3-6. Most computer security experts, the CVVM white paper noted, believe that these types of attacks are both a more likely threat to the Diebold system, and a threat that is more likely to succeed. *Id.* at 2. Indeed, the Hopkins Report had found this to be a “considerable” threat. *Id.* Because these types of attack cannot be stopped, the CVVM white paper again reiterated that a voter-verified paper audit trail for all Maryland votes, which would allow for an independent audit and recount of the vote, was absolutely necessary.

121. The CVVM white paper also stated that a voter-verified paper audit trail should not require Maryland to acquire any additional cost. *Id.* at 7. Indeed, Diebold had provided a voter-verified paper audit trail *for free* to four counties in California that had insisted upon such a requirement. *Id.* The CVVM report emphasized that Maryland has been significantly overcharged by Diebold in the past, *paying twice as much per machine as did California*, and that for some reason Diebold had taken an aggressive stance toward Maryland when it was suggested that it also require a voter-verified paper audit trail, citing the internal Diebold emails that revealed that Diebold wanted to

make it “prohibitively expensive” and charge the state “out the ying-yang” for the same technology that it provided to California for free. *Id.* According to the CVVM report, emphasized that “*it seems Maryland is paying more and getting less.*” *Id.*

122. But these entreaties -- from computer security professionals, the Department of Legislative Services, and concerned Maryland citizens -- fell on deaf ears. A mere week after the RABA report became public, Dr. Michael Werthheimer stated that he could “honestly say the problems we are describing will not be addressed in any immediate update.” Elise Ackerman, *Securing Electronic Voting; California Takes Steps to Safeguard System*, San Jose Mercury Times, Feb. 6, 2004 (Ex. 39).

While the State Board Subsidizes a Voter-Funded Corporate Advertising Campaign to Promote Diebold, the Maryland-Commissioned Reports Have Prompted Other States to Act

123. After the RABA report was published, numerous states across the nation began to take a hard line against electronic voting machines and began to require a voter-verifiable paper audit trail. For example, in California, a spokesman for California Secretary of State Kevin Shelley said: “Clearly, Diebold needs to get its house in order or it will not be allowed to continue to do business in California.” *Id.* The next day, Shelley announced extra requirements for computerized voting machines in the March primary to address e-voting security concerns until paper printouts could be provided. *California Taking Closer Look at E-Vote Security*, USA Today, Feb. 4, 2004 (Ex. 40). “The whole purpose is to prevent hackers from getting access to voting equipment,” said Shelley’s spokesman Doug Stone. *Id.* “What we’re talking about today is the overall security of the voting system.” *Id.*

124. Likewise, Nevada will have its systems equipped with printers that will generate a voter-verified paper audit trail in time for the November elections. “The issue is all about accountability,” said Dean Heller, Nevada’s Secretary of State. Robert Tanner, *ATM-Style Voting Machine Worries*, Apr. 2, 2004 (Ex. 41). “These votes are out there in cyberspace somewhere, and

nobody can prove that they exist. The paper trail does.” *Id.* Vermont, Missouri, Washington, and West Virginia have announced similar mandates or proposals.

125. While other states were taking the results of the Maryland-commissioned reports seriously and considering options for instituting a paper trail or decertifying the machines, however, the Maryland State Board of Elections was launching a \$1 million taxpayer-funded advertising blitz promoting the use of the Diebold electronic voting systems, including a website launch, advertisements on buses and billboards, radio and television commercials, and more than 1.5 million pamphlets and brochures. Stephanie Desmon, *Voting Devices Focus of Ads*, Baltimore Sun, Feb. 23, 2004 (Ex. 42). This taxpayer-funded corporate advertising campaign came as a shock to those who had identified the security vulnerabilities with the Diebold system. Avi Rubin observed: “I think the money would be better spent [to] make the system more secure instead of trying to win voter confidence through public relations and not necessarily through anything substantive. . . . The idea of a public relations campaign is showing the superficiality of their approach. They’re trying to (sway) public opinion the way Coca-Cola convinces people that it’s a good soft drink.” *Id.*

126. Maryland continued to aggressively press its Diebold-serving public relations campaign in the days leading up to the March 2004 primary. But reports of glitches with the Diebold systems in primary elections around the country, including Maryland, began surfacing soon after the polls closed. For example, in the March 2004 primary election in Maryland, Jeffrey Liss – a Washington D.C. partner of the law firm of Piper Rudnick -- realized after he had already “cast his vote” that he had not been presented with a ballot section for the United States Senate race on his Diebold touch-screen. Jeffrey F. Liss, *Think You Voted in Md.? Think Again*, Wash. Post, Mar. 7, 2004 at B8 (Ex. 43). When Liss returned and made inquiries to the Diebold technician, the technician confirmed “that the machine was not presenting whole election contests.” *Id.* Liss demanded that he be allowed to cast his vote again, but was told by the Senior Election Judge that it was too late. *See id.* Maryland’s election

officials subsequently rejected Liss's attempts to cast a provisional ballot for the race that his machine was "not presenting." *Id.*

127. These problems were widespread throughout the 2004 primary election season. In Florida, a victory margin in Palm Beach and Broward Counties (both of which use DRE systems) was 12 votes, but the voting machine recorded more than 130 blank ballots. Because it was highly unlikely that 130 people showed up to cast a nonvote in an election with only one race on the ballot, the runner-up wanted a recount. *Florida as the Next Florida*, N.Y. Times, Mar. 14, 2004, at 12 (Ex. 44). There was nothing to recount, however, because the machines were not equipped with a voter-verified paper audit trail. *Id.*

128. In Georgia, voters had to start out using paper ballots in Effingham County because, according to a spokesman for Georgia Secretary of State Cathy Cox, the encoders -- devices used to tally ballot access cards, which voters insert into the machines -- were not programmed. *E-Vote Glitches Found in Election*, Wired News, Mar. 2, 2004 (Ex. 45). And Georgia Tech student Peter Sahlstrom said he found 10 Diebold terminals sitting unprotected in the lobby of the school's student center on Primary Day. Sahlstrom photographed the machines in their unlocked cases. *See id.*

129. More recently, California's Alameda County lodged a formal contractual Complaint against Diebold in late March 2004, stating that Diebold is "not adequately performing its obligations." Ian Hoffman, *County calls out Diebold execs*, Alameda Times-Star, Mar. 24, 2004, (Ex. 46). Alameda demanded that Diebold deliver within 10 days a written plan to correct problems with its voting systems, such as flawed and uncertified voter-card encoders that broke down in 200 polling places in the March primaries and inclusion of uncertified software and hardware. *See id.*

130. The City of San Diego released a report in early April acknowledging that software glitches in the Diebold's vote tabulating system caused the city to miscount 2,821 votes in the Democratic presidential primary and the Republican U.S. Senate Race. San Diego also discovered in

mid-April that “faulty power switches built into a key component” of Diebold’s election system was the primary cause of computer glitches that occurred on March 2. Helen Gao, *Faulty Switches Blamed for Voting Woes Manufacturer Says It Will Fix Problem*, The San Diego Union-Tribune, Apr. 14, 2004 (Ex. 47). As a result, the California Voting Systems and Procedures Panel is currently considering decertifying the Diebold equipment. *See id.*

131. While these handful of instances are emblematic of a widespread problem, the most troubling aspect of Maryland’s embrace of the Diebold electronic voting system is that an eighth grader could completely alter the results of a Presidential election ... and no one would ever know. When the stakes are high, Avi Rubin has pointed out, “people will go to extraordinary measures to beat the system.” Schwartz, *supra*. For example, in the Breeders’ Cup betting scandal in 2002, a computer programmer, Chris Harn, and two accomplices exploited a hole for counting wagers to win a Pick-Six bet worth \$3 million. *Three Who Cheated Breeders’ Cup Computer System Face Sentencing*, USA Today, Mar. 20, 2003 (Ex. 48). Likewise, up until 1996, a conspiracy among slot machine workers rigged the devices with software patches that shifted the odds when a particular sequence of coins was entered. David L. Dill & Aviel D. Rubin, *E-Voting Security*, IEEE Security & Privacy at 1 (Ex. 49). The fraud went undetected from 1992 until 1996, when the ringleader, Rob Harris, won a \$100,000 jackpot with an accomplice in Atlantic City. *Id.* And these are only the cases that have come to light. Indeed, Rubin and David Dill warned of the unknown in a recent article on electronic voting: “We know about the *Harris* case only because he was caught, but how many times have such crimes occurred without being detected? We’ll never know.” *Id.* Therefore, since these concerns apply equally (if not more so) to electronic voting systems, Dill has cautioned that “[w]e don’t have any way of proving the absence of fraud in any of these elections” unless there is a voter-verified paper audit trail. John Schwartz, *Electronic Vote Faces Big Test of Its Security*, N.Y. Times, February 28, 2004 (Ex. 52).

**The State Board's Failure to Decertify the Insecure Voting Machines
Clearly Violates Maryland Election Law**

132. Although the Diebold AccuVote-TS electronic voting machines should not have been certified in the first instance pursuant to MARYLAND ELECTION LAW § 9-102(c), it is clear that the State Board of Elections is required to decertify the Diebold voting system after at least three state-commissioned reports and at least one independent review concluded that the voting machines are insecure and unreliable. Further, inexplicable problems during the March 2004 primaries clearly demonstrated that at least some Diebold machines were not counting and recording votes accurately.

133. The State Board of Elections, pursuant to Maryland Election Law § 9-103, “*shall* decertify a previously certified voting system if the voting system *no longer protects the security* of the voting process.” Maryland’s new electronic voting system, however, fails to protect the security of the voting process in several respects:

- the system contains significant and wide-reaching security vulnerabilities;
- these security vulnerabilities threaten the accuracy of voting and vote counting;
- the system’s current “paper audit capability” cannot “reconstruct” an election in the case that a recount becomes necessary;
- any paper audit conducted by the system necessarily cannot start on the level of the individual voter;
- the machines are only capable of printing after-tally ballot images after the GEMS software encodes the votes and transmits them to the central server over phone lines via modem;
- if a software glitch -- or a person with malicious intent -- caused the wrong information to be sent to the central server, then there would be no audit available to check the altered data against the ballot actually submitted by the voter; and
- the code contains critical security weaknesses that put the system at a high risk of compromise.

134. Similarly, the State Board of Elections, pursuant to Maryland Election Law § 9-103, “*shall* decertify a previously certified voting system if the voting system *no longer counts and records*

votes accurately.” *Id.* Maryland’s new electronic voting system, however, fails to reliably and accurately count and record votes, as:

- the programming code contains massive flaws;
- the flaws inherent in the Diebold system’s hardware and software jeopardize the likelihood that ballots will be counted and recorded accurately;
- inexplicable problems during the March 2004 Maryland primary demonstrated that some machines were not counting and recording votes accurately;
- some machines during the March 2004 Maryland primary did not even display all of the contests in the election; and
- the Diebold system does not provide a voter-verified paper ballot to ensure that the vote recorded by the system is the same as the vote entered by the voter.

135. Each of these requirements is mandatory. Once it became clear that the Diebold AccuVote-TS voting machines were neither secure nor reliable, the Maryland State Board of Elections was required by state law to decertify the machines unless and until the vulnerabilities are fully remedied and a voter-verified paper audit trail is instituted to preserve the integrity of the election.

PRAYER FOR RELIEF

FIRST CAUSE OF ACTION
Against All Defendants
(Maryland Election Law § 12-202)

136. Plaintiffs hereby reallege and incorporate by reference each of the foregoing paragraphs.

137. Maryland Election Law § 12-202 provides that, if no other timely and adequate remedy is provided by that article, a registered voter may seek judicial relief in Maryland circuit court from any act or omission relating to an election, whether or not the election has been held, on the grounds that the act or omission is inconsistent with the article, or other law applicable to the elections process, and it may change -- or has changed -- the outcome of the election and subsequent elections.

138. Plaintiffs are registered voters in the state of Maryland.

139. Defendants have committed several acts and omissions that are inconsistent with several sections of the Maryland Election Law and other law applicable to the elections process, including but not limited to the following examples:

- a. **First**, the Maryland State Board of Elections, pursuant to Maryland Election Law § 9-102(c), may not certify a voting system unless it determines that the voting system will, among other factors:
 - (1) protect the security of the voting process;
 - (2) count and record all votes accurately;
 - (3) protect all other rights of voters and candidates; and
 - (4) be capable of creating a paper record of all votes cast in order that an audit trail is available in the event of a recount.
- b. Defendants Linda Lamone and the Maryland State Board of Elections, as described in paragraphs 1 to 131, have committed an act or omission that is inconsistent with § 9-102(c) of the Maryland Election Law and other law applicable to the elections process by certifying Diebold AccuVote-TS electronic voting machines that do not (1) protect the security of the voting process, (2) count and record all votes accurately, (3) protect all rights of voters and candidates, and/or (4) create a paper record of all votes cast in order that an audit trail is available in the event of a recount.
- c. **Second**, the Maryland State Board of Elections, pursuant to the “Minimum System Requirements” outlined in Maryland State Regulation 33.09.07, has itself promulgated a regulation that provides that a “voting system **shall** be capable of providing an audit trail of all ballots cast so that, in a recount, the election can be reconstructed, **starting with the individual votes** of all eligible voters.”
- d. Defendants Linda Lamone and the Maryland State Board of Elections, as described in paragraphs 1 to 131, have committed an act or omission that is inconsistent with Maryland State Regulation 33.09.07 by certifying and deploying Diebold AccuVote-TS electronic voting machines that are not capable of providing an audit trail of all ballots cast so that, in a recount, the election can be reconstructed, starting with the individual votes of all eligible voters.
- e. **Third**, even if the machines were properly certified in the first place, the Maryland State Board of Elections, pursuant to Maryland Election Law § 9-103, **shall** decertify a previously certified voting system if the voting system **no longer counts and records votes accurately** or **no longer protects the security** of the voting process

- f. Defendants Linda Lamone and the Maryland State Board of Elections, as described in paragraphs 1 to 131, have committed an act or omission that is inconsistent with the mandatory provisions of § 9-103 of the Maryland Election Law by refusing to either (1) decertify the Diebold AccuVote-TS electronic voting machines once it became clear that they were insecure and unreliable or (2) take steps to remedy the security vulnerabilities that could be exploited by the system and institute a voter-verified paper audit trail so that a recount could be conducted if such security vulnerabilities were in fact exploited.

140. These acts and omissions may have changed the outcome of the March 2, 2004 election, and may change the outcome of the November 2, 2004 election.

141. Plaintiffs have brought this action within 10 days after the act or omission or the date the act of omission became known to them. Plaintiff Sharon Beard became aware of the State Board of Elections' actions and omissions with respect to the certification and subsequent refusal to either decertify or fix the Diebold AccuVote-TS electronic voting systems in contravention of state law on April 18, 2004. Plaintiff Judith A. Burns became aware of the State Board of Elections' actions and omissions with respect to the certification and subsequent refusal to either decertify or fix the Diebold AccuVote-TS electronic voting systems in contravention of state law on April 16, 2004. Plaintiffs Linda Shade, Andrew Harris, Mark Elrich, Terry Fitzgerald, and Paul Suh became aware of the fact that the State Board of Elections will use an insecure and unreliable electronic voting system without a voter-verifiable paper audit trail in the November 2004 election in contravention of state law on April 12, 2004.

142. Plaintiffs do not have another timely and adequate remedy under Article 33 of the Maryland Election Law.

WHEREFORE, Plaintiffs request relief on their First Cause of Action as set forth below.

SECOND CAUSE OF ACTION
Against All Defendants
(Mandamus)

143. Plaintiffs hereby reallege and incorporate by reference each of the foregoing paragraphs.

144. Plaintiffs are registered voters in the state of Maryland.

145. Defendants Linda Lamone and State Board of Elections owe mandatory and public duties to Plaintiffs and other registered Maryland voters under Article 33 of the Maryland Election Law and corresponding regulations, including but not limited to the following examples:

- a. **First**, the Maryland State Board of Elections, pursuant to Maryland Election Law § 9-102(c), **may not** certify a voting system unless it determines that the voting system will, among other factors:
 - (1) protect the security of the voting process;
 - (2) count and record all votes accurately;
 - (3) protect all other rights of voters and candidates; and
 - (4) be capable of creating a paper record of all votes cast in order that an audit trail is available in the event of a recount.
- b. **Second**, the Maryland State Board of Elections, pursuant to the “Minimum System Requirements” outlined in Maryland State Regulation 33.09.07, has itself promulgated a regulation that provides that a “voting system **shall** be capable of providing an audit trail of all ballots cast so that, in a recount, the election can be reconstructed, **starting with the individual votes** of all eligible voters.”
- c. **Third**, even if the machines were properly certified in the first place, the Maryland State Board of Elections, pursuant to Maryland Election Law § 9-103, **shall** decertify a previously certified voting system if the voting system **no longer counts and records votes accurately** or **no longer protects the security** of the voting process.

146. Defendants Linda Lamone and the Maryland State Board of Elections have neglected their mandatory and imperative duties under Article 33 of the Maryland Election Law and corresponding regulations.

147. Defendants Linda Lamone and the Maryland State Board of Elections steadfast refusal to either decertify the Diebold AccuVote-TS electronic voting machines or fully mitigate the associated security risks once it became clear that the machines no longer counted and recorded votes accurately nor protected the security of the vote (in violation of mandatory duties imposed upon them by state law) is arbitrary, capricious, and unreasonable. Defendants have abused their offices by

certifying the Diebold AccuVote-TS electronic voting machines, and have refused to perform their ministerial duties by refusing to either decertify them or fully mitigate the associated security risks.

148. Plaintiffs have a clear and indisputable legal right to a secure, reliable electoral process and a voting machine that is capable of providing an audit trail of all ballots cast so that, in a recount, the election can be reconstructed, starting with the individual votes of all eligible voters, and to ensure that Defendants Linda Lamone and the Maryland State Board of Elections properly exercise mandatory duties owed to Plaintiffs and other registered Maryland voters under the Maryland Election Law.

149. Plaintiffs do not have another timely, specific and adequate remedy that can afford complete satisfaction.

WHEREFORE, Plaintiffs request relief on their Second Cause of Action as set forth below.

THIRD CAUSE OF ACTION
Against All Defendants
(Maryland Code, State Government, Section 10-125)

150. Plaintiffs hereby reallege and incorporate by reference each of the foregoing paragraphs.

151. Plaintiffs are registered voters in the state of Maryland.

152. Under the Maryland Administrative Procedure Act, a court may determine the validity of any “regulation” if it appears to the court that the regulation or its threatened application interferes with or impairs, or threatens to interfere with or impair a legal right or privilege of the petitioner.

153. Under the Maryland Administrative Procedure Act, a “regulation” includes “a statement or an amendment or repeal of a statement” that has general application and future effect. It includes a guideline, rule, standard, statement of interpretation, or statement of policy.

154. A regulation may only be adopted pursuant to the procedures found at Maryland Code, State Government section 10-101 et seq.

155. Defendants' refusal to decertify the Diebold electronic voting system, notwithstanding the requirement of Maryland State Regulation 33.09.07 that a voting system "shall be capable of providing an audit trail of all ballots cast so that, in a recount, the election can be reconstructed, starting with the individual votes of all eligible voters," represents an amendment, repeal, interpretation or statement of policy with respect to Maryland State Regulation 33.09.07.

156. Defendants have in practical effect amended Maryland State Regulation 33.09.07 so as to allow voting systems that do not provide an audit trail. Defendants have effectively adopted this amendment without following the Administrative Procedure Act's requirements for adoption of a regulatory amendment. Defendants' action is effectively an underground regulation. Defendants' action directly affects the rights of the public.

157. A declaratory judgment is proper under Maryland Code, State Government section 10-125, to declare invalid Defendants' unlawful regulation.

158. An actual controversy has arisen and now exists between the parties.

159. Plaintiffs have suffered and will continue to suffer irreparable harm as a result of the Defendants' violations of the Maryland Administrative Procedure Act.

WHEREFORE, Plaintiffs request relief on their Third Cause of Action as set forth below.

FOURTH CAUSE OF ACTION
Against All Defendants
(42 U.S.C. § 1983)

160. Plaintiffs hereby reallege and incorporate by reference each of the foregoing paragraphs.

161. Plaintiffs are registered voters in the state of Maryland.

162. Defendants Linda Lamone and Maryland State Board of Elections, acting under color of state law, have certified and administered an electronic voting system that fails to comport with fundamental constitutional guarantees, including the right to vote and the plaintiffs right to have their votes uniformly, securely, reliably, and accurately recorded, counted, and able to be recounted.

163. Defendants' acts and omissions violate, and threaten to violate, plaintiffs' rights under the Fourteenth Amendment of the U.S. Constitution.

164. An actual controversy has arisen and now exists between the parties.

165. Plaintiffs have suffered and will continue to suffer irreparable harm as a result of the Defendants' constitutional violations.

WHEREFORE, Plaintiffs request relief on their Fourth Cause of Action as set forth below.

FIFTH CAUSE OF ACTION
Against All Defendants
Article 24 of the Maryland Declaration of Rights

166. Plaintiffs hereby reallege and incorporate by reference each of the foregoing paragraphs.

167. Plaintiffs are registered voters in the state of Maryland.

168. Defendants Linda Lamone and Maryland State Board of Elections, acting under color of state law, have certified and administered an electronic voting system that fails to comport with basic due process and equal protection rights under Article 24 of the Maryland Declaration of Rights, including the right to vote and the plaintiffs right to have their votes uniformly, securely, reliably, and accurately recorded, counted, and able to be recounted.

169. Defendants' acts and omissions violate, and threaten to violate, Plaintiffs' rights under the Article 24 of the Maryland Declaration of Rights.

170. An actual controversy has arisen and now exists between the parties.

171. Plaintiffs have suffered and will continue to suffer irreparable harm as a result of the Defendants' constitutional violations.

172. A declaratory judgment is proper under the Maryland Uniform Declaratory Judgment Act and MD. Code Ann., Cts. & Jud. Proc. § 3-409. An actual controversy exists between the parties, antagonistic claims are present between the parties indicating imminent litigation, and Plaintiffs assert

to vindicate their legal rights, which have been impinged by the actions of Defendants Linda Lamone and the State Board of Elections.

WHEREFORE, Plaintiffs request relief on their Fifth Cause of Action as set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court enter judgment in their favor:

On the First Cause of Action:

Entry of an Order declaring that Maryland's current voting machines do not comply with Article 33 of the Maryland Election Law, corresponding regulations, and other law applicable to the elections process; and entry of an injunction requiring Defendants to decertify all voting machines that do not comply with Article 33 of the Maryland Election Law, corresponding regulations, and other law applicable to the elections process in order to protect the security and integrity of the November 2, 2004 general and subsequent elections. The machines should stay decertified until such time as they can be updated to comply with the strictures of Maryland law that safeguard the security and integrity of Maryland's voting systems. Such updates should include without limitation the full implementation of the procedural safeguards identified in the RABA report and the IEEE's current security proposal, the institution of a voter-verified paper audit trail, and such other measures as prove necessary to ensure the accessibility of the new machines. The presence of these safeguards should be confirmed by independent experts. Although plaintiffs believe that such an update can be implemented in time for the November 2, 2004 election, if upgrading the voting machines in time for the November 2, 2004 election should prove impossible, the pre-existing infrastructure necessary to revert to the use of paper ballots remains in place in Maryland, and could be effectively utilized until such time as Defendants upgrade the new voting machines to comply with Maryland law.

On the Second Cause of Action:

Entry of a writ of mandate requiring respondents to decertify all voting machines that do not comply with Article 33 of the Maryland Election Law, corresponding regulations, and other law applicable to the elections process in order to protect the security and integrity of the November 2, 2004 general and subsequent elections. The machines should stay decertified until such time as they can be updated to comply with the strictures of Maryland law that safeguard the security and integrity of Maryland's voting systems. Such updates should include without limitation the full implementation of the procedural safeguards identified in the RABA report and the IEEE's current security proposal, the institution of a voter-verified paper audit trail, and such other measures as prove necessary to ensure the accessibility of the new machines. The presence of these safeguards should be confirmed by independent experts. Although petitioners believe that such an update can be implemented in time for the November 2, 2004 election, if upgrading the voting machines in time for the November 2, 2004 election should prove impossible, the pre-existing infrastructure necessary to revert to the use of paper ballots remains in place in Maryland, and could be effectively utilized until such time as Defendants upgrade the new voting machines to comply with Maryland law.

On the Third Cause of Action:

Entry of an Order or Orders declaring that Defendants actions and omissions have been and continue to be in violation of the Maryland Administrative Procedures Act.

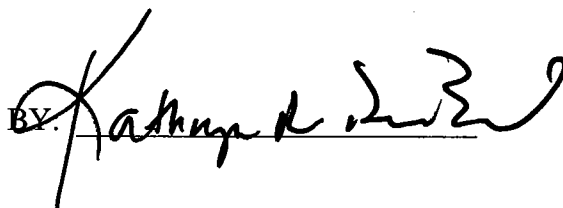
On the Fourth and Fifth Causes of Action:

Entry of an Order or Orders declaring that Defendants actions and omissions have been and continue to be in violation of their federal and state constitutional and statutory duties, including the Fourteenth Amendment to the U.S. Constitution.

On All Causes of Action:

1. Retention of jurisdiction over the parties and the subject matter to ensure that the Court's orders are followed;
2. An award of attorney's fees and costs pursuant to Maryland Code § 3-410;
3. For costs of the suit incurred herein; and
4. Such other and further relief as is just an equitable.

Ryan P. Phair
Kathryn R. DeBord
Daniel M. Nelson
KIRKLAND & ELLIS LLP
655 15th Street, N.W., Suite 1200
Washington, D.C. 20005
Telephone: (202) 879-5000
Facsimile: (202) 879-5200

BY: 

John B. Isbister
Daniel S. Katz
Richard D. Rosenthal
TYDINGS & ROSENBERG LLP
100 East Pratt Street, 26th Floor
Baltimore, Maryland 21202
Telephone: (410) 752-9700
Facsimile: (410) 727-5460

Counsel for Plaintiffs