

# 100 Reasons Why Georgians Need Verifiable Voting Machines

## Contents

A. Inadequate Voter Verification .....	2
B. Insufficient Audit Capabilities .....	2
C. Inappropriate Recount Capabilities .....	2
D. Lack of Transparency .....	3
E. Questionable Georgia Election Results .....	3
F. Vote Counting Vulnerabilities .....	3
G. Questionable Certifications .....	4
H. Questionable Testing .....	5
I. Legal Concerns .....	5
J. Lack of Conformance to Federal and State Guidelines .....	6
K. Questionable Results in Other States .....	6
L. Other State Actions Taken .....	6
M. KSU Expert Witness Admissions .....	7
N. Georgia Governmental & Academic Sources Positions .....	7
O. State Commissioned Studies .....	7
P. Corroborating Academic Studies .....	8
Q. Costs of Electronic Voting Machines vs. Optical Scan Tabulators .....	9
R. Public Opinion .....	9
S. Secretary of State Conclusions and Comments .....	9
T. Georgia Supreme Court Judicial Decisions .....	10

## **100 Reasons Why Georgians Need New Voting Machines**

### **A. Inadequate Voter Verification**

1. Voters cannot verify that the votes shown on the screen are actually recorded on the memory card used to tabulate the votes on Election Day
2. Voters cannot verify that the votes shown on the screen are actually recorded internally within the machine
3. There is currently no official ballot of record that documents the votes cast by each voter in a Georgia election
4. Voters no longer have any chain of custody with their actual ballot prior to casting it

### **B. Insufficient Audit Capabilities**

5. Precinct managers cannot audit the candidate totals produced by the machines on Election Day to ensure that the counts for each candidate in a given race are accurate
6. County and state election officials cannot audit the totals produced by the machines on Election Day to ensure that the counts for each candidate in a given race are accurate
7. The voting machines do not have a standard Voter Verified Paper Audit Trail (VVPAT) that was available on other machines in 2002 when Georgia's machines were purchased
8. If a county elections official chose to manipulate precinct results on the county elections server no audit trail is produced of the manipulation
9. If a state elections official chose to manipulate county results on the state elections server no audit trail is produced of the manipulation

### **C. Inappropriate Recount Capabilities**

10. No direct evidence of voter intent is retained for a recount so the voting machines can only re-accumulate and reprint the same unverifiable results previously reported
11. Absentee ballots are rescanned during a recount so if there was an error in the tabulator that error will not be detected in a recount
12. Every electronic vote recount has always produced, and will always produce, the same results as the original count according to the deposition of Professor Britain Williams, who oversaw testing of the machines when they were acquired

#### **D. Lack of Transparency**

13. The voting machines and tabulation servers use proprietary software that is not open for public inspection
14. The actual election data on CDs and other devices is stored with proprietary property of the vendor and does not belong to the counties, state or people of Georgia
15. The state's expert witness, Ray Cobb, of Kennesaw State University's (KSU) Center for Election Systems (CES), admitted in deposition that he is not aware of the format used to store votes cast on the voting cards, the voting machines or the tabulation servers.

#### **E. Questionable Georgia Election Results**

16. In 2002, 3,256 test votes were included in the live election results in Cobb County
17. In 2005, 285 blank voted ballots were recorded in a Cobb County SPLOST referendum that was decided by 114 votes. The blank voted ballots were accepted even though the SPLOST was the only contest on the ballot
18. In 2011, 95 blank voted ballots were recorded in a Cobb County SPLOST referendum that was decided by 79 votes. The blank voted ballots were accepted even though the SPLOST was the only contest on the ballot
19. Roughly \$1.4 billion in taxes were assessed against the people of Cobb County as a result of the lost votes on the blank voted ballots in the 2005 and 2011 Cobb SPLOSTS
20. In 2008, 947 test votes were included in live election results for Lowndes County and a voting machine technician who was not present during the accumulation was charged for the problem
21. In 2010, a GA Supreme Court candidate got 733,770 votes (35%) to earn a runoff position in a 3 way race but she did not campaign, advertise, have a web site, take donations, respond to surveys, accept media requests or register full contact data
22. In their first use in 2002, the voting systems produced gubernatorial and U.S. Senate race results that are nationally recognized as the biggest upsets in the country.
23. In December of 2008, a watchdog group named Velvet Revolution took out an ad in the AJC claiming that in 2002 one U.S. Senator stole the election from another U.S. Senator and there is no way to prove whether or not their allegation is true

#### **F. Vote Counting Vulnerabilities**

24. In 2008, the results of 25,000 Douglas Co. Election Day ballots were placed into a spreadsheet, reviewed by an Election Board member at his home and then re-entered the next day into the county servers
25. In 2012, counties began uploading election results for publication using a procedure that could introduce fraud and errors into the county servers prior to certification

26. Many county election results are now published by SOE software, a Tampa based subsidiary owned by SCYTL, a Spanish conglomerate
27. Our voting machines can be programmed to count improperly while in Test Mode and Election Mode
28. Our voting machines can be programmed to count improperly during a certain date range
29. Our voting machines can be programmed to count improperly after a certain number of ballots are processed
30. Our voting machines can be programmed to count improperly after a receiving an abnormal combination of votes on a ballot
31. Our county tabulation servers can be programmed to produce incorrect results after receiving a signal or false results via a modem or memory card
32. Our voting machines can produce incorrect results after receiving a virus or hack during accumulation

**G. Questionable Certifications**

33. No certifications of any kind have ever been produced for any of the six machine types procured during 2001 and used during the 2002 election
34. Former Secretary of State Cox claims to have certified voting machines in 2001 and 2002 even though they had no independent audit trail of the votes cast as required by law
35. Prof. Williams, the evaluator during the 2001-2002 time period, admitted in deposition that:
  - The machine software was patched in 2002 before the election
  - The '0808' patch required re-certification
  - The re-certification was not performed
  - Failure to recertify that patch is a violation of law
36. A Dec. 3, 2002 letter from S.O.S. office to Diebold indicated that a month after the office conducted the elections they were still awaiting:
  - "A verifiable analysis of the overall impact of the patch to the voting system.
  - "Confirmation that the statewide voting system is appropriately certified,"
  - "Confirmation that the '0808' patch was not grounds for requiring system to be recertified at the national and state level "
37. The tabulation servers were certified in 2002 with a security flaw in that they had hard coded, visible passwords for administration access as identified by the Johns Hopkins University study and acknowledged by Professor Williams in deposition
38. Federal certification conducted by "Independent Testing Authorities" is not independent because those authorities are funded by the voting machine vendors as acknowledged by Professor Williams in deposition.

#### **H. Questionable Testing**

39. In 2001 and 2002, KSU Professor Williams tested candidate voting machines and reported on them favorably even though they did not have an independent audit trail of each vote cast as the law required
40. In 2006, the Kennesaw State University Center for Election Systems tested the Diebold AccuVote TSX machines used for the 3 precinct audit trial pilot and reported favorably even though they were later found by the Secretary of State's 2007 Audit Trail Pilot Project report to have violated the law
41. The Technical Guidelines Development Committee of the Election Assistance Commission (EAC) concluded that: "The [National Institute of Standards and Testing] NIST and the [EAC Security and Transparency Subcommittee] STS do not know how to write testable requirements to satisfy that the software in a DRE is correct."
42. When asked, Professor Williams corroborated the conclusion by responding: "That was written probably by Ron Rivest to his chairman of that STS subcommittee and if he thinks NIST and the STS don't know how to write those requirements, then I don't have any reason to think they can."
43. The Software Qualification Test Report produced by Ciber Inc. for federal certification shows that no penetration analysis has been performed on the equipment to determine the methods and entry points for which they would be vulnerable to attack

#### **I. Legal Concerns**

44. The Georgia voting machines were required by law to have an independent audit trail of each vote cast when purchased on May 3, 2002 and officials admit that they do not have it [See GA21-2-301(B) of the 2001 GA Election Code]
45. Secretary of State Cathy Cox failed to include the legal requirement for an independent audit trail of each vote cast when she issued the 2002 voting equipment Request for Proposal
46. In 2013, a Cobb Superior Court judge ruled that a candidate has "no compelling reason" to view absentee ballots in an election office after a candidate competed in an election
47. Jeffrey Dean, a chief programmer and former Diebold board member was convicted on 23 counts of fraud and embezzlement in Washington state
48. The State Election Board and Georgia Attorney General were given a copy of the conviction papers for Jeffrey Dean but took no action
49. The April, 2007 Audit Trail Pilot Report produced by the office of the Secretary of State admitted that the Diebold AccuVote TSX audit trail used in three precincts during the 2006 election does not conform to Georgia law that mandates secrecy of the ballot

**J. Lack of Conformance to Federal and State Guidelines**

50. The tabulation servers do not comply with 1990 federal Voting Systems that require: “All types of equipment shall incorporate appropriate physical provisions to prevent fraudulent manipulation of the vote recording, counting and reporting processes”. The tabulation servers lack the audit trail capabilities to prevent such fraudulent manipulation as Professor William admitted in deposition
51. The tabulation servers, for the same reasons shown above, do not comply with the 2002 federal Security Standards that state: “Ultimately, the objectives of the security standards for voting systems are ...to protect the system from intentional manipulation and fraud, and from malicious mischief;” For the same reasons shown above
52. The tabulation servers, for the same reasons shown above, do not comply with the Secretary of State Certification policy\_ 590-8-1-.01, on Certification of Voting Systems that indicates certified voting machines will conform to these guidelines

**K. Questionable Results in Other States**

53. In 2010, Alvin Greene won a U.S. Senate primary in South Carolina. 60-40% winner over Vic Rawl, although he created no web site, had no campaign and lost the verifiable absentee ballot count by a 55-45% margin to Vic Rawl who ran an extensive, professional campaign
54. Diebold optical scan tabulators were found to have recorded 16,084 negative votes from a memory card in the 2000 Florida Presidential Election.
55. The Humboldt Co. Election Transparency Project revealed a Diebold software glitch where 200 ballots were deleted from the original certified results in California
56. In a Florida 2006 U.S. House race, electronic voting machines recorded 15% undervotes in a key race and had no audit trail to confirm the results
57. Many states have reported instances where a voter selected a candidate on the touch screen but the screen interpreted the selection as being made for the opposing candidate on the Ballot Summary screen

**L. Other State Actions Taken**

58. States including Maryland, California, Ohio, New Mexico, Florida & Colorado have taken action to ban, decertify or replace Diebold electronic voting machines identical or nearly identical to the ones we use
59. The Maryland House of Delegates voted 137-0 to replace voting machines that are nearly identical to ours with optical scan equipment
60. The state of California initiated a criminal investigation against Diebold and received an out of court settlement of approximately \$2.5 million

61. The state of Ohio filed for punitive damages against Diebold after election officials found accumulation discrepancies and Diebold admitted to a "critical programming error that can cause votes to be dropped while being electronically transferred from memory cards to a central tallying point".
62. The Attorney General of Maryland filed an \$8.5 million lawsuit against Diebold.

**M. KSU Expert Witness Admissions**

63. Professor Williams, who oversaw the evaluations of the voting equipment in 2002, admitted in a sworn deposition that: "If a machine itself was reporting inaccurately on a given election, nobody would know it".
64. Professor Williams also admitted in a sworn deposition that Gems database of election results that is used at the county and state levels can be altered without detection as explained in the Compuware report conducted for the state of Ohio.
65. Former KSU Center for Elections Director acknowledged under oath in deposition that our voting machines do not have an independent audit trail of each vote cast

**N. Georgia Governmental & Academic Sources Positions**

66. A May 2008 Georgia Tech Security Study of the Processes and Procedures Surrounding Electronic Voting in Georgia recommended to: "Study the feasibility of voting equipment offering either non-electronic election auditability or provable electronic vote tallying accuracy
67. A 21<sup>st</sup> Century Voting Commission study concluded in 2001 prior to the machine acquisition: "The chosen system shall have the capability to produce an independent and paper audit trail of every ballot cast"
68. A Senate Slogo Committee concluded prior to the 2002 machine acquisition: "A paper trail must be established in case of system failure"
69. The Fulton Co. Board of Registrations and Elections concluded in 2001 prior to the acquisition that: "Paper ballots are necessary for a recount"

**O. State Commissioned Studies**

70. The DRE Technical Security Assessment performed by Compuware for the state of Ohio explains on Page 64 that, for the Diebold Accuvote TS series machines, "There is a risk that an unauthorized person with access to the GEMS Server can access the database and change ballot definition files and elections results". Page 47 states that: "A tester was able to view records in the database with a viewer. The tester also altered counts and deleted audit log records using MS Access." Page 72 states that: "Risk Likelihood", "Impact Rating" and "Risk Level" for the security concerns mentioned are "High".

71. The same Compuware study also found that Diebold machines had the highest number of security risks of any machines evaluated
72. A study conducted by the Nevada Electronic Systems Division chief reported to the Secretary of State that Diebold machines as tested by Johns Hopkins were “a legitimate threat to the integrity of the election process”
73. An SAIC study commissioned by the Governor of Maryland found 26 critical security flaws out of 328 for the Diebold AccuVote TS
74. A RABA Technologies Study commissioned by the Maryland General Assembly found Diebold had “considerable security risks” that could cause “moderate to severe disruption in an election”
75. A California Voting Systems Panel study identified 23 security measures that required attention and recommended (8-0) for Diebold decertification
76. A subsequent California study led to the permanent ban of Diebold voting equipment after Diebold admitted that the tabulation server records could be altered or deleted without detection

**P. Corroborating Academic Studies**

77. A 2004 Free Congress Study ranked Georgia last in the country for system reliability and recount preparedness, giving the state an F- on a national average of C+. No significant changes have been made in voting equipment made since then
78. A Johns Hopkins Univ. study determined that: “With respect to the Diebold AccuVote TS and TSx, we found gross design and programming errors”
79. The same John Hopkins study also found a security flaw involving hard coded administration passwords that are visible to the programmer and constitute a security flaw also present in the Georgia voting machines as admitted by Professor Williams
80. A Princeton University study demonstrated live on its web site how a Diebold Voting machine could produce results different than what was actually entered by voters
81. A demonstration on HBO’s Hacking Democracy showed how county and state tabulation server results could be changed by a non-technical person without detection as explained in the Compuware study conducted for Ohio
82. A demonstration on HBO’s Hacking Democracy showed how an optical scan tabulator could be hacked to produce incorrect results without the hacker ever touching the machine
83. A University of Cal. Berkeley study corroborated the hacking demonstration shown on HBO and found more security flaws related to the code interpreter



#### **Q. Costs of Electronic Voting Machines vs. Optical Scan Tabulators**

84. Georgia's 30,000 expensive electronic voting machines could be replaced by roughly 3,000 simple optical scan tabulators and ballot markers for the visually impaired thus saving taxpayers millions of dollars per year in testing, certification, logistics and maintenance costs
85. A 2010 study commissioned by the Maryland legislature determined that the state could achieve a complete Return on Investment in about 8 years if they purchased optical scan voting machines to replace their electronic voting equipment that are nearly identical to ours
86. The 10 year useful life of our voting machines was exceeded in 2012 and the repair costs incurred by the taxpayers continue to climb

#### **R. Public Opinion**

87. A 2011 Election Advisory Council town hall series conducted by the Secretary of State's office found that the verifiable voting was the top concern of the Georgia public along with fair and equal ballot access
88. A 2006 Atlanta Journal Constitution survey found that voting machine security was listed by 88% of Georgia voters as an issue of concern, the sixth highest ranking issue of all state and national issues
89. Professor Williams acknowledged public outcry to the Secretary of state's office in 2002 when he admitted in deposition: "We were getting hit from all directions"
90. In his sworn deposition, former Asst. Dir. Michael Barnes authenticated Emails he received during the 2002 evaluation stating that machines "have no external audit trail for voters to ensure that their vote is electronically recorded for the candidate they actually chose"

#### **S. Secretary of State Conclusions and Comments**

91. Secretary Handel's 2006 Basics white paper concluded: "The electronic voting machines currently used in Georgia's elections are already obsolete"
92. Secretary Handel's 2006 Basics white paper concluded: "Voters should have the ability to review their ballot..."
93. Secretary Handel's 2006 Basics white paper concluded: "Procedures must be established for audits of elections to verify that the electronic vote totals are accurate"
94. Secretary Handel's 2006 Basics white paper concluded: "The paper audit trail should be the determining factor in discrepancies in the vote and should be the ballot of record"
95. By 2009, Secretary Handel had reversed her position on the voting machines while accepting roughly \$25,000 in campaign contributions from friends and family of the voting machine vendor lobbyist, Massey and Bowers.

96. In his first 2010 debate Georgia Christian Alliance Secretary of State Brian Kemp said that if the legislature introduced a bill to fix the verifiable voting problem “he would lead the charge” but reversed his position 3 weeks later when the bill was introduced

**T. Georgia Supreme Court Judicial Decisions**

97. In allowing unverifiable voting to continue, the Georgia Supreme Court ignored all U.S. Supreme Court case law for ballot counting and recounting. That case law unanimously requires strict scrutiny to be applied to the fundamental right of voting

98. The Georgia Supreme Court also ignored 41 disputes of fact in denying the right to trial of the Plaintiffs

99. The Georgia Supreme Court ruled that 17 conclusions of fact conflicting with the evidence in a lower court decision would not warrant a trial

100. The Georgia Supreme Court ruled that “voters must assume the risk of necessarily different procedures” even though our absentee ballot and election day voting procedures are unnecessarily different and such a constraint would be a violation of the Equal Protection clauses of the Georgia and U.S. Constitutions.