

---

## Supporting Documentation for:

### “Saving Our Lever Voting System Before Democracy Goes Down for the Count”

One-page summary available at:

<http://sites.google.com/site/remediaetc/home/documents/DownForTheCount.pdf>

<sup>1</sup> Problems plague states around the nation that have moved to electronic voting systems. See lists documenting thousands of software-based voting machines breakdowns as reported in the media at: <http://www.votersunite.org/electionproblems.asp?offset=0&sort=&selectstate=&selectvendor=&selectproblemtyp>

A Pennsylvania legislator recently introduced legislation to allow counties in that state to return to the use of lever voting machines. <http://www.pahouse.com/PR/056041309.asp>

<sup>2</sup> [Voting System Companies Fail to Meet New York State’s Requirements for “Responsible Contractors”](http://www.votersunite.org/info/VendorsProhibited.pdf): *New York State Law Prohibits the State from Entering into Contracts with Any of the Vendors Presently under Consideration*, <http://www.votersunite.org/info/VendorsProhibited.pdf>, and <http://www.votersunite.org/info/UpdatedVendorIrresponsibility807.pdf>

<sup>3</sup> HAVA Section 301(a)(1)(A) expressly states that so long as: “the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall...” comply with five federal standards, the system is HAVA-compliant.

SBoE Commissioner Kellner testified to the NYC Voter Assistance Commission on 12/7/04:

"The federal Help America Vote Act “sets minimum standards for voting machines. Our lever machines satisfy all but one of those standards, that there be at least one machine at each poll site that is 'accessible for individuals with disabilities."

See also, *New York’s Voting System Satisfies and Surpasses HAVA*, <http://sites.google.com/site/remediaetc/home/documents/EACAdvisoryShouldbeRevoked.pdf>

See also *Discredited federal E-voting oversight commission issued an incorrect 2005 'legal advisory' helping to keep NY on a collision course with democracy*, <http://www.bradblog.com/?p=6956>

<sup>4</sup> The litigation synopsis, prepared by the Election Transparency Coalition, describes the various ways in which ERMA is unconstitutional. <http://sites.google.com/site/remediaetc/home/documents/LitigationSummaryfinal109.pdf>. In particular, the Legislature exceeds its authority in precluding election commissioners - who are constitutional officers by virtue of NY’s Constitution, Art II, sec.8 - from performing those duties integral to their office. For example, the ability to safeguard and control the conduct of elections by being able to observe and prevent error and fraud is impossible when software invisibly tabulates votes and election commissioners can no longer witness that the voting machines have been properly programmed. A finding that ERMA is unconstitutional would render any agreement by the State to comply with ERMA null and void.

In 2006 the Department of Justice (DoJ) sued NYS in order to enforce compliance with HAVA. In 2006 the State was not in compliance with HAVA because it had not yet installed BMDs in every polling site. The State, having already enacted ERMA in 2005 requiring the replacement of the levers with software systems, entered into a timetable for the execution of ERMA, *U.S.A v New York State Board of Elections, et. al.*, Civil Action No. 06-CV-0263 (the so called Federal court order). The State never argued that augmenting NY’s lever voting system with BMDs would also be HAVA-compliant since it was intent on implementing ERMA. Therefore there was never a federal court order ruling the lever machines had to be replaced, only an agreement by NYS to comply with a schedule for ERMA’s implementation.

When Governor Cuomo (and later Governor Pataki) entered into an agreement with a Native American tribe to build gambling casinos, legislators, organizations, and individuals opposed to casino gambling commenced litigation challenging the agreement as unconstitutional. The Supreme Court declared the agreement null and

---

void. The Court of Appeals affirmed, finding the Governor had exceeded his constitutional authority in entering into the agreement, *Saratoga v Pataki*, 100 NY2d 801 (Court of Appeals, 2003).

Similarly the State's agreement to implement ERMA in the Federal action commenced by the DoJ, would be null and void if ERMA was declared unconstitutional. There is nothing preventing the State from declining the small fraction of the \$220 million in federal funds earmarked for lever replacement, having now complied with HAVA by installing BMDs.

<sup>5</sup> These are two letters from suppliers of lever machine parts. In the first letter, the Voting Machine Service Center stated that it "can say with confidence that the AVM lever machines in the State of New York could be maintained indefinitely."

<http://sites.google.com/site/remediaetc/home/documents/VotingMachineServiceCenterletter.pdf>

<http://sites.google.com/site/remediaetc/home/documents/ShoupMaint.pdf>

<sup>6</sup> "Elections have gotten very complex and federal and state legislation . . . keeps driving the cost of elections up," Larimer County Scott Doyle said. The vast majority of those costs are paid by county taxpayers. Given the current economic pressures, "I don't know that counties can continue to bear the weight," Doyle said.-- *Counties Struggle on Election Costs*:

<http://www.rockymountainnews.com/news/2009/jan/24/counties-struggle-on-election-costs/>

"Webster County, Iowa: On-going fees charged by ES&S have doubled the cost of elections. In 2005, the county budgeted \$49,000 for elections, but in 2007 the cost skyrocketed to \$110,700 for only 29 precincts and 25,300 registered voters. According to County Auditor Carol Messerly the **increase was primarily because of the maintenance contracts** for the new optical scanners and ballot-marking devices. At this point, the county saw no realistic alternative to paying the exorbitant costs of maintenance since they had already bought the system."

"In March 2006, the Columbus Dispatch reported that, "**The cost of service contracts for new touch screen voting machines has left county elections officials across Ohio in sticker shock.**" The state had a five-year warranty contract for the equipment itself. The service contract at issues was additional — for technical service and support only."

"It just about blew our minds away," said Alice Nicolía, director of the [Fairfield] county Board of Elections."

"We just do not have the money," said Janie DePinto, elections board director. Holmes County officials, too, were in shock."

"This completely blind-sided the county," said Ray Feikert, a Holmes County commissioner in northeastern Ohio. "It's kind of a back-door expense that no one saw coming."

"When the state purchased the equipment, the one-year warranty was equivalent to the ES&S' "Gold Plan," which promises full coverage for the machines, software, and support for all the counties. But, according to Ms. Lyman, the promise wasn't fulfilled. She said that during the first year, ES&S didn't fix even one broken machine — and there were quite a few sitting in the warehouse waiting for repairs. Further, she said they "held parts in hostage," refusing to send them to the counties so they could do their own repairs. Mr. Lyman told the author: ES&S has New Mexico over a barrel. They won't fix the machines; they won't train us to fix them; and they say if we open the hood the warranty is nullified."

--Excerpts from *Vendors are Undermining the Structure of U.S. Elections*,

<http://www.votersunite.org/info/ReclaimElections.pdf>:

<sup>7</sup> See endnote 6

<sup>8</sup> "- Illinois Commissioner of Elections in Cook County, citing tabulation problems by the Sequoia's optical scanners and DREs in the 2006 election said: "**The administration of this election was a train wreck.**" Sequoia officials insisted however that the system "performed very well, overall."

---

“- Texas election programmer William Singer wrote the Secretary of State's office after the 2004 vote to report that ES&S pressured officials to install unapproved software during the presidential primaries. **"What I was expected to do in order to 'pull off' an election ...was far beyond the kind of practices that I believe should be standard and accepted in the election industry."**"

“- California's Secretary of State's 2007 Top to Bottom Review of the voting computers in the state **revealed that Sequoia's voting system could be subverted without "leaving any evidence that the security of the system had been compromised.... Sequoia's security hardening consisted in large part of a customer relations campaign to allay fears that tampering would be a problem."**"

"[A] 2007 Electoral Commission Report produced in response to the problems with the **Dominion optical scanner** used in Britain last year for the first time. Dominion is new to the field, but as the report reveals, the myriad of breakdowns and computer problems experienced by election officials in Britain are not at all new. As the annexed newspaper account describes, **the elections "ended in chaos as the electronic votes were chucked out following a catalogue of errors and the whole thing was recounted by hand, delaying results by several days."** The article went on to state that, "The list of things that went wrong is far too extensive to repeat here, but if you want an example of how not to manage an IT project, look no further than the link at the end of this story."

--Excerpts from *What New York Election Commissioners have to look forward to if Computerized Voting Systems are Permitted to Replace our Existing Lever Voting System*, [http://sites.google.com/site/remediaetc/home/documents/Election\\_Problems\\_Counties\\_Across\\_Nationfor\\_EC\\_NY.pdf](http://sites.google.com/site/remediaetc/home/documents/Election_Problems_Counties_Across_Nationfor_EC_NY.pdf)

<sup>9</sup> See, *New York State Law Prohibits the State from Entering into Contracts with Any of the Vendors Presently under Consideration*, <http://www.votersunite.org/info/VendorsProhibited.pdf>, and <http://www.votersunite.org/info/UpdatedVendorIrresponsibility807.pdf>, See also, *Vendors are Undermining the Structure of U.S. Elections*, <http://www.votersunite.org/info/ReclaimElections.pdf>

<sup>10</sup> *Federal Vote-Counting Accuracy Mandate Is Ignored*, <http://www.votersunite.org/info/AccuracyIgnored.asp>

<sup>11</sup> Over three dozen independent computer scientist reports have proven that software can be undetectably manipulated. Software can be infected by a rogue code which can disguise its tracks and force the machine to mimic normal behavior and election commissioners or other election officials and observers will not be able to detect or prevent the software from miscounting the votes. These studies are available at: [http://sites.google.com/site/remediaetc/home/documents/Scientific\\_Studies\\_7\\_20\\_08.pdf](http://sites.google.com/site/remediaetc/home/documents/Scientific_Studies_7_20_08.pdf)

"Malware can also be designed to be adaptive - changing what it does depending on the direction of the tally. It could also potentially be inserted at any of a number of different stages in the development and implementation process - from the precinct all the way back to initial manufacture - and lie in wait for the appropriate moment." - *Congressional Research Service Report for Congress*, November 4, 2003 <http://theory.lcs.mit.edu/~rivest/voting/reports/Fischer-ElectionReformAndElectronicVotingSystemsDREs.pdf>

The National Institute of Standards and Technology (NIST), the very experts who advise the Federal government on the writing of the certification standards to which New York is trying to adhere, have rejected the notion that certified systems could be secure, finding that:

"[T]esting to high degrees of security and reliability is from a practical perspective not possible."

-- *Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC*, 11/06, <http://vote.nist.gov/DraftWhitePaperOnSlinVVSG2007-20061120.pdf>

All of the testing demonstrating the vulnerability of software voting machines to undetectable hacking was performed on certified system. Certification does not make software safe for use because software can be programmed to perform one way during testing and another way on the day of the election.

"[Y]ou cannot certify an electronic voting machine the way you certify a lever machine. Once the voting machine goes through a lengthy and expensive certification process, any change to the software requires that it be certified all over again. What if a vulnerability is discovered a week before an election? What about a month

---

before the election, or a week after it passes certification? Now the point is that we absolutely expect that vulnerabilities will be discovered all the time. That would be the case even if the vendors had a clue about security.” <http://avi-rubin.blogspot.com/2007/08/secretary-bowens-clever-insight.html>

<sup>12</sup> “There would be no way to know that any of these attacks occurred; the canvass procedure would not detect any anomalies, and would just produce incorrect results.” -- California Voting Systems Technology Assessment Advisory Board Security Analysis, 2/06, commissioned by California's Secretary of State, [http://ss.ca.gov/elections/voting\\_systems/security\\_analysis\\_of\\_the\\_diebold\\_accubasic\\_interpreter.pdf](http://ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf)

For a century lever machines have proven to be difficult and time-consuming to fraudulently modify, each machine having to be separately tampered with. However, with computerized voting systems, the following excerpts from the scientific reports reveal the ease with which election results can be falsified on an optical scanner:

“An attack could plausibly be accomplished by a single skilled individual with temporary access to a single voting machine. The damage could be extensive – malicious code could spread to every voting machine in polling places and to county election servers.” -- *California Secretary of State, Source Code Review of the Diebold Voting System*, July 20, 2007  
[http://www.sos.ca.gov/elections/voting\\_systems/ttbr/diebold-source-public-jul29.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf)

“An Accu-Vote Optical Scan can be compromised with off-the-shelf equipment in a matter of minutes even if the machine has its removable memory card sealed in place. The basic attack can be applied to effect a variety of results, including entirely neutralizing one candidate so that their votes are not counted, swapping the votes of two candidates, or biasing the results by shifting some votes from one candidate to another.

....  
Such vote tabulation corruptions can lay dormant until Election Day, thus avoiding detection through pre-election tests.... [V]oters could be unaware of any discrepancies between their cast votes and the internally recorded votes.” -- *Univ. of Connecticut Voting Technology Research Center, Security Assessment of the Diebold Optical Scan Voting Terminal*, October 30, 2006, [http://voter.engr.uconn.edu/voter/Report-OS\\_files/uconn\\_report-os.pdf](http://voter.engr.uconn.edu/voter/Report-OS_files/uconn_report-os.pdf)

“At any point in a voting machine’s life, from the manufacturer’s shipping dock through intermediate storage to the day of the election, a voting machine could potentially be reprogrammed to report incorrect results.

....  
[R]egardless of whether the software ... is improved to better resist attacks, bugs will always occur and the risk of tampering cannot be overcome. In particular ... while “logic-and-accuracy testing” can sometimes detect flaws, it will never be comprehensive; important flaws will always escape any amount of testing.” -- Dan S. Wallach, *Testimony to National Institute of Standards and Technology and Election Assistance Commission Technical Guidelines Development Committee*, September 20, 2004, <http://www.cs.rice.edu/~dwallach/pub/eac-tgdc-20sep2004.pdf>

A Princeton University computer scientist “describes how the virus propagates ... via memory cards, without requiring any network.” - *Ed Felten, Refuting Diebold’s Response*, September, 2006, <http://www.freedom-to-tinker.com/?p=1065>

“An infected machine will infect any memory card that is inserted into it. An infected memory card will infect any machine that is powered up or rebooted with the memory card inserted. Because cards are transferred between machines during vote counting and administrative activities, the infected population will grow over time.”-- Ariel J Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Princeton University, September 13, 2006, <http://itpolicy.princeton.edu/voting/ts-paper.pdf>

<sup>13</sup> ERMA (EL 7- 202) requires that any voting machine or system **shall**:

“r. ensure the integrity and security of the voting machine or system by:

(i) being capable of conducting both pre-election and post-election testing of the logic and accuracy of the machine or system that demonstrates an accurate tally when a known quantity of votes is entered into each machine.”

---

However, as explained at endnote 14 below, no software-based system can comply with this requirement of ERMA. And here is an actual case of votes miscounted by a Sequoia optical scanner in NY that repeatedly passed its "Logic and Accuracy" test:

"During the canvassing process, it was noticed that the accumulating number of votes reported by ... the scanning system did not match the number reported by individuals who were keeping a hand-tally of votes as the envelopes were opened. .... The test ballots had scanned successfully during the usual [Logic and Accuracy] testing of the scanning system prior to the election and canvass. ... The Pre-election Test ... was repeated again for public observation.... It was repeated again for the Pre-canvass Test ... the day ... of the commencement of the canvass. The results of all of the tests were verified and matched exactly against each other. When the test was run again ... during the canvass, it ran successfully.

"When the ballots of the last Election District were scanned, ... although the ballots had votes correctly marked, the system had reported no votes for those three ballots. A ... report ... was run, and it reported three overvotes for the three ballots. The ... test deck ... again ... ran successfully. The final [Sequoia] Report for the complete paper canvass for the 43rd Council District showed twenty-two overvotes and five blanks. The total results differed from the candidates' hand-tallies." <http://wheresthepaper.org/NYCBOEScanRpt030515.pdf>

<sup>14</sup> Malicious coding, or "malware," can be inserted into software, spread from voting machine to voting machine, and be programmed to disappear once the fraud is accomplished. Election Management System (EMS) computers, commonly known as "central tabulators," reprogram all voting devices before each election, and accumulate and report precinct-level results after an election. Every optical scanner or DRE is reprogrammed before each election using a memory card that tells the machine who is on the ballot and how to count it. But this inherently flawed design poses significant security risks:

"[F]unctionality – the critical element to be certified during the certification process – can be modified every time an election is prepared. Functionality is downloaded separately into each and every machine, via memory card, for every election. With this design, there is no way to verify that the certified or even standard functionality is maintained from one voting machine to the next." -- Harry Hursti, *Security Alert: July 4, 2005, Critical Security Issues with Diebold Optical Scan Design*, Black Box Voting, <http://blackboxvoting.org/BBVreport.pdf>

<sup>15</sup> *Most electronic voting isn't secure, CIA expert says*, <http://www.mcclatchydc.com/226/story/64711.html>  
The article reports that Smartmatic, a voting machine company that partnered with a firm hired by Chavez's government, owned U.S.-based Sequoia Voting Systems until 2007 and that in response to the U.S. Treasury Department's Committee on Foreign Investment investigation, Sequoia divested from Smartmatic, thus ending the inquiry. In fact, the Committee's national security concern was not abated. Recent court documents make clear that Smartmatic still retains the intellectual property (IP) rights over Sequoia, as well as licensing control of the software used in their voting machines and tabulators.  
<http://www.alternet.org/democracy/86135/?page=entire>.

<sup>16</sup> See endnote 4

<sup>17</sup> German Constitutional Court ruling excerpt in English,  
<http://www.bundesverfassungsgericht.de/en/press/bvg09-019en.html>

<sup>18</sup> With the exception of a lone vote in Columbia, these resolutions were passed unanimously by Dutchess, Columbia, Ulster, Schulyer, Greene and Essex Counties, as well as the state-wide Association of Towns.  
<http://sites.google.com/site/remediaetc/home/documents/DutchessLeverRes.pdf>,  
[http://sites.google.com/site/remediaetc/home/documents/ColumbiaCtyLeverResoFeb12\\_09.pdf](http://sites.google.com/site/remediaetc/home/documents/ColumbiaCtyLeverResoFeb12_09.pdf),  
<http://sites.google.com/site/remediaetc/home/documents/UlsterReso.pdf>,  
<http://sites.google.com/site/remediaetc/home/documents/AoTLeverResolution.pdf>,  
<http://sites.google.com/site/remediaetc/home/documents/SchuylerResolutionNo80-1.pdf>,  
<http://sites.google.com/site/remediaetc/home/documents/GreeneCountyLeverResolution.pdf>  
<http://sites.google.com/site/remediaetc/home/documents/EssexCo.Resolution14705.04.09.pdf>

It is irresponsible for NYS to waste its taxpayers' dollars when the evidence that has accumulated since ERMA was enacted overwhelmingly proves what a disgraceful waste, particularly at this time of fiscal crisis, abandoning New York's superior technology, would be.

---

“It all sounds ... too familiar. Taxpayers being asked to throw out millions of dollars worth of voting equipment ... With no guarantee the new equipment will provide a solution to the problems. Technology can often offer a solution to a complicated process, in this case, accurately recording votes. But technology poorly conceived, designed, integrated and tested is a recipe for failure. In this instance, subsidizing the same outfits that couldn't get it right the first time, giving them more chances could lead to the further waste of millions upon millions of taxpayer dollars. “ – Dan Rather, [http://www.hd.net/transcript.html?air\\_master\\_id=A4755](http://www.hd.net/transcript.html?air_master_id=A4755)

“In my analysis, the lever machine deserves recognition as one of the most astonishing achievements of American technological genius, a fact that is reflected in their continued competitiveness against recent voting technologies in every accepted performance measure. .... they offer a level of accuracy, theft deterrence, and transparency that is missing from contemporary technologies.” -- Professor Bryan Pfaffenberger, recipient of National Science Foundation Scholar's Award granted for the study of the history of lever voting machines.

The very close race in NY's 20<sup>th</sup> CD proved lever machines succeed where software machines fail: New York's lever voting machines provide reliable, observable evidence of the count at the election. Software voting machines do not. -- *Clear evidence: Lever voting works* , <http://www.timesunion.com/AspStories/story.asp?storyID=790729&category=COMMENTARY>