Memo I

Supplemented:	To The Honorable Eliot Spitzer, The State Board of Elections, The Office of General Services, The Comptroller's Office
From:	Andrea Novick , Esq.
Date:	August 22, 2007
Re:	New York Cannot Contract with Private Voting Vendors

Since I submitted my July 24, 2007 Memo I (*The voting vendors scheduled for certification testing are ineligible to contract with New York State)* there has been additional critical information further substantiating the theft-enabling potential and highly inferior quality of the electronic voting machines being sold in America today, as well as startling evidence of the irresponsibility of these vendors. Under any and every criteria described in the procurement laws, these vendors cannot qualify as responsible contractors; nor can New York consider purchasing voting machines with such deplorable performance histories whose use poses such enormous risk for our continued democracy.

I have included below some of the additional evidence which has come to light in the past month. This includes California's top to bottom review of these vendors' voting systems, corroborating the unreliability and insecurity of all computerized voting systems;[1] the report from the University of Connecticut demonstrating why VVPAT are worthless[2]; the Florida State University Security and Assurance in Information Technology Laboratory (SAIT) report commissioned by its SOS, validating prior reports that Diebold's Optical Scanners can be hacked without detection; [3] and the Dan Rather investigative report elevating the focus on these vendors from irresponsible to potential violators of state and federal anti-fraud statutes[4]. I do not represent this supplement to be at all comprehensive, since, as I state in my Memo which this supplements, that would be the job of the state employees responsible for ensuring that New York complies with its laws. However, as a citizen concerned with the future of democracy and the threat that secret vote counting on these private computers poses to our sovereignty, I will continue to assist my state in pursuing the proper application of the law.

For my efforts, I have been accused by the OGS of being a vendor or representing the interests of a vendor. For the record I wish to state in writing that I have no such interest. I believe the State of New York should be working towards the development of a secure, transparent, observable voting system in which the people cast their ballots on paper and count those ballots by hand under a strict protocol with sufficient safeguards to minimize election fraud and ensure that the will of the people is reflected in the election outcome. Since no electronic computerized system exists which can accomplish that, I am opposed to the use of any means by which the people are deprived of their constitutional franchise,

which right includes the right to know that their vote is being counted accurately. I further understand that the privatization of the public's elections is illegal, unconstitutional and the essence of undemocratic; particularly when the private companies New York is considering delegating its responsibilities to, insist on the right to process and count the people's votes in secret.

As to the ineligibility of the voting vendors being considered by New York and the inability of the their voting systems to securely and accurately count our votes I add the following information to the memo I submitted to the SBOE, the OGS and the Governor's office.

California's Top to Bottom Independent Testing Confirms That the Existing Private Voting Systems Being Offered in the U.S. Are Insecure, Unreliable and Inaccessible

The Secretary of State of California has now undertaken the most extensive independent testing of DREs and Optical Scanners used throughout the nation. In July, 2007 California's Secretary of State, Debra Bowen, released these reports ("California Reports") going beyond what independent testing by prestigious universities had already exposed. The software security measures in every system tested (Deiblold, Sequoia, Hart Civic[5])could be easily bypassed. In other words, every voting system was readily hackable.

The California reports found that all voting systems examined had a myriad of very serious vulnerabilities. All were susceptible to computer viruses that could infect any of the systems, spread between voting machines and steal votes on the infected machines. All three systems use central tabulators (the machines at election headquarters that accumulate ballots and report election results) which can be penetrated without great effort.

As a result of the findings, all electronic voting systems in the state were decertified. The optical scanners and a single DRE per precinct (for use by the disabled) were recertified for use subject to a long list of conditions yet to be satisfied. Permitting one DRE per polling place was a compromise the SOS felt forced to make to accommodate the disability community and requirements of HAVA, which is unfortunate given that the California researchers found that none of the DRE systems met federal disability standards.

The voting vendors' entire selling point for these more expensive DREs have been the necessity for the disabled to vote on the same machines as other citizens. On this basis DREs have been foisted upon America, the vendors falsely representing that their machines meet federal HAVA mandates for an accessible means of voting in every polling place. The California Reports exposed the falsity of this representation[6].

The results of the California tests were devastating and worse than anticipated even by many election activists and computer scientists who have followed the numerous university security reports, all of which have now been confirmed by the SOS's top to bottom review. Avi Rubin, professor of computer science and technical director of the Information Security Institute at Johns Hopkins University stated:[7]

> *I had expected them to find problems -- but to be able to replace firmware in all three systems is nothing short of* ***an utter takeover of machines, and that shouldn't be possible.***
> ***I was shocked*** *by how severe the problems were.* ***What's even scarier is that the researchers were looking at certified systems that have been already used in an election****.*
>
> (emphasis supplied)

As Rubin points out, the failed systems had passed federal and state testing certification expose the sham certification process Americans have been forced to rely on to protect what are supposed to be free and fair elections.

Matt Bishop, California's principal investigator, generously offered the vendors a way to deflect some fault from themselves by blaming some of these systems problems on Microsoft. As the article, *California Team Finds Three E-Voting Systems Susceptible to Attack*[8], points out in commenting on the report:

> In fact, it went out of its way to be fair, at one point stating that in many cases, the integrity of the voting machines' software may only be as strong as that of the underlying operating system - which, in all three cases was Windows.
>
> "**As Windows is known to be vulnerable to many forms of attack**," Bishop writes, "vendors should ensure that the underlying Windows system is locked down sufficiently to counter these threats. **If an attacker can gain privileged access to the underlying operating system, they can control the election management system**."
>
> That said, the biggest vulnerabilities any of these systems could possibly face is the overwriting of their firmware, through a Trojan file or other means: and in all three cases, UC's "red teams" were able to accomplish this. (emphasis supplied)

The fact that Microsoft shares the blame along with the voting vendors for these eminently tamperable machines is hardly a relief to citizens being told they must vote on these systems developed by the vendors who chose to use Microsoft Windows in creating their voting systems. With or without Microsoft's contribution to the defects, the California Reports substantiate that malicious coding, often referred to as the Trojan horse, can alter the outcome of the election without anyone being able to detect the fraud!

All of these voting machines thus violate New York law which requires that our voting systems or machines be capable of demonstrating their "integrity and security" by being able to "demonstrate an accurate tally" and provide "a means by which a malfunctioning voting machine or system shall secure any votes already cast on such machine or system"[9]. The California Reports have demonstrated, as have prior security reports, that none of the voting machines can comply. None are secure or safe from fraud. None have the safeguards a democratic election requires.

DREs Cannot be Verified, Enable Tampering and are Thus Not Legal for Use in Democratic Elections

The California Reports Found DREs to be Easily Hackable and Unverifiable

The focus of 200 years of voting in America has been the mitigation of tampering in elections. The history of legislative efforts reflect the numerous reforms to protect the integrity of our votes by minimizing the opportunities for tampering. While the legislature may and should legislate to prevent the possibilities for fraud and manipulation, it is constrained from restricting or restraining the right to vote in any other way.

> ***Freedom in voting is guaranteed by the Constitution.....Some restrictions may be necessary in order to so regulate the right as to properly protect it, but any unnecessary or unreasonable restraint is in conflict with the Constitution.***
>
> *Hopper v Britt,* 204 NY 524, 531 (Court of Appeals, 1912)

The researchers in California found all the computerized voting systems, the only systems being considered by New York, lacked effective safeguards to prevent tampering and fraud. Indeed the lack of security revealed by the California Report is so serious that these electronic voting systems potentially disenfranchise millions of citizens and can do so in a way that can never be discovered. Corrupted or malicious data by insiders or poll workers or temporary staff with limited access could alter the outcome of the entire election. The California researchers found[10]:

Virtually every important software security mechanism is vulnerable to circumvention

In the source code review of Sequoia's systems the investigators stated:

> *In fact we are not optimistic that acceptable and practical and secure mitigation procedures are even possible for some of the Sequoia's systems' components and features, at least in the absence of a comprehensive re-engineering of the system itself.*

The Security Evaluation of the Sequoia System Public Report concluded:

> *All of the attacks described in this report can be carried out without any knowledge of the source code.*

The Liberty/Nedap DRE was not among the machines tested in California because New York is the only state considering using the Liberty DRE (see Memo I on the European's experience with this deficient and insecure machine). However the California report of the Hart Voting System[11] refers to the insecurity of the Liberty DRE, describing how the system fails to provide any of the tamper sealing mechanisms commonly employed:

> Key locks: To prevent access to memory cards or sensitive machine ports, many voting machines place a plastic or metal door in front of these ports, using a key lock. Assuming the keys are suitably controlled (and unauthorized duplication is prevented), attackers would be prevented from accessing the protected ports. Of course, if bypassable lock mechanisms are used, or **if access to the locked compartment can be gained without opening the lock, then the locks will offer neither tamper resistance nor tamper evidence as has been observed with both Diebold [11] and Nedap/Groenendaal [14] voting systems.** (emphasis supplied)

California lead investigator Matt Blaze has said about the voting machine code:

> ***The problems we found in the code were far more pervasive, and much more easily exploitable, than I had ever imagined they would be.*** *In other words,* ***the designs of these systems expose generously wide "attack surfaces" to anyone who seeks to compromise them. And the defenses are dangerously fragile*** *-- almost any bug, anywhere, has potential security implications. This means that strengthening these systems will involve more than repairing a few programming errors. They* ***need to be re-engineered from the ground up.*** (emphasis supplied)

The University of Connecticut Confirmed That Paper Trails Are Worthless Because They, along with the Electronic Vote Cast, Can Be Hacked Without Detection, Leaving No Evidence of How a Voter Actually Cast a Vote on a DRE

Exposing the utter insecurity and unreliability of DREs, the California Reports warned that VVPAT of votes cast is not sufficient to guarantee the integrity of an election run on a DRE. A recent report from the University of Connecticut[12] released a few days before the California Reports, demonstrated once again that paper trails (VVPAT) provide no verification that the electronic ballot was counted as the voter intended.

The University of Connecticut researchers hacked into a Diebold DRE. In *"Why VVPAT 'Paper Trails' Are Not Enough*[13]" the author describes how:

> It is possible to alter the ballot definitions of the DRE. The alteration would create the behavior where the votes for two candidates are exchanged. Thus, the voter touches the screen next to the name of John Smith, the screen lights up the selection for John Smith, the voter verifiable paper audit trail prints the name John Smith, but, nonetheless, the invisible electronic ballot accrues the vote to Pocahontas.

It should be observed that the U Conn team had no access to source code or any information not publicly available. The voting vendors' spin in attempting to deflect responsibility for the revelations of the California Report, was that the scientists had the source code and therefore it was like "giving the keys to a thief". The U Conn team didn't have the source code to the DRE they were able to alter. Their report confirms that anyone with access to the DRE can rig the machine and produce what appears to be consistent election records (the electronic tally and the paper trail match) that are not accurate election records. The report also exposed that there were multiple ways to rig the votes cast on a DRE with a VVPAT[14].

New Jersey Denies Certification to its DREs Based on the Failed Performance of the Printers Found by the Independent Testing Authorized by the Attorney General

New Jersey had used paperless DREs in the previous elections. It has relied on reports from the national, so-called independent testing authorities for assurance that these machines were worthy of use. NJ has now changed its law to require that its DREs produce paper records no later than January 1, 2008 and for the first time in the state's history, the state contracted with independent computer experts to conduct testing as part of a certification process. As a result of the testing of the printers to be used to produce

paper trails off the DREs, 33 flaws were found.

The Attorney General contracted with the New Jersey Institute of Technology to test the voter verified paper audit trail printers provided by Sequoia and Avante International. The printers, supplied by the vendors so there is no reason to expect that these were not the best of the printers the vendors could find, ran out of paper too fast, lacked concealed printer cables, and had problems alerting poll workers to malfunctions.

As reported in the Star Ledger[15], *Study: 2008 election paper trail unreliable: Electronic voting records can fail:*

> **The problems**, found by the New Jersey Institute of Technology and posted online yesterday by the state elections division, **potentially could compromise voter privacy and election security, according to the experts' reports**. (emphasis supplied)

As a result, on August 10, 2007 the NJ Attorney General denied certification of Voter Verified Paper Record Systems for Electronic Voting Machines based on the failed testing of the printers. [16]

The printers tested were part of the DRE systems provided by Sequoia and Avante, both of which New York is planning on testing for use in New York. Among the problems cited in the NJ report were the fact that the Sequoia Advantage machine's printers needed to be sealed with locking mechanisms and the mechanical error messages were not specific enough if, for example, there is a paper jam. The committee also said there was too little time for a voter to verify his or her vote on the third and final ballot. (The system allows voters to recast ballots up to three times if they find they have miscast a vote, or failed to cast a ballot for a particular office or missed a ballot question.)

For the Avante Vote Trakker, the committee said the storage unit on some machines needed to be replaced or repaired so that unauthorized paper cannot be slipped into the storage unit. The committee also said the voter-verified paper record system needed to be equipped with a warning system to notify polling officials when there is a malfunction, and voting operations should be suspended if there is a disconnect between the voting machine and the printer.

Avante and Sequoia will attempt to correct the printer problems for retesting in NJ, but the U Conn report and the California Reports have already revealed that regardless of how the printer performs, the DRE is too insecure and unverifiable to be used in any election. The fact that New York is still considering testing any DREs for use is

indefensible.[17]

California Reports Find That Sequoia's Security System is Non-Existent and Based on Lies and Misrepresentations

Not only did Sequoia's voting systems lack the security necessary to provide accurate and reliable elections, but Sequoia's ethics and integrity was again seriously impugned by the California Report which found that Sequoia's security system essentially consisted of a dishonest customer relations campaign.

The findings of the California Reports were particularly disturbing as they reflect on Sequoia's lack of integrity and dishonesty because in addition to submitting a DRE for New York testing certification, Sequoia is also offering Dominion's Optical Scanner for testing. If the Dominion Optical Scanner were to be certified for use in New York, Sequoia would be responsible for the scanners' servicing, maintenance and training.

From *California Team Finds Three E-Voting Systems Susceptible to Attack* (endnote 8):

> **A red team** from UC Santa Barbara **examined the Sequoia Voting System**, which also found itself having fun with ordinary hand tools. "The testers **were able to gain access to the internals of the systems**," writes Matt Bishop [principal researcher for California Reports], "by, for example, unscrewing screws to bypass locks. The screws were not protected by seals. Similarly, plastic covers that were protected by seals could be pried open enough to insert tools that could manipulate the protected buttons **without damaging the seals or leaving any evidence that the security of the system had been compromised."**
>
> The Santa Barbara team uncovered what appeared to be evidence that **Sequoia's security hardening consisted in large part of a customer relations campaign to allay fears that tampering would be a problem**. **It cited Sequoia literature that actually explained to customers that since its software doesn't access any other libraries besides Microsoft SQL Server, no one else could possibly have remote or unauthorized access to its SQL Server database. That whole notion is fundamentally flawed**, the Sequoia red team pointed out, adding that it was able to execute arbitrary commands on the Sequoia database using ordinary SQL Server queries.
>
> Like the Hart system, Sequoia leaves the choice of Windows version installation to its

customers, particularly for its client-side voting systems. Sequoia's documentation recommends Windows 98 and Windows ME, probably for lower profiles or less expensive, older equipment. "This is a problem," writes the Sequoia red team, "because **those Windows versions provide no user-level security**."

The final report for the California Secretary of State paints a picture of a trio of information systems whose security integrity is either fragile or non-existent. In some cases, it seems to indicate that the job of reinforcing security may have, for at least one manufacturer, been assigned to its public relations department. (emphasis supplied)

Notwithstanding the repeated exposure of Sequoia's false statements Sequoia persists undaunted in misrepresenting its product stating at its web site[18]:

> The AVC Edge® provides nothing less than 100 percent accuracy, privacy and security.
>
> The Audit Trail provides an unalterable electronic record of all votes cast during an election

The California Report has now corroborated Sequoia's fraudulent and false representations exposing not only Sequoia's unethical conduct, but its willingness to lie to conceal the fact that its voting system provides an open invitation for manipulation of our elections.

Dan Rather's Investigative Report on Sequoia and ES&S Reveal the Problems of Permitting Our Elections to be Privatized

Not only have Sequoia's security representations been found to be a lie and their systems (as well as the other vendors' systems) lacking the safeguards required of a democratic election, but Dan Rather has now broken some previously unknown and startling news concerning Sequoia's apparent effort to manipulate Florida's 2000 election by sending defective paper, known to create problems, to the heavily Democratic county of Palm Beach County.

Rather spoke with seven whistle blowers, all former employees of Sequoia, who revealed that Sequoia switched to inferior and rejected paper which pre-election testing by Sequoia showed would produce defective punching patterns and hanging chads on the punch card machines used in many states in the 2000 election. The paper, which had been refused

and sent back by Sequoia employees, was brought back in and signed off for by plant managers. The paper was not only different from the paper used in other elections, but was known to not perform well in high humidity conditions, like Florida.

Rather revealed that more than 50,000 Sequoia punch cards were discarded as invalid because it appeared voters had overvoted and on 17,000 of the Sequoia cards, voters seemed to have voted for three or more presidential candidates. In Palm Beach County, 10,000 citizens apparently showed up to vote, but decided not to vote for the Presidential election. Not only were at least tens of thousands of citizens disenfranchised, but Sequoia, has enjoyed huge sales increases as its punch cards machines were replaced by computerized voting machines since the 2002 HAVA response to the problems in Florida!

Voter Action, a national election integrity organization, has called for a congressional investigation of the vendors to determine whether certain voting vendors have committed crimes under federal and state anti-fraud statutes and to look at the increasing influence and control that private companies wage in the way we conduct our elections. [19]

The 8 month investigation by Rather's team also revealed that ES&S was producing voting systems for use in the U.S. in Filipino sweat shops. The factory workers told Rather's team about the faulty, defective touch screens that were being shipped to the Filipino factory for assembly. The video and transcript of the Rathers expose can be found at http://www.hd.net/drr227.html. Rather's report reveals that the ES&S voting systems were created in rat-infested conditions where workers were paid a few dollars/hour working in sweltering, sweatshop conditions, making it difficult for workers to work effectively. There was no testing, no quality control and no concern for the defects that the workers were seeing in the various parts of the voting systems that were shipped to the Phillipines. Nor did ES&S reveal to the EAC that it was using a Filipino factory to assemble some its voting systems, a violation of the EAC's requirements.

The investigative report reveals not only the role Sequoia played in the 2000 debacle as well as ES&S's willingness to deceive and profit at any cost, but demonstrates why private companies, their allegiance to profit, not democracy, have no place in public, democratic elections. It further raises the problem of vendor dependence in which election officials have the vendors taking responsibility for all aspects of the election such that public officials have delegated their entrusted responsibilities and cannot be said to be accountable to the people. This is a blatant breach of New York's Public Officers Law, which provides:

> *The people are entitled to expect from their public servants a set of standards above the*

> *morals of the market place. A public official of a free government is entrusted with the welfare, prosperity, security and safety of the people he serves.* ***In return for this trust, the people are entitled to know that no substantial conflict between private interests and official duties exists in those who serve them.***"
>
> McKinney's Public Officers Law, § 74 (emphasis supplied)

In conclusion Rather asks the question whose answer is implied:

What's more important to you: knowing that your vote is recorded as you cast it? Or the profits of voting machine manufacturers? It's an obvious question, but when citizens try to get to the bottom of how these machines, bought with your taxpayer money, either work or don't work, manufacturers continually hide behind the wall of "trade secrets." Are these machines that determine who decides our laws, who runs our states, and who sits in the White House with the power to direct our armed forces, no different from say the formula for Coca Cola, or McDonald's special sauce? We don't think so, and that's why we tried to get answers tonight and raise questions about accountability.

But, unlike Congress or prosecutors, we aren't armed with subpoena power; we can't force companies to prove that they take concerns about their machines and their ballots seriously. Their message is "trust us," but the information we have been able to obtain suggests that trust has not been earned, and that voting machines warrant, at the very least, much closer scrutiny than they have received so far. Because, as we heard Florida's governor Crist ask, " what could be more important in democracy than making sure that the right to vote is one that we can have confidence in?"

In fact corporate "trade secrets" can never trump the people's right to know, as our legislation has acknowledged:

> ***It is essential to the maintenance of a democratic society that the public business be performed in an open and public manner and that the citizens of this state be fully aware of and able to observe the performance of public officials****.....* ***The people must be able to remain informed if they are to retain control over those who are their public servants. It is the only climate under which the commonwealth will prosper and enable the governmental process to operate for the benefit of those who created it.***
>
> McKinney's Public Officers Law § 100

And "trust us" can never be earned, as Rather suggests might be sufficient were these voting vendors not so undeserving of our trust. Our system of government is built on checks and balances precisely because we are never to sit back and just trust.

Optical Scanners Can Only Be Verified with a Hand Count by the People – in Which Case Why Bother Buying the Machines

Diebold's Optical Scanner Remains Unsafe and Uncorrected Year after Year, Examination after Examination

As a result of the California Reports all optical scanners were decertified, but may be used if the vendors are able to bring them into compliance with restrictive conditions imposed by California. The Diebold Optical Scanner that New York is planning on wasting our tax dollars testing would appear to be the same scanner California has the following to say about [20].

In their executive summary for the Diebold source code review, California researchers conclude:

> Although we present several previously unpublished vulnerabilities, many of the weaknesses that we describe were first identified in previous studies of the Diebold system. **Our report confirms that many of the most serious flaws that these studies uncovered have not been fixed in the versions of the software that we studied.**
>
> … Due to these shortcomings, the security of elections conducted with the Diebold system depends almost entirely on the effectiveness of election procedures. Improvements to existing procedures may mitigate some threats in part, but others would be difficult, if not impossible, to remedy procedurally. **Consequently, we conclude that the safest way to repair the Diebold system is to re-engineer it so that it is secure by design.** (emphasis supplied)

The conditional re-certification requirements for Diebold's Optical Scanners are based on a number of criteria, including reformatting and reinstallation of all software, and for Diebold to work with California to provide documented plans including, but not limited to:

– preventing viral propagation of malicious software
– automated mechanisms to confirm and document system configuration standards and implementation
– prohibition of unauthorized software installation
– procedures for implementing approved security updates
– procedures for operating and maintaining physical and logical security
– prohibition of any network communications among voting system devices
– procedures for programming, pre- and post-election logic and

accuracy testing, and chain of custody
– procedures for vote results auditing and reconciliation
– post election manual auditing requirements to be paid for by the vendor
– problem log for all jurisdictions, available to the public for inspection and review upon request
– increased poll worker training regarding chain of custody, tampering, and other security related issues
– disaster recovery plan for jurisdictions experiencing computerized voting equipment failure
– provision of a working version of all hardware, software voting equipment, and vendor agreement to pay for all software and hardware review by the Secretary of State
– responsibility for representations regarding compliance with all state and federal standards
– establishment of a state user group and hold at least one annual meeting
– escrow deposit of all source code for Secretary of State inspection through independent review

The Diebold AccuVote firware version tested in California was 1.96. The report found that the entire system needed to be re-engineered because it is so insecure by design. If New York's SBOE intends to proceed with an examination of the Diebold Opscan, notwithstanding the abundance of damning evidence, it would behoove it to obtain a representation from Diebold that the model New York plans on testing has been re-engineered before wasting tax payers' dollars.

Report Commissioned by Florida's Secretary of State Corroborates Once Again that Diebold's Optical Scanner Remains Vulnerable to Being Hacked Without Detection

Most recently, even as the California reports were being released, a Florida report[21], confirmed that insider computer hackers can change Diebold voting results without leaving a trace. In a report commissioned by Florida's SOS, experts found still again that Diebold's Optical Scanners remain seriously flawed and uncorrected. As reported by the Associated Press on August 1, 2007 [22]:

> someone with only brief access to a machine could replace a memory card with one

> preprogrammed to read one candidate's votes as counting for another, essentially switching the candidates and showing the loser winning in that precinct.
>
> "The attack can be carried out with a reasonably low probability of detection assuming that audits with paper ballots are infrequent," the report said.

According to a story in the Miami Herald [23]:

> the Florida Secretary of State's office has conducted an elections study that confirmed Tuesday what a maverick voting chief discovered nearly two years ago: Insider computer hackers can change votes without a trace on Diebold optical-scan machines.

Indeed all the reports that have examined the Diebold Optical Scanner have reported the same security flaws, each time finding additional ones (see my Memo I which this Memo updates). The Diebold Scanner is incapable of ensuring the integrity of our elections: it is flawed by design! And yet the SBOE plans on spending good money testing this flawed and failed design.

Questionable Solvency of the Voting Vendors

The inferior quality of these voting machines is becoming increasingly apparent. Two of the three major vendors, Diebold and Sequoia, have tried unsuccessfully to find buyers for their election businesses. Finding no takers, Diebold[24] separated its voting machine division from the parent company . In the first week after SOS Bowen announced she was decertifying and then only restrictively re-certifying some of Diebold's voting systems, a dozen Diebold officers sold off more than a half million dollars in the week *before* the value of the company's stock price would plunge[25].

Sequoia has been looking to sell off its US subsidiary for more than a year, but who would purchase any of these companies after examining the evidence of these faulty, defective, not useable for democratic elections, voting systems. It is this very evidence that I am imploring the SBOE, the OGS and the Comptroller's office to look at.

As the truth of these unreliable, inadequate, insecure voting systems becomes exceedingly difficult to conceal, the lawsuits by the counties who have been saddled with these lemons will continue to grow; as will the penalties, fines and recoveries of monies for the sale of these defective products.

In Riverside County, California the county supervisor, who had been an ardent supporter of DREs, is considering seeking a return of monies wasted on these faulty voting machines[26]. Riverside County has spent almost $25 million on the Sequoia touch-screen machines and may finally be appreciating that these machines are not what they were represented to be. In Pennsylvania, three counties are considering taking their lever machines out of storage after their electronic voting machine company, Advance Voting Systems (AVS) refused to pay the bill to the federal "Independent Testing Authority" (ITA) lab iBeta Quality Assurance which has, according to NJ's Express-Times, found "thousands of source code irregularities and 24 documentation irregularities with AVS machines[27]. In Kentucky, the Attorney General demanded that its electronic voting companies (Diebold and Hart) immediately upgrade their systems in compliance with the California Reports or face a lawsuit by Kentucky[28].

Just this past Tuesday, August 221, 2007, Secretary Bowen announced she'd be holding hearings next month to examine whether ES&S sold uncertified voting machines to as many as five counties. From a statement reported at the Brad Blog (see endnote 5) ES&S faces massive fines in California for illegally modifying the Automark ballot marking devices sold by ES&S:

> "ES&S sold nearly 1,000 voting machines in California without telling the counties that bought them that they had never been certified for use in this state," said Secretary Bowen, the state's chief elections officer. "Given that each machine costs about $5,000, it appears ES&S has taken $5 million out of the pockets of several California counties that were simply trying to follow the law and equip their polling places with certified voting machines."
>
> "Not only did ES&S sell machines to California counties that weren't state certified, it's clear the machines weren't even federally certified when the company delivered them to California," Bowen continued. "While ES&S may not like California law, I expect the company to follow the law and not trample over it by selling uncertified voting equipment in this state."
>
> "If ES&S has broken the law and misled counties into buying nearly 1,000 uncertified machines, I intend to go after the company for the full $9.72 million in penalties allowable by law, along with the original $5 million the company took from counties' pockets," concluded Bowen.

ES&S's InkaVote Plus system, which was sold for use in Los Angeles County, is also in trouble. That system has been decertified pending a top to bottom review, now that ES&S has finally relented and handed over its source code (see my Memo I re: ES&S's arrogance in refusing to comply with California's law). If it turns out the Inka

Vote software was also uncertified (the source code which was eventually turned over did not match the version stored in escrow under state law) ES&S may face similar penalties in Los Angeles County.

Now that California has officially revealed what the voting vendors have been trying to conceal, the misrepresentation and fraudulent contract litigation along with investigations will no doubt subsume the counties and states who are stuck with systems that have been found to be so defective they can't be used. More and more states are refusing to accept the rubber stamp testing the voting vendors had been willing to pay for, instead hiring independent experts who will continue to reveal what the university studies have exposed: that none of these voting systems are fit for democratic elections.

Conclusion

It is irresponsible for New York to continue to waste time and money testing such flawed voting systems produced by vendors who are not responsible and therefore ineligible to do business in New York. The State needs to be spending this valuable time between now and 2008 developing a secure voting system, fully observable by the people, with sufficient safeguards to ensure that voters are not disenfranchised. Anything less is a deprivation of New Yorkers' constitutionally protected franchise. None of the systems being considered by the SBOE can satisfy these minimum standards required by a democracy.

I implore the State to look at the evidence, determine that none of these vendors are qualified to do business in NY and none of their products are acceptable and use the year we have left to design a voting system that is democracy and HAVA-compliant either by instigating the necessary planning for the state to commence hand counting and/or undertaking the development of a publicly-owned open source optical scanner that combines a partial hand count in every precinct on election night along with ensuring that the ballot images of the scanned paper ballots be made immediately accessible to the public.

Government is owned by the people: we support it with our tax dollars, we choose it through our elections. Government only exists by the "just powers from the consent of the governed." In return we are entitled to expect that our government will be responsible for the stewardship of our elections and secure our inalienable and civil rights. Only the people can secure the election of their government through an

observable, transparent, open process which is designed to permit them the greatest scrutiny over the process which selects their public servants. The ability to oversee that the outcome of elections represents the will of the people cannot be delegated to the government nor to private entities. It must remain with the people if they are to retain control over those public servants.

New Yorkers are entitled to a voting system which ensures this oversight and integrity. We have the ability to provide that voting system in time for the next election, but only if the State recognizes that the path it is on will never lead to such an outcome. The People are entitled to hand count their votes and not be told such a method is backwards or inconvenient or not favored by appointed or elected officials. Democracy does not exist for the convenience or favor of public officials. Democratic elections must be controlled by and accountable to the citizens if government is to have any legitimacy.

ENDNOTES

1. The Executive Summary of the California report, Accessibility Review Report for California Top-to-Bottom Voting Systems Review: http://www.sos.ca.gov/elections/voting_systems/ttbr/accessibility_review_report_california_ttb_absolute_final_version16.pdf

2.http://voter.engr.uconn.edu/voter/OS-TSX-Report_files/TSX_Voting_Terminal_Report.pdf

3. http://election.dos.state.fl.us/pdf/SAITreport.pdf

4. http://www.hd.net/drr227.html

5. ES&S failed to submit the source coding requested by the SOS and hence was not tested along with the other machines used in California. All ES&S voting equipment was decertified for use in California. See http://www.bradblog.com/?p=4985#more-4985

6. See John Gideon's post at BradBlog, http://www.bradblog.com/?p=4890, quoting from the California Reports:

> *Three voting systems, the Diebold AccuVote TSx, Hart eSlate and Sequoia Edge I and II, were evaluated for usability and accessibility for voters with disabilities and voters with alternate language needs, using both heuristic and user testing techniques. Although each of the tested voting systems included some accessibility accommodations, none met the accessibility requirements of current law and none performed satisfactorily in test voting by persons with a range of disabilities and alternate language needs. In some cases the accessibility or usability deficits could be partially or wholly mitigated. Some of these mitigations would not require new federal and state certification testing.*

7. TechNewsWorld at http://www.technewsworld.com/story/58572.html

8.http://www.betanews.com/article/Three_EVoting_Systems_Susceptible_to_Attack_California_Team_Finds/1185822412

9. McKinney's Election Law sec. 7-202 1 (r)

10. See endnote 1 and http://www.sos.ca.gov/elections/elections_vsr.htm for full reports.

11. http://www.sos.ca.gov/elections/voting_systems/ttbr/Hart-source-public.pdf

12. http://voter.engr.uconn.edu/voter/OS-TSX-Report_files/TSX_Voting_Terminal_Report.pdf

13. http://www.bradblog.com/?p=4902.

14. The U Conn report also mentions how to suppress the display of a given candidate (from the article referenced at endnote 13):

> This exploit manipulates the ballot definition and nothing else. The successful exploits in the UCONN report take advantage of the fact that the ballot definition is split between the election database and the display portion stored the .XTR files, but without corresponding mechanisms to maintain referential integrity between the two halves of the ballot definition. The election database portion of the ballot definition controls how votes accrue to candidates based on the ballot line. The display portion of the ballot definition controls how names are printed on the screen and VVPAT record based on the ballot line. Both exploits introduce a referential integrity break between these two halves of the ballot definition.
>
> In the example above, the election database has Pocahontas and Smith on ballot lines 5 and 20; respectively. By swapping the .XTR files, the display portion of the ballot definition has Pocahontas on ballot line 20 and Smith on ballot lines 5. Thus, a screen touch to ballot line 5 accrues a vote to the candidate assigned to ballot line 5. According the election database portion of the ballot definition, this is Pocahontas. The screen and VVPAT print the name associated with ballot line 5. According the display portion of the ballot definition (the .XTR files) this is Smith. Thus, both the screen and VVPAT say Smith, but the vote on the invisible electronic ballot actually accrues to Pocahontas.

15.http://www.nj.com/news/ledger/jersey/index.ssf?/base/news-7/118499337617870.xml&coll=1

16.http://www.allamericanpatriots.com/48728252_new_jersey_nj_attorney_general_denies_certification_voter_verified_paper_record_systems_ele

17. New York is presently scheduled to test DREs from Liberty, Avante and Sequoia.

18.http://www.sequoiavote.com/bAVCEdge.php:

19.

DID CRIMES OCCUR?
VOTER ACTION CALLS FOR A FULL CONGRESSIONAL INVESTIGATION OF VOTING SYSTEMS COMPANIES

Public Call Issued Following New Evidence Revealed by Dan Rather Reports – "The Trouble with Touch Screens"
Group Says Voting Systems Companies May Have Engaged in Commercial Fraud

Voter Action today released the following statement calling for a full congressional investigation into the new evidence revealed by Dan Rather Reports – "The Trouble with Touch Screens", which aired last night on HDnet and can now be accessed via this link: www.voteraction.org

Last night's broadcast by Dan Rather Reports of "The Trouble with Touch Screens" raises serious questions as to whether US voting systems companies have engaged in commercial fraud by knowingly marketing defective products to jurisdictions throughout the country. It also serves as a wake-up call to the nation of the dangers associated with the outsourcing of key election functions to private vendors. Voter Action today calls on the United States Congress to launch a full investigation into the increasing influence and control that private companies wage in the way we conduct our elections and to determine whether certain US voting systems companies have committed crimes under federal and state anti-fraud statutes which should be referred to the appropriate authorities for prosecution.

This investigation should include a focus on the following revelations emerging from "The Trouble with Touch Screens":

• The report quotes an employee of a contractor for the ES&S voting machine company who was sent to overhaul operations at a factory in the Philippines as saying that 15,000 or more potentially defective voting machines were shipped from that factory to the United States. Did the ES&S voting machine company knowingly market defective voting machines to jurisdictions throughout the United States? Did the company's subcontractors knowingly market defective parts in the manufacturing of these machines? Have any of the other voting machine manufacturers or their subcontractors knowingly marketed defective products for conducting our elections?
• The report cites the 2006 election for Florida's 13th congressional district as an example of the problems with electronic voting machines. Where did the potentially defective voting machines assembled at a Manila factory get used and in which elecions? Are there previously unknown discrepancies in those election outcomes?
Are those machines still in use?
• The report cites seven former employees of Sequoia, the company that made punch card ballots used in the 2000 election in Florida, as saying that in 2000, the company began printing ballots on cheaper and possibly defective paper. Did the Sequoia company knowingly market defective paper for the printing of ballots in the 2000 election in Florida? Have any of the other voting systems companies knowingly marketed defective paper for the printing of ballots and, if so, in which other US elections have voters cast their votes on such ballots?
• The report demonstrates that election officials in this country increasingly rely on private vendors to carry out key functions of our democracy – from the printing of ballots to the counting and recording of our votes. This outsourcing extends to other critical aspects of the way we conduct our elections, including the maintenance of voter registration databases, the use of electronic poll books, and the means by which we recount and audit our elections. What is the relationship between election officials and vendors? How prevalent is the pattern of election officials becoming employees

of the private vendors after leaving their public positions or becoming otherwise compromised? What standards, if any, are in place in the nation to avoid actual conflicts or the appearance of conflicts between the public and private interests at stake in this arena?

The American public deserves answers to these questions and others emerging from this report. Congress should get to the bottom of this and should determine whether any private voting systems companies have committed commercial fraud in the marketing of their products to election officials around the country. Further, it should fully investigate the threat to our democracy posed by the outsourcing of key election functions to private companies, and it should take all necessary measures to reclaim our elections for the public domain.

20. See http://www.democracyfornewhampshire.com/node/view/4469

21. http://election.dos.state.fl.us/pdf/SAITreport.pdf

22. http://www.ajc.com/search/content/news/stories/2007/08/01/voting.html

23. http://www.bradblog.com/?p=4900&print=1

24.*Election Unit Spins off from Corporate Parent, Becomes 'Premier Election Solutions' After Failure to Find Buyer for Failing Unit!*

Diebold Elections Systems, Inc. is no more. At least in name.

After a year and a half of conversely trying to dump their failed voting unit and/or lying to customers about the reliability and security of their voting systems, corporate parent Diebold is giving up the ghost of their election business which, according to an analyst in a Reuters report, was "responsible for less than 10 percent of Diebold's revenue, and 100 percent of its bad publicity.

According to a company statement just released, Diebold Elections Systems, Inc. will become Premier Election Solutions as of today. The company president, David Byrd, who has overseen the disastrous election unit for some time, will stay on as President to go down with the ship, apparently.

After a string of disastrous reports on the quality and security of their voting systems, along with plummeting stock prices since last week, it seems clear that Diebold, the once-great, more-than-100-year old company, is doing whatever they can at this point to save the corporate parent. While their stock price (DBD) plummeted at today's opening bell, and is currently down some 5.6% from yesterday, the price has begun to rise again in the last hour or so on news of the sale.

More than anything, however, the move may well be a harbinger of a coming declaration of bankruptcy for Diebold/Premier as we see it. With the unit now spun off from the blue chip Diebold parent, declaring bankruptcy or dissolving the company all together would be less trouble for investors and the main company as a whole... see http://www.bradblog.com/?p=4962

25. **Insider Trading at Diebold?** *Mass Sell-Off by Company Officers Occurs Simultaneously Just Days Prior to Stock Price Plunge, Announcement of Jettisoning of Election Division,* http://www.bradblog.com/?p=4972

26.http://www.bradblog.com/?p=4973

27.http://www.bradblog.com/?p=4970

28. http://www.davickservices.com/KY_AG_voting_mach_lawsuit_.htm