Memo I: To The Honorable Eliot Spitzer, The State Board of Elections, New York State Legislature
From: Andrea Novick , Esq.
Date: July 24, 2007
Re: The voting vendors scheduled for certification testing are ineligible to contract with New York State

New York State Law Prohibits the State from Entering into Contracts with Any of the Vendors Presently under Consideration

New York State is about to start testing the products of vendors who by any reasonable application of the State Finance Law (SFL) and New York State Comptroller's Procurement and Disbursement Guidelines (Vendex rules) should be barred from doing business in New York. I have included below a partial documentation of the available evidence revealing the myriad of ways in which the vendors fail to meet the criteria for responsible contractors.[1] The State is responsible for affirmatively requiring all necessary disclosure to satisfy itself of the sufficiency of a vendor's responsibility. To assist in this effort, I have prepared this memo.

The Vendex rules[1] require that state agencies award contracts only to "responsible" vendors. These rules are intended to ensure that public dollars are being spent appropriately. Not only should contracts be awarded based on the lowest price or best value, but New York State is enjoined from doing business with vendors who lack business integrity or whose past performance is wanting. Under the criteria imposed by the SFL and Vendex rules, none of the voting machine vendors New York is presently considering doing business with are eligible for contracts.

Pursuant to the Vendex rules, the first set of factors a state agency must examine involve the vendor's integrity. Integrity involves, *inter alia,* a consideration of the ethical

[1] Simultaneously with my preparation of this memo, Voters Unite issued a similar indictment of the voting system companies New York is preparing to do business with entitled, *Voting System Companies Fail to Meet New York State's Requirements for "Responsible Contractors"*, http://www.votersunite.org/info/IrresponsibleVendors.pdf . The documentation contained in the Voters Unite report in some instances overlaps with the documentation contained herein and in some instances adds even more damning evidence of the voting vendors' ineligibility to do business in New York. Voters everywhere owe Voters Unite a debt of gratitude for the invaluable resource they have provided in documenting the atrocities which have been American elections under the Orwellian Help America Vote Act (HAVA).

violations of the vendor. Governor Spitzer has called on state government to maintain the highest ethical standards because he recognizes how critical this is to an accountable government. So paramount are ethical considerations that the Governor has taken this issue under his wing. At a press conference earlier this year Governor Spitzer was asked why he felt that the executive should have control over the new State Commission on Public Integrity (now known as the Ethics and Lobbying commissions). The Governor responded:

> *Because I believe that the governor - and I was elected for this purpose - is uniquely accountable for the ethics and the function of the state agencies, the state authorities…I expect to be held accountable, and I want to be held accountable.*
> .....
> *In one bold action, lawmakers have set New York on a path toward true integrity in government.*

The ethical violations are highlighted both because Governor Spitzer has placed this issue first and foremost in his administration and because the contracts being considered are for nothing less than the running of our democratic elections. Ethical violations are but one of the factors New York State must consider in determining whether a vendor is eligible to do business in New York. Other factors which look at the vendor's integrity to perform the contract include criminal indictments and convictions, civil fines, formal complaints and investigations, as well as consideration of past performance. All of the vendors are guilty of multiple infractions of any notion of responsibility.

While I recognize that the SBOE could conclude that a more thorough investigation of the vendors is premature at this time, given that no systems have been certified, I would urge the consideration of the available evidence now. It would be wasteful of time and resources as well as taxpayers' money to engage in certification testing only to then recognize that none of the conventional vendors satisfy New York's standards. Since sufficient information is publicly available to conclude now that these vendors are ineligible to do business in New York, I expect that the State would act accordingly and take appropriate action to protect citizens' legal rights.

Voting Vendors Should be Held to a Higher Standard

I would also submit that when considering an award of a contract to a voting machine vendor, the scrutiny of these factors must be even higher. After all, these voting machines

vendors are responsible for the proper functioning of their systems to be used in our democratic elections.

We expect to hold our public servants to the highest possible standards. If the State is to consider permitting private vendors into our elections, we should expect no less of those who would control the process which leads to the selection of our public servants. As we have seen across the country, these vendors are in a position to influence the process by which we elect our representatives. To hold them any less accountable than we hold our public officials is to make a mockery of our government and insults the public will.

As is aptly described in the Historical and Statutory Notes of the Code of Ethics contained in the Public Officers Law, McKinney's Public Officers Law, Section 74:

> *"Declaration of intent. A continuing problem of a free government is the maintenance among its public servants of moral and ethical standards which are worthy and warrant the confidence of the people.* ***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.***" (emphasis supplied)

The scrutiny we bring to bear upon prospective voting vendors should be at least as high as the standards we apply to our public officials, to wit, "moral and ethical standards which are worthy and warrant the confidence of the people"; "standards above the morals of the market place". Accordingly the standards for contracting with voting vendors should be *even higher* than those set forth in the SFL and Vendex rules.

Contracting with These Vendors Would Be a Violation of New York's Laws Applying Any of the Relevant Criteria

Even applying the less stringent, standard criteria imposed by the SFL and Vendex rules, all of the voting machine vendors New York is presently considering doing business with fail to meet the responsibility requirements.

Notwithstanding the vendors's ineligibility to do business in New York, the New York State Board of Elections (SBOE) is poised to commence certification testing of these vendors' voting machines. This testing will cost millions of taxpayers' dollars.

These vendors have exhibited grievous examples of unethical, irresponsible behavior, some with criminal histories. Four of the five vendors have demonstrated shoddy performance records and inferior products; the newest vendor to enter the field lacks a track record for performance, but has already exhibited an arrogant lack of integrity in trying to evade NYS laws. Most significant among the disqualifying criteria shared by these vendors are the critically serious security flaws of their voting machines which New York is nonetheless considering entrusting our sacred ballots to.

As detailed below, the voting machines offered by these vendors have shown themselves to be susceptible to hacking and other security vulnerabilities which deprive citizens of their constitutionally protected franchise; a right which includes not merely the act of casting a vote, but the assurance that the vote is accurately counted.

None of the voting vendors seeking our business even approach the standards of the marketplace, much less the higher standards we should be demanding. Indeed, because of the inherent conflict between the private interests of the vendors and the official duties of electoral administration, I would submit that private vendors have no place in the people's elections.

New York State Owes a Duty to its Citizens to Safeguard Our Constitutionally Protected Franchise

The State holds the ultimate responsibility for protecting our constitutional right to vote and to have our vote counted as cast. The Court of Appeals has held:

> *The right of an elector to vote is conferred by the Constitution.....**[the elector] is entitled to see that his vote has been given full force and effect.***
> ***....any method of holding an election which would deprive the electors..... of the right of casting their ballots and having effect given to the votes so cast would plainly be unconstitutional.*** (emphasis supplied)
>
> *Deister v Wintermute*, 194 NY 99, 108

New York State must be able to exercise full control over the electoral process which the public must be able to observe and scrutinize in order to hold its government accountable. Computerized voting systems conceal that which must be transparent. When counting the votes consists of running proprietary software to process that data, the voter who is "entitled to see that his vote has been given full force and effect" can no longer observe

the process (quoting *Deister v Wintermute*, *supra*). Public transparency, oversight and accountability are thus rendered impossible.

The State owes a duty to its citizens to run democratic elections in an open and trustworthy manner. This duty cannot be delegated to private corporations. Private corporations are not accountable to the public. The voting vendors New York is considering awarding contracts to have all asserted proprietary rights to the very information citizens are entitled to know about how their elections are being run and their votes counted. Once the State permits privately controlled computers into our election process it can no longer fulfill its fundamental obligation to the people to provide a safe and secure means of protecting the integrity of the ballot.

Even if such delegation was permissible, the lack of integrity and failed past performance of the vendors seeking our business should bar their entry to New York's electoral process. These vendors' products have had an unacceptably high rate of breakdowns and failures that the vendors have tired to conceal.

Reports by citizens and voting precincts across the nation have been documented, but due to lack of cooperation by vendors, such reports represent the tip of the iceberg. Vendors cite their trade secret and intellectual property contractual restrictions on disclosure of technical information about their products hoping to prevent investigation of their systems' defects. Hiding behind these claimed proprietary rights, vendors have concealed the very information citizens and election official are entitled to. In addition, vendors have used intimidating, bullying responses to citizens' efforts to document security flaws in their voting systems. Vendors have gone so far as to take legal actions to prevent exposure of the flaws in their systems. Such arrogant and intentionally threatening behavior is deeply disturbing and serves to compound these vendors' lack of integrity and ineligibility to do business in NYS.

The requirements articulated in the Vendex rules and SFL, include the "**integrity to perform the contract**," which expressly includes such considerations of responsibility as a vendor's "criminal indictments, criminal convictions, civil fines and injunctions imposed by governmental agencies, anti-trust investigations, [and] ethical violations". They also include the vendor's **past performance** [2], which would include consideration in this instance of how these voting machines functioned during elections, timely delivery of necessary services and products by the vendor and most importantly, the reliability and security performance of these machines. In all of these criteria the vendors have failed miserably. Below is the documented evidence.

1) Election Systems and Software (ES&S)

Lack of Integrity to Perform the Contract

ES&S's current ethical violations, violations of state laws and civil fines and injunctions, as documented below, are significant enough to demonstrate the company's ineligibility to do business in New York. It is inconceivable that this state, particularly under this Governor, would choose to do business with ES&S given the repeated complaints across the nation of abusive and irresponsible business practices. These include repeated acts of lying to and threatening of state officials. Some background history of how ES&S came into existence sheds light on who this company that New York is nonetheless proposing to do business with, really is. The companies which have been merged into what is now ES&S reflect the very abuses Governor Spitzer targeted as Attorney General.

A short history of the mergers, acquisitions, dubious investors and conflicts of interest which came to be what is now, ES&S

Todd and Bob Urosevich founded ES&S's seminal corporation, Data Mark, in the early 1980s, after obtaining financing from the far-Right Ahmanson family, with documented family ties to the Christian Reconstructionist movement (which had the stated goal of taking control of the American government). The Ahmanson family purchased a 68% ownership interest and the company's name was changed to American Information Systems (AIS). In 1987 the Amhansons sold their shares in AIS to Omaha World-Herald (45%) and the McCarthy Group (35%)[3] .

In providing a brief history of how ES&S came into existence, I have highlighted those factors articulated in the Vendex rules as relevant to the State's consideration.

Omaha World-Herald was owned by Peter Kiewit, the head of Peter Kiewit Sons' Inc. Peter Kiewit Sons' Inc. and its subsidiaries have been involved with a string of **bid-rigging cases in 11 states and 2 countries:**
– In an **antitrust case that involved charges of bid-rigging** in New Orleans, Kiewit pleaded no contest and paid **$100,000 in fines and $300,000 in a civil settlement**.
– In South Dakota, a Kiewit subsidiary **pleaded guilty to bid-rigging on road contracts** and **paid a fine of $350,000.**

– In Kansas, a Kiewit subsidiary was **found guilty of bid-rigging and mail fraud** on a federal highway project. The firm was **fined $900,000 and a company official was sentenced to a year in jail.**
– In Nebraska, a Kiewit subsidiary **paid $1.8 million for bid-rigging on a state highway project and a Kiewit vice president was jailed.**

When the **state of Oklahoma forbade Kiewit to bid on any projects, Kiewit set up a different company and lied in a sworn affidavit to the transportation department saying it had no parent company, affiliate firms or subsidiaries. When Oklahoma found out, it pulled all of Kiewit's contracts.** Continuing in its deceitful practices, Peter Kiewit & Sons took contracts in Washington State under the guise of a minority-owned firm. **Kiewit paid more than $700,000 in fines**.

In 1997 AIS acquired election-industries giant Business Records Corp (BRC), formerly a Texas-based election company and embarked on an acquisitions blitz to corner the elections industry. Upon purchasing BRC, AIS changed its name to Elections Systems and Software (ES&S). The **SEC objected to the merger of BRC and AIS on antitrust grounds**, but for unstated reasons the SEC withdrew its objection after an arrangement was made in which the assets of BRC were shared between ES&S and Sequoia, the third largest voting machine vendor.

Just about the same time that AIS bought BRC to become ES&S, Bob Urosevich, one of the two founding brothers of what is now ES&S, moved to Global Election Systems (which subsequently became Diebold Elections Systems).

In July 1992, Chuck Hagel, who valued his investment in the McCarthy Group at up to $5 million, became chairman and CEO of AIS (now ES&S). **While Hagel was running AIS, the company was building and programming the machines that would later count the votes in his 1996 senatorial race.** Hagel stepped down as chairman in late March 1995 and a few days later announced his bid for the US Senate. In public documents, **Hagel lied about his ownership in ES&S, failing to disclose his relationship and his obvious conflict of interest**.

In 1996 the Washington Post said Hagel's "Senate victory against an incumbent Democratic governor was the major Republican upset in the November election". Hagel was the first Republican to win a Senate seat in Nebraska in a quarter of a century. He won virtually every demographic group, including many largely Black communities and Native American communities that had never before voted Republican.

In 2002 Hagel ran for re-election against Democratic challenger Charlie Matulka and won in a landslide. His website said he "was reelected to his second term in the United States Senate ...with 83% of the vote. That represents the biggest political victory in the history of Nebraska." The website failed to mention that about 80% of those votes that put him in office were counted by computer-controlled voting machines, built and programmed by his company.

Matulka had written to the Senate Ethics Committee in 2002, requesting an investigation into Hagel's ownership and nondisclosure of ES&S. His complaint was dismissed. **The Washington publication, the Hill, confirmed that Hagel was the head of and continues to own part interest in the company that owns the company that installed, programmed and largely ran the voting machines that were used by most of the citizens of Nebraska.**

After the election, Matulka asked for a recount. His request was denied by the Nebraska Secretary of State because Nebraska had just passed a law that prohibits government-employee election workers from looking at the ballots (Nebraska uses optical scan systems manufactured by ES&S). "They can take over our country without firing a shot," Matulka said, "just by taking over our election systems". Matulka later told the NY Times, "This is the stealing of our democracy".

Hagel still owns stock in McCarthy & Co., which still owns a quarter of ES&S.
.....

This history of how ES&S came into existence should be sufficient to preclude an ethical entity, like New York State, from contracting with this vendor. It reflects on the company's current lack of ethics.

In February, 2002, Arkansas' Secretary of State (SOS) plead guilty to accepting bribes and kickbacks from BRC, now merged with ES&S. When confronted, an ES&S spokesperson sought to deflect responsibility, claiming the bribe was unconnected to ES&S. When asked about BRC company executive Tom Eschberger, who was involved in the kickback scheme but granted immunity for his cooperation, the ES&S spokesperson misleadingly claimed Eschberger wasn't involved with ES&S. In fact Eschberger went to work for ES&S after the merger with BRC. At the point ES&S misrepresented that Eschberger no longer worked for ES&S, a Pittsburgh television station investigation team revealed that Eschberger was still employed by ES&S as an independent contractor. (See footnote 1, p 8)

If the above information and documentation isn't cause enough, New York, under the broader category of "business integrity", must also consider ES&S's performance failures and the company's actions to prevent investigation of security breaches. ES&S's performance failures include machine breakdowns, inability to timely fulfill contracts and security breaches. ES&S has responded with arrogant, threatening actions to prevent efforts to independently examine security flaws in their systems or to reveal the flaws to all jurisdictions using the equipment. As a result of ES&S's success in preventing jurisdictions using their equipment from knowing about the problems experienced by others with the same equipment, their equipment has caused repeated similar election irregularities in multiple jurisdictions.

Lack of Integrity to Perform the Contract: ES&S's Irresponsible Efforts to Cover Up, Intimidate and Suppress Exposure of Failed Performance and Security Flaws

From the beginning ES&S has had the reverse Midas touch. When their machines failed in Hawaii in 1998 **ES&S had to pay over half a million dollars to settle contract disputes** and recount ballots. Simultaneously in Dallas, bugs in ES&S equipment lost one our of every eight votes. In 2000, **flaws in ES&S tabulating equipment caused Venezuela to postpone "the biggest election in Venezuela history**." ES&S kept selling equipment and kept losing votes --flipping screens in Arkansas, counting more votes than voters in San Francisco, giving votes to the wrong candidate in Florida, Kansas and Texas. And through it all ES&S has refused to acknowledge responsibility, choosing instead to blame others or cover up the revelations or make sure other flaws are never discovered.[4]

A 2003 **report released by the Miami-Dade Inspector General[5] revealed that it was ES&S that had mislead county officials "about the equipment and delivered goods that were "hardly state-of-the-art technology**," according to the Miami Herald, which obtained a copy of the inspector general's report [6]. Moreover, the report found that ES&S told county officials that its electronic voting machines would provide voters with a system that could run a trilingual ballot and would not require additional data capacity, even while the company's own documentation from 2001 indicated this to be a **misrepresentation.**

In Texas, 2004, William Singer, an election programmer in Tarrant County, wrote the secretary of state's office after the 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," Singer wrote, "was far beyond the kind of practices that I believe should be standard and accepted in the election industry."

Preparing for elections in 2006, Texas director of elections Ann McGeehan called the situation "**completely unacceptable and disturbing**," and authorized local officials to create "emergency paper ballots" as a backup. Referring to **ES&S's poor performance** she stated:

> ***We regret the unacceptable position that many political subdivisions are in due to poor performance by their contracted vendor***. (See endnote 15)

In March, 2004, the Indiana Election Commission discovered ES&S had installed uncertified firmware in some of their voting machines. When forced to reinstall the certified version, it didn't tabulate the votes correctly. An exasperated member of the election commission said, "**I just think I was absolutely lied to by your CEO ... I sat in this room and you all lied to me. You're so derelict in your duties ..."**. In response to the unethical behavior of ES&S the state legislature passed a law providing strict penalties on voting machine vendors who act on their own initiative without the permission of the state and install or change a voting system without state election commission approval. (footnote 1, p 7)

In 2005 ES&S once again installed uncertified software in the voting system of another Indiana county. **Indiana sued ES&S alleging ES&S lied** about swapping out the uncertified software. The **lawsuit was settled by ES&S paying $1.2 million**.

In 2006 **Indiana filed a formal complaint against ES&S** for failing to provide working equipment and ballots in several counties in time for an election and providing defective voting equipment, software and services.

In the 2006 race in Florida's 13th Congressional District, ES&S voting machines' "official tally" indicated that **18,000 Sarasotans showed up to vote**, voted for the governorship and other races, but decided not to cast any vote for a candidate to the House of Representatives, an undervote rate far higher than the undervote rate in other districts. The anomaly resulted in a **so-called independent audit**. **ES&S sent a letter to the state of Florida dictating the terms of the audit, including how the review of their source code should be restricted and what the audit of their own voting systems should and shouldn't be allowed to reveal[7].** A review of ES&S's letter, which is excerpted at endnote 7, reveals the extent of the information ES&S was trying to hide.

After the November 2006 elections in Texas, when it was discovered **ES&S's machines were counting the votes in triplicate** – which was only revealed because election officials were wondering why there were more votes than voters – **ES&S refused to accept responsibility for the problem**, blaming human error, not its machines that should be designed to never permit such an error, human or otherwise, to occur.[8]

In March of 2007, California's SOS decided that anyone providing electronic voting machines in their state had to withstand testing from independent security experts. Among the vendors**, ES&S was the only one to resist turning over their source code as required by the SOS** and just recently might have relented. ES&S waited until at least three months past the due date set by the SOS's office as part of its review and then in an **arrogant letter threatened, "ES&S will hold not only the examiners responsible, but the SOS as well, for any prohibited disclosure or use of ES&S' trade secrets and related confidential proprietary information.**" ES&S clearly does not want its source code examined and it appears ES&S may have violated California's Law. The menacing letter then ends with a threat that if any need for changes is found, Los Angeles County will have to pay for those changes.[9]

ES&S's Past Performance Failures

A Partial List of ES&S's Documented Failures: [10]

The 51 page partial list of ES&S's machine failures was compiled by VotersUnite.org in order to document the breakdowns and other problems with the vendors' voting machines. In order to assist NYS's inquiry I went through this material to identify those incidences of failures relating to the Unity models since those are the machines New York is slated to begin testing. The specific incidences of ES&S's Unity model failures is found at the endnote herein[11]. It is important for the state to review the entire list, however, because the history of repeated breakdowns and security failures even as the vendor "improves" or changes its models, renders all models and their problems relevant to evaluation of the vendor's responsibility.

In addition to the long list of failures in VotersUnite.org's partial list cited above, I have included a few examples of what New York might expect should it voluntarily choose to give up control of its elections and become dependent on an outside voting contractor that

can't meet its contract obligations. The news articles supporting these incidents are all reported at www.Votersunite.org.

In March 2006, North Carolina, **ES&S's delivery of machine parts was so late it delayed poll worker training** for May 2 Elections. Key missing components include, memory chips for tabulators, AutoMARK voting-assistance machines, and voting booths.

In April 2006, Arkansas, the Election Commission held an emergency meeting to discuss anticipated problems with **ES&S new voting machines because delivery dates had not been met.**

In June, 2006 Arkansas, the run-off election which subsequently ensued was described by an Arkansas County Clerk as "a royal mess."

> "Our PEB's that were received were wrong. We have no absentee ballots. We can send ballots like we are using for early voting, but **ES&S was supposed to have paper ballots to us by Friday and no ballots have been received. It is definitely a mess**."
>
> "**ES&S has now proven in four states that they are unable to meet deadlines** for the delivery of programming, regardless of the time period they have to do the work," [White County Election Commissioner John] Nunnally wrote to Janet Harris in the Secretary of State's office. "ES&S even had the gall to show up Friday and tell me they had already done all the testing on my PEB's 'to save me time,'" Nunnally wrote. "That's a violation of the law, and besides that, **on what grounds would I trust their testing**?"
>
> "**ES&S is set up to box us into [sic] using their proprietary services for election preparation,**" Nunnally wrote. "They are doing this in every state they sell. **They don't have the resources to meet the needs for these services and that is a verifiable fact at this point.** This cannot continue."
>
> "November is going to be a massive train wreck," Nunnally wrote **"Getting a bunch of lawyers together to come up with financial 'damages' settlement won't fix anything."**
>
> "Do you think ES&S keeps enough well trained people on their staff to program nationwide, general elections every month? Of course not!" Nunnally wrote. **"So who is going to be doing the programming in October for the general elections?** Either there are going to be far too few trained people to get the job done, or we are going to have our most critical election programmed by StaffMark, Kelly Girl, and illegal aliens."
>
> "**Would someone please find out the password to the ES&S software that keeps me from producing my own ballots and send that to me?"** Nunnally wrote**. "I can't do any harm trying to produce my own, right or wrong. Wrong is all I've gotten from ES&S so far**, **so there's a chance I just might do better**. It was pretty infuriating to

spend two hours learning how to build a database only to find out that I had been password locked out of any attempt to produce a ballot. That just poured fuel on my fire."

emphasis supplied, see endnote10, Voters Unite list at p 49

In May, 2006, West Virginia, **ES&S failed to meet its deadline for delivering "programmable ballots" needed to administer the election in all 55 counties in West Virginia.** As a result of ES&S's failure to "meet required delivery of performance schedules"[12] 6 of the 55 counties weren't able to use the machines they'd purchased because there was no time to test them[13]. The chief of staff for the SOS said "It created an undue stress and anxiety on the clerks and county elections officials throughout the state...this was the toughest election to prepare for in many years...due to the fact that most counties were not able to adequately prepare and familiarize themselves with the new equipment used in the primary election." The Secretary of State accused ES&S of "vast delays" and "broken promises". West Virginia's Secretary of State filed a formal complaint with the Election Assistance Commission regarding **ES&S's delays in programming ballots that left the state unable to properly prepare for its primary election.**

In April, 2006, **Oregon, Secretary of State Bradbury sued ES&S for breach of contract for failure to deliver the voting machines** for the disabled. **ES&S had agreed to all of the standard state contract terms, but subsequently informed the Secretary of State that it would not agree to the terms of the contract, and would not deliver the voting machines unless the Secretary changed the terms of the contract**. Bradbury refused to alter the contract to meet ES&S's demands, which led to the lawsuit. Bradbury said:

> ***We will not leave our elections in the hands of companies that do not follow through on their obligations, and we will not be coerced into altering our contracts.***

Of all ES&S's failings, the most serious performance failures are always the security flaws in the voting system. While these are listed under failed performance failures in that they are included in the 51 page partial list of ES&S failures at endnote 10, they deserve heightened attention. Some of those security breaches are included as examples of ES&S's lack of integrity to perform the contract because ES&S' responses to the exposure of these flaws reveals that lack of integrity further. Below I have included a single security report because it relates specifically to the ES&S Unity model New York is scheduled to test.

As the security report reveals, not only is ES&S's equipment far too vulnerable for New York to consider using, but ES&S seems satisfied with their faulty product and not inclined to remedy the myriad of problems.

Past Performance Failures: Security Flaws in ES&S's Voting Systems

New York is slated to test ES&S's Unity 3.0.1 Opscan. As detailed at endnote 11, **ES&S's Unity software has caused the mistabulating of votes in numerous states. The software is responsible for causing optical scanners to malfunction, losing votes, subtracting votes from the total by counting backwards, double counting ballots. As the security report discussed below reveals, Unity software has been shown to be easily modified because Unity relies on Microsoft Windows. As the report states, it is possible to manipulate the vote tally without detection.**

Nonetheless New York is slated to begin testing this Opscan. A recent security report prepared for the state of Massachusetts by a recognized supporter of electronic voting, Dr. Michael Shamos, examined the various options for disabled voters in a state that uses optical scanners. While the review did not focus on the ES&S Opscan, it did focus on the same Unity model software.

Included below and at the endnote are some relevant excerpts from the security report regarding Unity's security vulnerabilities. [14] Unity 3.0.1 is a suite of Windows XP programs used to set up, manage and tally an election. ES&S's Unity software, as revealed in this report, can compromise an entire election. ES&S's decision to continue to use Microsoft contributes to this unacceptable security exposure. The fact that Dr. Shamos passes the system with caveats cannot be good enough for New York.

> *Because **Unity is a Windows application**, it is difficult to maintain it and its data in a secure manner.*
>
> ***A continuing problem with Unity, which ES&S has not shown any inclination to correct, is that it offers a plethora of ballot setup options which even the vendor's representatives are unable to explain. If a jurisdiction uses Unity on its own, the possibility of setting up an illegal election is significant.** The vendor counters that these operations are generally performed by experts who know what they are doing, but no such person has appeared at any examination I have conducted.*
>
> ***Unity's log files are unprotected and can be modified easily using Windows accessories.** In Notepad, for example, it was easy to change the login ID of a person performing an operation or delete a log entry entirely.*

In Unity it is possible to insert or alter unofficial vote totals manually. These operations are logged. However, it is possible to modify the logs to eliminate any trace of the modification, making it impossible to audit the election or explain irregularities.

Unity provides insufficient security for election and log files. They are too easy to modify outside Unity using Windows. (emphasis supplied)

2. Diebold Election Systems

Lack of Integrity to Perform the Contract

Below is the story of the felons who created what is now Diebold Elections Systems, with the relevant Vendex criteria bolded. As is detailed below, while the original founders are gone, mostly due to jail terms, the programmers they'd hired and managed are now key people in Diebold and some of them are convicted felons as well. Moreover, the pattern reflected in this early history continues.

As of March 31, 2006, there were ten outstanding lawsuits against Diebold charging Securities and Exchange Commission (SEC) violations. The Voters Unite report referenced at footnote 1, describes a **securities fraud class action suit filed against Diebold in December, 2005 on behalf of investors who allege a fraudulent scheme** by Diebold and its executives to deceive shareholders. **The SEC is formally investigating**. (Supporting references regarding the lawsuits and the SEC investigation are provided at the Voters Unite report, footnote 1, at p 3).

Particularly in light of the high ethical standards set by the Governor's Ethics Reform Act, New York should not be contemplating entering into any contract with Diebold.

Early Founders and High-Level Employees - Convicted Felons:

Diebold Election Systems (Diebold) was formed when in 2002 Diebold Inc. of Ohio acquired Global Election Systems, Inc. a Canadian Company. Global Election Systems (Global) was originally 'Macrotrends' at its founding in 1988. Macrotrends had a US subsidiary, North American Professional Technologies (NAPT), which became the manufacturing body of Global and later Diebold.

Founders:

Norton Cooper - who marketed for NAPT and Macrotrends had been **jailed for defrauding the Canadian government in 1974**. He also **served a year in jail in the mid-1980s for fraud against the Canada government; he was part of the collapse of the Vancouver stock exchange** and was ordered by decree not to pitch stock after 1992 or so because, in the words of Barron's and Forbes, he was a "hazard to avoid at the golf course".

Charles Hong Lee - a director of both NAPT and Macrotrends was Cooper's **partner pitching deals, stock schemes,** etc. Lee was **ordered to pay $555,380 in restitution** when he and Norton were sued. In 1994 Lee and another partner, Michael Graye, defrauded 43 Chinese immigrants out of $614,547 which fees were paid to a corporation controlled by Lee and Graye.

Michael K. Graye - When in 1991 NAPT and Macrotrends were reorganized and the name changed to Global Election Systems, Graye became a director. In 1996 Graye was **arrested on tax fraud and money laundering charges, but before he was sentenced in Canada he was indicted in the US on stock-fraud charges in another company he ran with Lee. He spent 4 years in prison. In April 2003 he admitted to the misappropriation of $18 million from 4 corporations and tax fraud back in the late 1980s. He was returned to prison.**

Key Personnel:

Jeffrey Dean – had been **convicted** in the early 1990s of **23 counts of computer-aided embezzlement** . **He was a computer consultant for a large Seattle law firm and defrauded them of about $450,000 in what US courts called a "sophisticated computer-aided scheme**". Dean was made a director of Global in 2000 and then made head of research and development with access to all components of the voting system.

According to the findings of fact in the criminal case against Dean, no. 89-1-04034-1:

"Defendant's thefts occurred over a 2 1/2 year period of time, **there were multiple incidents, more than the standard range can account for, the actual monetary loss was substantially greater than typical for the offense, the crimes and their cover-up involved a high degree of sophistication and planning in the use and alteration of records in the computerized accounting system** that defendant maintained for the victim, and the **defendant used his position of trust and fiduciary responsibility as a computer systems and accounting consultant for the victim to facilitate the**

commission of the offenses."

John Elder - is a **convicted cocaine trafficker** who met Dean in prison. By the late1990s Elder handled ballot printing for Global and went on to direct the punch card printing.

Global Election Systems was formally purchased by Diebold Inc. in January 2002 and at that time Jeffrey **Dean became a paid consultant to Diebold** while John Elder took over Diebold's national printing division. Six weeks later Diebold landed the biggest voting-machine order in history: The $54 million conversion of the entire state of Georgia to touch-screen voting on paperless DREs.

.....

If the extraordinary story of how Diebold came to be and remains, is not sufficient for New York to conclude that this is not the type of vendor that can be described as "responsible", I have included a partial list of failures of machine breakdowns, inability to timely fulfill contracts and security breaches under the subheading Deibold's Past Performance Failures. As was the case with ES&S, Diebold fares no better.

Equally disturbing are Diebold's inappropriate and vindictive actions to intimidate or otherwise gag anyone who attempts to expose the vast security flaws of Diebold's voting systems. These underhanded efforts reflect a further lack of integrity and therefore are included immediately below.

Lack of Integrity to Perform the Contract: Diebold's Irresponsible Efforts to Cover Up, Intimidate and Suppress Exposure of Failed Performance and Security Flaws

In the 2000 presidential election, the distracting issue of the hanging chad problem tended to conveniently overshadow the Diebold computerized voting system malfunction in Volusia County, Florida, that led several networks to incorrectly call the race for Bush. A Diebold optical scanner started subtracting more than 16,000 Gore votes. Rather than accepting responsibility for the Florida debacle Deibold blamed "a faulty memory chip". As described in one of Robert F. Kennedy Jr's exposes in Rolling Stone Magazine[15]:

Amid the furor over hanging chads and butterfly ballots in Florida, however, the "faulty

memory card" was all but forgotten. Instead of sharing culpability for the Florida catastrophe, voting-machine companies used their political clout to present their product as the solution. In October 2002, President Bush signed the Help America Vote Act, requiring states and counties to upgrade their voting systems with electronic machines and giving vast sums of money to state officials to distribute to the tightknit cabal of largely Republican vendors.

But according to recent e-mails obtained by Rolling Stone, ***Diebold not only failed to follow up on most of the recommendations, it worked to cover them up.*** *Michael Wertheimer, who led the RABA study, now serves as an assistant deputy director in the Office of the Director of National Intelligence.* ***"We made numerous recommendations that would have required Diebold to fix these issues," he writes in one e-mail, "but were rebuffed by the argument that the machines were physically protected and could not be altered by someone outside the established chain of custody."***

In another e-mail, Wertheimer says that ***Diebold and state officials worked to downplay his team's dim assessment. "We spent hours dealing with Diebold lobbyists and election officials who sought to minimize our impact," he recalls. "The results were risk-managed in favor of expediency and potential catastrophe."*** (emphasis supplied)

A cadre of **computer scientists showed how easily Diebold's machines could be hacked** and published those findings on various web sites in 2003. **Desperate to cover up this critical information, Diebold sent cease-and-desist letters** to more than two dozen programmers and students. Swarthmore College students responded to the attempts to abridge their first amendment rights and their efforts to reveal the threat to democracy with an "electronic civil disobedience" campaign: Diebold would shut down one site and the students would post to another.

While Diebold hid behind its proprietary rights to conceal vital information from the public, Diebold machines were installed throughout the country. As Kennedy described:

During the 2004 presidential election, with Diebold machines in place across the state, things began to go wrong from the very start. A month before the vote, an abandoned Diebold machine was discovered in a bar in Baltimore. "What's really worrisome," says Hood, "is that someone could get hold of all the technology - for manipulation - if they knew the inner workings of just one machine."

Election Day was a complete disaster. "Countless numbers of machines were down because of what appeared to be flaws in Diebold's system," *says Hood, who was part of a crew of roving technicians charged with making sure that the polls were up and running. "****Memory cards overloading, machines freezing up, poll workers afraid to turn them on or off for fear of losing votes."***

Then, after the polls closed, Diebold technicians who showed up to collect the memory

***cards containing the votes found that many were missing**. "The machines are gone," one janitor told Hood - picked up, apparently, by the vendor who had delivered them in the first place. **"There was major chaos because there were so many cards missing,"** Hood says. Even before the 2004 election, experts warned that electronic voting machines would undermine the integrity of the vote. **"The system we have for testing and certifying voting equipment in this country is not only broken but is virtually nonexistent," Michael Shamos, a distinguished professor of computer science at Carnegie Mellon University, testified before Congress** that June. "It must be re-created from scratch."*

*Two months later, the U.S. Computer Emergency Readiness Team - **a division of the Department of Homeland Security - issued a little-noticed "cyber-security bulletin**." The alert dealt specifically with a database that Diebold uses in tabulating votes. **"A vulnerability exists due to an undocumented backdoor account,"** the alert warned, citing the same kind of weakness identified by the RABA scientists. **The security flaw, it added, could allow "a malicious user [to] modify votes."***

Such warnings, however, didn't stop states across the country from installing electronic voting machines for the 2004 election. In Ohio, jammed and inoperable machines were reported throughout Toledo. In heavily Democratic areas of Youngstown, nearly 100 voters pushed "Kerry" and watched "Bush" light up. At least twenty machines had to be recalibrated in the middle of the voting process for flipping Kerry votes to Bush. Similar "vote hopping" was reported by voters in other states. (emphasis supplied)

Georgia was the first state in the country to conduct an election entirely with touch screen voting machines with the entire election run, not by the government, but by Diebold. With *no evidence left behind* on these paperless DREs, the "official" outcomes of Georgia's races were as impossible and improbable as Chuck Hagel's wins on the machines built by his company (now ES&S). From RFK Jr's article:

*It is impossible to know whether the machines were rigged to alter the election in Georgia: Diebold's machines provided no paper trail, making a recount impossible. But **the tally in Georgia that November surprised even the most seasoned political observers**. Six days before the vote, polls showed Sen. Max Cleland, a decorated war veteran and Democratic incumbent, leading his Republican opponent Saxby Chambliss - darling of the Christian Coalition - by five percentage points. In the governor's race, Democrat Roy Barnes was running a decisive eleven points ahead of Republican Sonny Perdue. But on Election Day, Chambliss won with fifty-three percent of the vote, and Perdue won with fifty-one percent.*

***Diebold insists that the patch was installed "with the approval and oversight of the state." But** after the election, the Georgia secretary of state's office submitted*

a "punch list" to Bob Urosevich of "issues and concerns related to the statewide voting system that we would like Diebold to address." One of the items referenced was" Application/Implication of '0808' Patch." The state was seeking confirmation that the patch did not require that the system "be recertified at national and state level" as well as "verifiable analysis of overall impact of patch to the voting system." In a separate letter, Secretary Cox asked Urosevich about ***Diebold's use of substitute memory cards and defective equipment as well as widespread problems that caused machines to freeze up and improperly record votes****. The state threatened to delay further payments to Diebold until "these punch list items will be corrected and completed."*

*Diebold's response has not been made public - but its machines remain in place for Georgia's election this fall. Hood says it was "****common knowledge" within the company that Diebold also illegally installed uncertified software in machines*** *used in the 2004 presidential primaries - a charge the company denies. Disturbed to see the promise of electronic machines subverted by private companies, Hood left the election consulting business and became a whistle-blower.* ***"What I saw," he says, "was basically a corporate takeover of our voting system."***

In December 2005, Ion Sancho, elections supervisor in Leon County, Florida, concerned about the security of the Diebold optical scanners, arranged for Harri Hursti, a computer programmer from Finland, to independently examine a Diebold Accuvote Optical Scanner. **Hursti hacked the machine** in the simplest way (considered a level one hack capable of being executed by an eighth grader) and exposed just how vulnerable the **Dieblod Scanner was – it was possible to subvert the memory card without detection.**[16]

Diebold, along with the other major vendors, reacted with a collective temper tantrum. Subsequently, when Ian Sancho was required to acquire machines for the disabled community, **Deibold refused to sell to Supervisor Sancho's county unless he promised not to have outsiders reveal the Diebold machine's flaws** through any more independent testing. Sequoia backed out of discussions with Mr. Sancho and ES&S didn't respond[17].

Diebold, as it has done consistently in refusing to accept responsibility for its system's serious security failures, attempted to minimize the damaging exposure as merely a "theoretical security vulnerability". In Diebold's letter trying to spin the damage it was alleged without support "the probability for exploiting this vulnerability to install unauthorized software that could affect an election is considered low". [18] A spokesperson for Diebold went on to lay blame anywhere but with Diebold: "For there to be a problem

here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software...I don't believe these evil elections people exist."

Diebold's self- serving and irresponsible statement stands in marked contrast to the Carter Baker Report[19]:

> *The greater threat to most systems comes nor from external hackers, but from insiders who have direct access to the machines. Software can be modified maliciously before being installed into individual voting machines.* ***There is no reason to trust insiders in the election industry any more than in other industries****.*

Subsequently, in **February 2006, California election officials arranged for experts to perform a similar analysis on Diebold machines and found** them to be vulnerable (see p 23 and endnote 28 herein). They found **an even wider variety of flaws than Hursti had found in Florida,** vindicating Supervisor Sancho's actions in responsibly trying to do his job.

In May of 2006, Bruce Funk, a county clerk of 23 years in Utah, was concerned that the numerous problems with the Diebold machines purchased by his county were not reliable enough for the voters, "I'm the one ultimately responsible and I felt I needed to be assured myself that everything was okay," he said [20]. Funk called Black Box Voting and arranged for Hursti to perform an independent inspection which revealed the same security holes Hursti had uncovered in Florida in Ian Sancho's district [21].

For his diligence and integrity Mr. Funk was forced to resign. **Diebold accused both Funk and Sancho of breaches of contract in letting an unauthorized third party inspect the machines.** Even though Funk only permitted Hursti to examine two machines, the county is recertifying all 40 models at the price of $1,260/day /technician. Funk said commissioners accused him of causing $40-50 thousand in "recertification" costs and pressured him to resign.

Diebold has been highly successful in threatening and suing its way to greater profits at the expense of the citizens of the United States. But a case in North Carolina is particularly instructive for New York. North Carolina had enacted a source code escrow requirement similar to New York's. In 2005, on the day voting equipment bids to the state were due, Diebold sought and received relief in North Carolina's superior court, claiming, at the last minute, it was unable or unwilling to comply with North Carolina's

law. Diebold had obtained a TRO, permitting it to evade key transparency requirements of the law, until Electronic Frontier Foundation (EFF) intervened and the court dismissed the action.

Notwithstanding, Diebold managed to get certified even though it did not comply with the escrow requirements. Similar to the situation in New York where Avante is making Diebold's arguments, Diebold argued that none of the vendors can comply with the statute because they all rely on proprietary software. The argument appeared to save the day for Diebold. But then Diebold withdrew from the bidding.

> *Despite the judge's recent ruling, the company seems concerned that at some future point it could be convicted of a felony for not complying with the letter of the law. In its letter* ***the company generously offered to help the state revise its legislation so that "all vendors will be able to comply with the state election law."*** *As the EFF rightly points out, though, the legislature's job is not to craft rulings that all American companies can comply with, but to write fair laws that companies are required to meet. The EFF opines:*
>
> ***Too many (though certainly not all) election officials across the country treat the certification process as if the vendors were their clients, deserving of favors and rule bending. Voters – the only constituency that matters in this process – are too often treated like ill-mannered party-crashers when they try to ensure that their interests are being protected.*** [22] (emphasis supplied)

Diebold had withdrawn from the bidding claiming it was not at liberty to disclose the source codes controlled by Microsoft, which is curious since Diebold had escrowed Microsoft source code in other states (ie, Georgia). Thus it remains unclear whether Diebold withdrew for the reason given or because North Carolina also imposes harsh criminal and civil penalties. **Dieblod had already been decertified in California for misrepresentations to the SOS regarding the installation of uncertified software on their machines**. **A False Claims Act lawsuit filed against Diebold was settled by Diebold's paying $2.6 million.** [23]

The example of Diebold, in choosing to ignore North Carolina's law and then seeking to evade it at the 11th hour, is precisely what Avante and Microsoft are doing in New York at the present time. All of the major vendors *chose* to use Microsoft's products, thereby voluntarily making themselves unable to comply with New York's 2005 escrow requirements. (see discussion of this issue at pp 35-39)

Avante's and Microsoft's tactics show insulting disregard for the laws of a sovereign state and a brazen willingness to disrespect those laws with the intention of later strong arming the powers that be in order to override the law. It is a direct consequence of the privatization of our elections, particularly when those private corporations have a monopolistic hold. As discussed at the Conclusion, this is one of the compelling reasons why New York must resist falling prey to such domination if it is to abide by our Constitution and the rights of its citizens.

Diebold's Past Performance Failures

A Partial List of Documented Diebold Failures: [24]

Voters Unite has put together a 28 page list documenting some of Diebold's machine failures. 26 of the 28 pages involved problems withe Diebold's Accuvote, the model New York is testing for certification. The AccuBasic software language exists on all Diebold systems, as Diebold admitted in a memo to Pennsylvania authorities on January 5, 2006. [25]

Because Diebold's history of unacceptable past performance is so intertwined with its unethical efforts to mislead, intimidate or otherwise suppress this information the performance failures are not separately listed herein, but are contained in the earlier section entitled *Lack of Integrity to Perform the Contract: Diebold's Irresponsible Efforts to Cover Up, Intimidate and Suppress Exposure of Failed Performance and Security Flaws.* The security flaws however, deserve special attention and are included below.

Notwithstanding the myriad of uncorrected security risks which only increase with each successive independent analysis, New York intends to waste tax payer money testing the Diebold optical scanner still again!

Past Performance Failures: Security Flaws in Diebold's Voting Systems

As described below, Diebold has been the subject of numerous damaging security

reports beginning in 2003 with the Rubin study and continuing with the RABA study, the Hursi Report and the two Hursti Hacks, the California Security Analysis, the University Of Connecticut Security Assessment in the fall of last year, to name some of the extensive examinations that have focused exclusively on Diebold's security holes. These reports should be enough to cause anyone to conclude that New York has no business with Diebold. The corruptibility of Diebold's product is matched only by Diebold's behavior in response to these continuous exposures of unsafe voting equipment.

It is the Diebold AccuVote OS Opscan (sometimes referred to as AV-OS) which is the subject of these reports and which the SBOE is scheduled to test for New York's use.

In July 2003, a team of computer scientists at Johns Hopkins University and Rice University led by Dr. Avi Rubin released a report on the Diebold software (the Rubin Report) which was devastating because it **documented numerous programming flaws and security issues.**[26]

In November 2003 the Department of Legislative Services, Maryland General Assembly of the State of Maryland, entered into an agreement with RABA Technologies, LLC to perform a "trusted agent" evaluation of, *inter alia*, the Rubin Report [27]. The **RABA Report's confirmation of Diebold's general lack of security awareness** as reflected in the Diebold code, is a valid and troubling revelation. A working key to the **AccuVote hardware is readily available to an attacker. One team member picked the lock in approximately 10 seconds**. Individuals with no experience (in picking locks) were able to pick the lock in approximately 1 minute.

The team also found the GEMS (Diebold's **election management software) server lacks several critical security updates from Microsoft**. The team was able to remotely upload, download and execute files with full system administrator privileges. **One can insert a CD that will automatically upload malicious software, modify or delete elections**, or reorder ballot definitions.

In July, 2005 the **Hursti Hack of the Diebold Accu Vote optical scanner (AV-OS**) was released (see endnote 16). The Hursti Hack, referred to as "**the mother of all security holes"** concerned the changing of votes on memory cards, which Diebold had insisted to election officials across the country, was impossible. Then Hursti was permitted access in December of 2005 by Ion Sancho, election director of Leon

County, Florida, and proved how easily the votes could be changed on the Diebold optical scanners.

In response to the Hursti report, the **California Secretary of State commissioned a separate independent review** which found significant, previously unknown, vulnerabilities associated with the Diebold AccuVote optical scanner. The findings of the California report issued by the California Voting Systems Technology Advisory Board on February 14, 2006 [28]confirmed **Hursti's findings that the Diebold optical scanners can be hacked without detection** and described how serious this vulnerability in the Diebold software was. **The California Security Analysis looked at the source code for the Diebold Accuvote Optical Scanner – the Optical Scanner New York is scheduled to test!**

While the report listed short term mitigation strategies that could be employed for use in local elections, they recommended not using the Dieblod systems in statewide elections unless the vulnerabilities were fixed by re-writing the architecture of the system, because "Larger elections, such as a statewide election, provide a greater incentive to hack the election and heighten the stakes." Additionally, the California report warned:

> ***successful attacks can only be detected by examining the paper ballots. 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. The only way to detect and correct the problem would be by recount of the original paper ballots.*** (emphasis supplied)

In October, 2006 the **University of Connecticut examined the Diebold AccuVote-OS Optical Scan and identified a number of new vulnerabilities, which if exploited maliciously can invalidate the results of an election process**. The report[29] also indicates that the AV-OS 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 the election day, thus avoiding detection through pre-election tests.**

Avi Rubin, Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University, who led the first group of computer scientists examining Diebold's software in the Rubin Report, described the report from the University of Connecticut this way:

> *Reading this report was a hair raising experience for me. Diebold has clearly not learned any of the lessons from our 2003 report, and it is startling to see that their optical scan ballot counter is as vulnerable to tampering, vote rigging, and incorrect tabulation as the DRE.* [30]

3) Sequoia Voting Systems

Lack of Integrity to Perform the Contract

The third largest electronic voting machine manufacturer has demonstrated the very unethical business practices condemned by Governor Spitzer's Public Employee Ethics Reform Act of 2007. Sequoia's revolving door practices are precisely the kind of behavior the Governor has singled out as prohibited in New York. In addition Sequoia has shown the same lack of ethics and violations of the Vendex rules as have the other vendors. The violations relevant to consideration pursuant to the Law are highlighted below. Sequoia's rampant corruption and regular violations of New York's Law and rules should enjoin New York from continuing to do business or entering into new contracts with Sequoia.

David Philpot, Sequoia's exclusive agent in Louisiana, was **convicted of bribery in a 1999 kickback scandal**. Philpot was the brother-in-law of Philip Foster, Sequoia's southern regional sales manager, who was indicted in 2001 for crimes related to this scandal. The two were **charged with counts of conspiracy, money laundering and malfeasance in office after giving $100,000 in kickbacks to Louisiana state elections chief Jerry Fowler. Philpot plead guilty and Fowler went to federal prison.**

Foster was granted immunity in exchange for his testimony and has since been promoted by Sequoia. He is presently serving as the Vice President of Administration & Strategies. He remains one of Sequoia's key employees. He served on the Palm Beach County Election Technology Advisory Committee from September 2005- May 2006.

In November, 2001, two Florida counties, after learning of Foster's background, halted purchases of Sequoia voting systems. (See the report referenced at footnote 1 for further documentation)

In a 2002 lawsuit challenging an election in Palm Beach County it was revealed that **under the county's purchase contract with Sequoia, disclosure of any specifications of how the DREs operate was a third degree felony!**

Sequoia also has a prolific habit of hiring its own regulators:

– Kathryn Ferguson, the elections official who helped purchase Sequoia machines for Clark County, Nevada and Santa Clara County California.

–Former California Secretary of State Bill Jones.

– Former executive director of the Denver Election Commission, Michael Frontera (went to work for Sequoia after awarding $6.6 million in contracts to them).

– Former spokesman for Secretary of State Bill Jones, Alfie Charles, now a Sequoia spokesman.

Sequoia's Vice President, Howard Cramer, has been repeatedly accused of lying and misrepresentation to various state officials. (See footnote 1 at p14 therein for Cramer references)

– In November, 2006, a Sequoia electronic pollbook system crashed in a Denver election. It was estimated by officials that more than 20,000 people didn't vote because of the delays caused by the Sequoia-designed software. Sequoia's VP Cramer tried to lie his way out of assuming responsibility. He lied to the Mayor's panel hoping to pass the blame on the election commissioners for ES&S's failure.

– Cramer had told the mayor’s panel he was surprised to learn Denver was using the company’s technology as an “e-pollbook” to check in voters at the polls. Sequoia

spokeswoman Michelle Shafer said Cramer's statements may have been misconstrued. "Howard (Cramer) certainly knew that we had a product that was being used in Denver, however, that has never been marketed as an electronic pollbook," she said. "That is not what we provided."

– Subsequently documents were released showing the Denver Election Commission had expressly requested that type of technology from Sequoia for its e-pollbook use. "It is not up for debate," Election Commission operations manager Matt Crane said. "I don't know how we can be any more clear on that."

In November 2002, **Cramer had been accused of a cover up by New Mexico election officials, for failing to them of a known software bug that mis-tabulated votes.** The Albuquerque Tribune reported New Mexico Commissioner Tom Rutherford accused Cramer of a "cover-up" and said Cramer had never intended to tell New Mexico officials that the same error occurred on Sequoia's voting machines in Nevada just a few weeks earlier. Sequoia admitted to knowing about the bugs in the Nevada election but never mentioned this to election officials in New Mexico.

Another known and relevant aspect regarding the excessively high costs associated with DREs also goes unmentioned. A recent article about the astronomical and wasteful "hidden"costs of Sequoia's DREs should be noted since these expenses are not being taken into consideration by election commissioners in deciding how to spend taxpayers' money. On July 3, 2007, The New Jersey Record reported that Sequoia DREs required $44,000 worth of electricity for their *monthly* battery charge in Bergen County, New Jersey. The machines need to be charged monthly and the machines don't like humidity. These fees for battery charging are on top of the extra costs associated with air-conditioning! These expenses are not reimbursed by the federal government and are yet additional expenses to be incurred by taxpayers[31].

Lack of Integrity to Perform the Contract: Sequoia's Irresponsible Efforts to Cover Up, Intimidate and Suppress Exposure of Failed Performance and Security Flaws

As explained below under *Past Performance Failures: Security Flaws in Sequoia's Voting Systems*, just like ES&S and Diebold, Sequoia shuns responsibility for its

products preferring the spin-control/crisis management method of claiming it is either no problem or whatever it is, they can fix the problem. One wonders why their systems, notwithstanding their alleged ability to correct the security problems, keep getting hacked.

In March 2006, Pennsylvania's Allegheny County had decided to use Sequoia's Advantage DREs because the Diebold DREs they'd been planning on using were shown to be hackable. **But the Sequoia Advantage DRE, the model New York is planning on testing, has now been shown to be hackable as well**.[32] Sequoia's response to the problems found were characteristically, "no big deal".

Dr. Michael Shamos, a Carnegie Mellon University professor and state voting-machine examiner didn't see it as no big deal and shut down the testing, concerned that a malicious hacker could do just what Shamos had been able to do in the testing. The testing of the Sequoia DRE revealed a myriad of problems including Shamos' findings during "tampering tests" he was able to instantly "transform a handful of votes into thousands".

Sequoia, claiming they could simply fix the software problem, replaced the tabulation software, but that didn't alleviate Dr. Shamos' concerns. Sequoia continued to minimize the problem through spin, "We know the hardware is fine. It's been out there for eight or nine years.... The software doesn't need to work until just before the election so we've got time. It's no big deal," he said.

Sequoia had been under scrutiny because of **tabulation software problems** in Chicago's 2006 primary elections [33]**. Sequoia blamed those problems on poll workers, rather than accepting responsibility** for creating the equipment that could according to Sequoia, be so easily compromised.

This past **February, 2007, it took a professor of computer science at Princeton University only seconds to hack a Sequoia Advantage DRE**. Again rather than accepting responsibility, Sequoia revealed its concern is not with the faulty product it produces so much as with the appearance of that product. **Sequoia's crisis-management team's responded in kind, referring to "our tamperproof products, including.... the AVC Advantage, are sought after from coast to coast for their accuracy and reliability." [34] That's a bald face lie!** There isn't a computer scientist in the country who would claim there is any such thing as tamperproof software or a

tamperproof computer. Indeed Sequoia's "tamperproof products" have been found to be highly tamperable as discussed above and at *Security Flaws in Sequoia's Voting Systems*, below.

Sequoia's Past Performance Failures

A Partial List of Documented Failures[35]

Again, this is the list referred to earlier compiled by Voters Unite, broken down by vendor. There are 27 pages relating just to Sequoia's machine failures, almost every page of which involves Sequoia's AVC DRE or the Optech scanner, the models New York is slated to begin testing. Presumably Sequoia will promise to correct the past problems that have been documented, notwithstanding its efforts to prevent these revelations. The evidence that newer models or fixes don't in fact improve the problems, however, speaks for itself.

It is significant to note that results of **Sequoia's Advantage DREs, the model the SBOE is considering for use in New York, were so flawed and suspect that New Mexico banned the use of DREs across the entire state after their disastrous experience with these Sequoia DREs during the 2004 Presidential Election**.

In New Mexico, presidential undervotes were greater for ballots cast on the Advantage DRE than those case on any other type of system used on Election Day. **One in every 19 ballots cast on Sequoia Advantage DREs simply did not register a vote for president**. The undervoting wasn't seen uniformly across the state, but in the heavily democractic Native American and Hispanic areas. Details now out from New Mexico reveal that undervote rates dropped precipitously in both Native American and Hispanic areas after the state moved to paper-based optical-scan systems in 2006.[36]

Past Performance Failures: Security Flaws in Sequoia's Voting Systems

In November, 2006 a major security flaw was revealed in all of Sequoia's DREs. It turned out that every DRE produced by Sequoia had a yellow button on the back of each Sequoia DRE, which when pressed once could place the machine into manual mode allowing anyone to cast as many votes as they desired.[37]

Given the nightmarish experience of New Mexico in using Sequoia's DREs – so bad the state abandoned its DREs and switched to paper ballot optical scanners– and given the very recent hack of the Sequoia AVC Advantage DRE, why is the SBOE testing the same model for potential sale to New York?

The Princeton University computer science professor, who hacked the Sequoia Advantage DRE this past February, 2007, revealed that a student was able to pick the machine's lock "in seven seconds" to access the removable chips containing Sequoia's vote-recording software. At the Princeton professor observed, not only was the hack simple, but Sequoia's literature was untrue.

> ***The AVC Advantage can be easily manipulated to throw an election*** *because the chips which control the vote-counting are not soldered on to the circuit board of the DRE. This means the vote-counting firmware can be removed and replace with fraudulent firmware.*
>
> .....
>
> ***We can take a version of Sequoia's software program and modify it to do something different --- like appear to count votes, but really move them from one candidate to another. And it can be programmed to do that only on Tuesdays in November, and at any other time. You can't detect it.*** (emphasis supplied, see endnote 34)

4) Liberty Election Systems

Lack of Integrity to Perform the Contract

The Liberty DRE marketed in the United States by Liberty Election Systems is manufactured by the Dutch company, Nedap. It is the same machine marketed in Europe as the PowerVote Voting System.[38] These DREs and their software have been found to have crucial security and accuracy flaws; serious enough to enjoin New York's contracting with Nedap/Liberty. Moreover, given the repeated examples of coercive and threatening antics exhibited by Nedap in the Netherlands, Governor Spitzer's commitment to high ethical standards would proscribe this company's doing business in New York State.

In 2003, Ireland spent 50 million euros on 7500 Nedap DREs, but has never used the machines because of their vulnerabilities. The Irish government created an

Independent Commission on Electronic Voting (the Irish Commission) to examine the security of these DREs. The Irish Commission published two reports that raised **critical doubts about the accuracy and reliability of the software used to count votes on the Nedap/Liberty DREs.**[39] In September 2006 an independent Dutch voting integrity group **published a highly critical analysis of the Nedap/Liberty DREs, revealing how easily the machines could be hacked and how open they were to undetectable control over the election results.** [40] The security concerns of these DREs are discussed below, see *Security Flaws in Liberty's Voting Systems*.

Public disclosure of Nedap's security weaknesses angered its CEO who in retaliation attempted to extort the Dutch government by threatening to disrupt the elections. A letter to the NYS BOE detailing this information was sent by The Voting Integrity Project on April 26, 2007 [41]. The inappropriate bullying behavior of Nedap is discussed under the subheading, *Nedap/Liberty's Irresponsible Efforts to Cover Up, Intimidate and suppress Exposed Failed Performance and Security Flaws*.

In May of this year Bo Lipari, founder of New Yorker's for Verified Voting, described Liberty's "... brazen attempt to get their uncertified DREs used in New York State. Liberty Election Systems and their Dutch partner Nedap made the City School District of Troy New York an offer they couldn't refuse –use of their DREs in the upcoming May 15, 2007 School District Election *at no cost to the district*."[42] **Nedap/Liberty distributed a brochure on the Troy City School District Election containing numerous misleading statements and false claims– a highly improper commingling of the private company promotion with official School District election information – *a disturbing combination of public elections and corporate advertisement.*** [43]

Further evidence of Liberty's unsuitability to do business in New York is detailed below and can be found at New Yorkers for Verified Voting's website, www.nyvv.org.

Lack of Integrity to Perform the Contract: Nedap/Liberty's Irresponsible Efforts to Cover Up, Intimidate and Suppress Exposure of Failed Performance and Security Flaws

In the fall of 2006, a Dutch TV program featured a story about the voting integrity group, "We don't trust voting computers foundation", publicly airing the hacking of

the Nedap/Liberty DRE. [44] The exposed vulnerability caused the Dutch authorities to order an investigation. They then set up an independent commission to scrutinize the electoral process in the Netherlands. Nedap provides 90% of the software for the electoral districts in the Netherlands.

In response to the revelation of how easily the Nedap/Liberty DRE could be hacked, Jan Groenendal, CEO of Nedap, threatened to sue the television program and demanded that the two machines acquired by the voting integrity group be confiscated. **He also wrote to Dutch election officials suggesting the hacker**, who had demonstrated the vulnerability of the voting system, **be arrested and detained stating** "After all, **his activities** are destabilizing society and are as such **comparable to terrorism."**[45]

A FOIA request revealed additional startling reactions by Mr. Groenendaal, intended to intimidate and bully the authorities. Mr. Groenendaal **threatened to stop "cooperating" with the Dutch government if they did not accede to Nedap's demands**. The Dutch government is of course dependent on Nedap to run its elections since 90% of its software is supplied by them. The **CEO warned the ministry that his company will cease all activity if Rop Gonggrijp, who exposed the very serious security problems by readily hacking the DRE, is permitted to become a member of the independent commission** that was created in response to this exposure of the vulnerability of Nedap's voting software.[46]

Rather than accepting responsibility for the myriad of insecurities revealed in the various security reports, Nedap instead sent letters to all Dutch municipalities blaming the Ministry of Interior for their handling of the crisis over the verifiability of the voting computer election results. The various emails and letters by Nedap, rejecting all responsibility by the company are included in the document at endnote 46.

In August of 2006 Groenendaal misrepresented that his voting system was not a computer, but rather a specialized voting machine "that was manufactured for elections and for nothing else"[47]. Groenendaal added that he would "like to see someone demonstrate that you can play chess with our voting machine" as if it were a computer, which is precisely what the voting integrity group, We don't trust voting computers foundation, did!

In response to these revelations in the Netherland that Nedap's DREs could be easily

hacked, made to record inaccurate voting preferences and could even be secretly reprogrammed to run a chess program, Nedap tried to minimize evidence of these critical flaws. In response to the Irish Commission's reports that it was impossible to determine if one's vote is recorded correctly on these Nedap DREs, Nedap hid behind its spin control – "It is really much ado about nothing. ... Groenednaal's software doesn't have anything to do with determining the results in the elections, that is all done on our machines and is developed in house" – (endnote 46).

This willingness to hide such significant problems with its DREs and evade responsibility, is characteristic of the disregard American voting vendors have shown for their continuing exposure of the security risks conveniently hidden behind their proprietary software.

Nedap/Liberty's Past Performance Failures

The security reports from the Netherlands and Ireland expose the Liberty DRE as too unsafe and unreliable to entrust New Yorkers' ballots to. In addition, as detailed below, the DRE created for use in New York does not comply with New York's requirement that a DRE produce a permanent paper record to enable voters to verify their vote and permit an audit of the paper records.

New York requires that DREs produce a "voter verified permanent paper record which shall be presented to the voter" McKinney's Election Law sec 7-202 (1) j. The regulations, Part 6209.1 (am), refer to this as a VVPAT, a voter verifiable paper audit trail. One of the reasons for requiring a VVPAT is, as the name says, so a **V**oter can **V**erify her/his vote to see if it was properly recorded as cast.

Liberty's machines have not had this VVPAT in Europe and Nedap has been resistant to providing same. Nedap's contempt for supplying a VVPAT is apparent from the product it is now offering in New York. As explained below what is provided as Liberty's VVPAT is a sorry excuse for same and cannot be considered as complying with New York's requirements.

In Nedap's comments contained in the Second Report of the Irish Commission on Electronic Voting, Nedap took the position that its system should essentially be trusted without needing any paper audit! Nedap argued that a VVPAT is not only

unnecessary, but actually undesirable (see endnotes 39 and 50). In support of this claim Nedap misrepresented the arguments made in a paper by Selker and Goler (the paper is referred to at endnote 50 at note 3). However the Selker paper actually advocates VVPAT, but considers a voter-verified audio audit a better alternative to VVPAT.

Begrudgingly, and in order to do business in New York (business in Europe isn't looking very good since these DRE's insecurities were revealed [48]), Liberty has created the *appearance* of complying with New York's VVPAT requirement. But what it has created is so violative of the intention of the statute that it insults the purpose for which the law was written, to wit, to permit the **Voter** to be able to **Verify** that her/his vote was correctly cast and that there are no discrepancies.

Instead of creating a means for the voter to be able to perform this audit of her/his vote, Nedap/Liberty has provided a tiny window which displays a very small 3" x 1" paper *summary* that is difficult to see. The VVPAT window is so small, all that can fit on it is an incomprehensible summary containing symbols that are supposed to correspond to the way the voter voted. There are numbers and letters appearing on the tiny piece of paper (ie., 2A, 4C, 6B, etc) which have no meaning to the voter. As portrayed at the photographs of the system at this endnote[49], the DRE displays a larger screen with over 200 ballot positions, each square, or ballot position having a little symbol printed in it. The voter is supposed to match up the numbers on the 3"x1" summary to the symbols appearing somewhere on the screen with the more than 200 ballot positions. Effectively it's the equivalent to not having a VVPAT because no one will be able to have the time or ability to do this.

In fact, it is difficult to imagine how one could create a more incomprehensible and unusable means to verify a vote, short of not having a VVAT at all, which is precisely the outcome Nedap advocated for! [50] For the SBOE to consider this unverifiable scrap of paper in coded, non human-readable form, as satisfying the legislation requiring a VVPAT, is to mock the intention of the law which was to provide an actual means by which voters could believe they were verifying their votes.

Past Performance Failures: Security Flaws in Liberty's Voting Systems

The two reports produced by the Irish Independent Commission on Electronic Voting are thorough and extensive. The Irish commission found it was 'very easy' to bypass

security measures on the computer doing the count, and it had concerns about the secrecy of the ballot. According to the Irish Citizens for Trustworthy Evoting's submission to the commission, the Nedap/Powervote electronic voting system had a fundamental design flaw because it had no mechanism to verify that votes would be recorded in an actual election. Consequently, **results obtained from the system could not be said to be accurate.** [51]

The Irish Commission's first report in 2004 (see endnote 39) found the Nedap/Liberty DREs to be so insecure that the Irish government has refused to permit their use, incurring 700,000 euros/year in storage costs instead. [52] The first report from the Irish commission found:

> "There is no post fact method of validating that the votes stored in the data cartridge are the same as those entered at the keyboard by the voters", **making any auditing unfeasible.**
>
> "Someone with access to Nedap's source code could alter the program while also ensuring that it returned the expected checksum at start-up" and that "An exchange of the ROM chips including fraudulent presentation of the correct checksums cannot be avoided by software but by means of sealing only." Thus there was **no way to ensure the integrity of installed software**.
>
> "In practice it took a technician about 40 seconds to open the machine from the back. We observed that the controlling program chips are actually socketed for ease of access. Therefore there is little to prevent removal and substitution of the program..... We estimate that 2 minutes of unauthorized access would be sufficient to switch programs."
>
> "The seals on the voting machine peeled back equally easily. Four Phillips head screws had to be removed."

In the Second Report of the Irish Commission on Electronic Voting, issued in July, 2006 (see endnote 39) the commission concluded that only if further work on the voting equipment, **which involved complete replacement of the IES election management software**, [53] would the commission consider recommending its use. The Commission noted that even with a complete replacement of the election management software and other changes to the overall operation of the elections system, more testing would still be required.

According to this second report, the IES election management software is composed of three main sections: 1) Preparation and Administration, 2) Programming and reading in ballot modules, and 3) The Count, run on Microsoft Windows 2000. It is this third part – the IES election management and counting software – that the commission has required must be completely rewritten.

A Review of the Second Report of the Irish Commission on Electronic Voting (endnote 50) noted that auditing of Nedap/Liberty DRE was:

> ***"complicated by the fact that the IES is critically dependent on third-party software such as Microsoft Windows and the Microsoft Access database system****, as well as the Borland Delphi software development environment, none of which has been independently audited. While some of these difficulties can be mitigated, and others entirely corrected,* ***it is impractical, if not impossible, to be able to guarantee that any electronic voting system is completely trustworthy and, as important, is seen to be trustworthy. The fact that a company with the resources of Microsoft has not been able to guarantee the security of its own web browser (let alone the entire Windows operating system) despite years of effort and large incentives, suggests that a fully secure and trustworthy electronic voting system may be an unattainable goal."*** (emphasis supplied)

Notwithstanding the almost 1,000 pages contained in the two comprehensive reports by the Irish Commission on Electronic Voting, the Security Analyses by Rop Gronggrijp detailing the open access to virtually undetectable control over the election results and the obvious insult to New York's requirements that the DRE have a VVPAT, the SBOE is planning on testing and potentially certifying this demonstrated theft-enabling DRE! No set of regulations or statute which respects the constitutional rights of citizens could permit the use of this voting system.

5. Avante

Lack of Integrity to Perform the Contract

Avante has been around since 2001, but has had trouble getting certified anywhere. Consequently there isn't much history to evaluate. However, Avante has already manifested an arrogant and flagrant disregard for the laws of New York that should foreclose consideration of contracting with such a company.

Since June, 2005, New York has required the archiving of source codes used in voting equipment. Section 7-208 of Election law, requires that "a complete copy of all programming, source coding and software employed by the voting machine shall be placed into escrow with the SBOE. **The vendors were aware of New York's escrow requirements, but chose to ignore them. Only Open Voting Solution (OVS), which produces the only open source optical scanner but is not currently being considered by the SBOE, took New York's requirements seriously and adapted its voting system so that all of the source code was open.** [54] OVS is alone among the vendors who all chose to disregard New York's law, hoping to have the law rewritten or reinterpreted in their interests. This singular act speaks volumes about the type of vendor OVS is and the type of vendors New York is proposing to do business with.

Avante, as well as the other vendors, have created voting systems that thwart the public's right to the most essential information the public is entitled to: how their elections are run, including how their votes are being counted. Avante, and the others, claim the way their computers are programmed to process and count our votes is confidential information that must be kept from the public.

In creating its closed voting system Avante (and Sequoia) chose to use Microsoft's proprietary software for their operating system and for their election management system (EMS). Diebold, ES&S and Liberty use Microsoft in their EMS, but not in their operating system. Microsoft would not permit its source code to be escrowed, but Avante (as well as the other vendors) chose not to modify their system to comport with New York's requirements, the way OVS did. Avante chose to stay with its closed software voting system and simply ignore our law (as did the other vendors). Thus Avante's and the other vendors' inability to comply with the law is their own doing.

After waiting two years and on the eve of New York's commencing certification testing again, **Avante commenced a campaign to persuade our election commissioners to ignore New York's law, just as Avante had done**. On June 20, 2007, Rick Gleim, vice president for Avante, sent an email[55] to all New York State election commissioners and officials disingenuously blaming the SBOE for Avante's refusal to comport with New York State's Law.

In that email Avante asserts that New York's law is unfair to Avante and therefore New York should change its law or interpret it in such a way that favors Avante and the other private vendors, in order to allow them to escrow only what they want to escrow**. Avante's position – protect our corporate interest in concealing**

information so our computers can be certified to process and count New Yorkers' votes in secret – is blatantly outrageous. Avante understands that and therefore has invented a specious 'all or nothing' argument to cloak its position.

In evaluating the security of a computerized system there are different levels of source code to be considered. There is the source code which actually operates the voting system and directs the computer how to process the votes; the source code which directs the election management system (EMS), part of which tells the computer how to tabulate the votes; and the software contained within the commercially produced hardware (firmware). Ideally all source code information should be known and made available for public scrutiny. Commercial-off-the- shelf hardware manufacturers, who are not in the election business, don't always choose to make their source code available. However those who endeavor to manufacture voting systems must choose the most openly available software in creating their systems.

Avante, knowing no vendor has control over the source code for the lower level firmware, disingenuously concludes that since no vendor can escrow the source code for the firmware, then no vendor should be required to escrow source code for the more critical aspects of the voting system – the operating system and the vote tabulation system. The argument is intended to obfuscate the fact that Avante can't escrow the source code for any of these critical functions because it chose to use Microsoft Windows operating system in its DRE.

In what could perhaps be described as a copycat case or perhaps just a lack of corporate imagination**, Avante has lifted the arguments Diebold made in the North Carolina litigation two years ago and offered them anew to New York** (see endnote 22). In that litigation Diebold argued, as Avante does now, that North Carolina's escrow statute was too broad and couldn't possibly mean what it said, but that if it did mean that, Diebold couldn't comply.

Similarly Diebold and now Avante **whine that it is the SBOE who is to blame for the vendor's inability to comply with the law** (in N. Carolina's case for providing "conflicting guidance" and in NY's case because "Your state board can't agree") – both bogus claims intended to distract from the underlying failing in both situation, to wit: Neither vendor was able to meet the requirements of the states' statutes. Both vendors employed the same **tactic of waiting until the eleventh hour to object to having to comply with the Law, hoping it would be too late for the state to do anything but accept their disregard for the power of the state to determine and**

enforce its laws in the best interest of its citizens. The tactic is designed to force the state to bend to the will of the vendor. It didn't ultimately succeed in North Carolina, where both Diebold and Sequoia pulled out at the last minute, and it shouldn't be permitted to succeed in New York. [56] **Failure or refusal to conform with New York's Law is not a legitimate excuse for non compliance.**

The current dispute at the SBOE is over how much source coding needs to be escrowed, not how little should be escrowed. For Avante to argue that since the SBOE can't agree on how much is necessary, nothing should be escrowed except what Avante minimally chooses to supply, is not only contemptuous of its responsibility to comply with the law, but exposes Avante's argument for what it is: self-serving and dishonest.

Equally deceitful and arrogant is Avante's claim that "It is not possible to design new equipment with new operating systems, new EMS …… in less than a couple of years. *And that is, if the vendors wanted to do this*." Clearly the vendors don't want to do this or they would have done it. The vendors only want to sell us a voting system which prevents the public from knowing how their elections are processed and their votes counted. The more open system, which Avante claims will take a couple of years to create, is what Open Voting Solutions has already created (see my Memo II entitled *Alternative Voting Systems that are HAVA-compliant, NYS-compliant and Democracy-compliant).* If Avante had used the last two years to make its system more open rather than hoping to strong arm New York to change its law, it wouldn't have to resort to these dishonest arguments to persuade New York to reinterpret its law in Avante's interest.

Perhaps the clearest example of Avante's lack of integrity to do business in New York is exposed in the closing lines of Mr. Gleim's email. Trust us, Avante concludes because "Vendors voting equipment has been proven worthy around the country." Really? One needs only look at the extensive evidence of faulty equipment, excessive breakdowns, tampering, vote flipping, mysterious under votes, impossible vote tabulations, etc. to see Mr. Gleim's claim is patently false.

The most revealing and the only honest claim in this email is Mr. Gleim's: "The point of changing the law is to allow NY to certify new equipment. The current law makes that impossible." Either Avante is correct that New York's Law must be changed to allow Avante's equipment to be certified or the Law should remain as is, providing some means to be able to see how these private computers are programmed to process

and count our votes.

As the attorney for EFF in the North Carolina Diebold litigation referred to earlier states:

> *the company generously offered to help the state revise its legislation so that "all vendors will be able to comply with the state election law." As the EFF rightly points out, though,* ***the legislature's job is not to craft rulings that all American companies can comply with, but to write fair laws that companies are required to meet.*** *The EFF opines:*
>
> *Too many (though certainly not all) election officials across the country treat the certification process as if the vendors were their clients, deserving of favors and rule bending. Voters – the only constituency that matters in this process – are too often treated like ill-mannered party-crashers when they try to ensure that their interests are being protected.*

If we rely on the Avantes of the world, who tell us "voting equipment has proven worthy around the country" and disregard the evidence before our eyes, democratic elections are doomed.

Avante's Past Performance Failures

Because of Avante's difficulties in obtaining certification, there isn't must of a performance track record to evaluate. However, a study of *The Importance of Usability Testing of Voting Systems* [57] rated Avante's DREs (along with Nedap's DRE) lower on most criteria as compared to the other DREs in the study.

The DREs in the study were the Avante Vote-Trakker, Diebold AccuVote-TS, Nedap LibertyVote and a Zoomable prototype (developed specifically for the study). There was also an optical scanner and a fifth system (Hart Intercivc eSlate), described as using a dial and buttons to move through the ballot and vote. The systems were evaluated in terms of usability because of the concern that to the extent systems had features "making the voting experience less pleasant and more difficult than necessary while causing voters to ask questions about what should be a simple process and to doubt the validity of the outcome", this was significant and should be remedied. The study found (emphasis supplied):

Navigating the Ballot:

*"**The Avante system**... **offers voters less control in navigating the ballot**. After a candidate for office is selected, the software automatically moves the voter to the election for the next office until the ballot is completed. The speed at which this occurs, and the **loss of control over the voting process, led many to rate the Avante system lower than the other two touch screen systems**."*

*"**Nedap....was rated significantly lower across the board due to the challenges it poses for voters**. First, glare on the ballot surface combined with the small blue lights that glow when voters make a selection (rather than a large X or lighting up the entire box containing the candidate's name) make it difficult to see how one has voted if the room is brightly lit. Second, the membrane buttons a voter must push to make a selection are covered by the ballot so one does not actually see them, and they must be pushed directly using some force. A third of the subjects who commented on this system criticized the buttons."*

Correcting or Changing a Vote

*"**The Avante system is perhaps the most challenging of the three systems.** Because of the automatic navigation system, voters have to wait until the review stage of the voting process to make changes—if they remembered to make them. **This caused voters to rate the system considerably lower than the other touch screen systems** on comfort and ease of use. A quarter of those who commented on the system, disapproved of this aspect of their experience."*

***"Changing votes on the final two systems was not as trying as on the Avante system**, but not without challenges..... **The Nedap system**.... required voters to deselect a candidate before selecting a new one. However, **voters appeared to find this system more taxing** because of the need to locate the membrane buttons behind the ballot"*

Write-in Votes

*"With electronic systems, write-ins took more time than with the paper ballot, but other problems existed as well. On the **Nedap LibertyVote, the size of the window was very small** and it was below the large ballot. **On the Avante system**, the need to enter the first name, then tab to a second field to enter the last name **resulted in considerable confusion**."*

Reviewing and Casting the Ballot

*"**Reviewing a ballot on the Nedap system** is simple, and it is impossible to overvote on it. Still, **more errors are likely on it than on the previous four systems**. As was the case with the paper ballot, voters review their selections which are displayed throughout the entire voting process. **Voters are warned of undervotes on a small window at the bottom of the system** and given the option of filling in missing votes or casting the ballot as is. **However, the text window is so small that some participants did not notice the message. Others did not understand the problem; some voted for one office they had left blank, failing to notice other blank offices, which led to a series of undervote messages**. In addition, when the screen said Ballot Complete, voters often failed to realize that they still had to press Cast Ballot. These difficulties contributed to the low rating given this machine on confidence that one's vote would be recorded accurately."*

The Need for Help

***"A question of substantial importance to election officials is: Can voters cast their ballots unassisted?** The answer is that most but not all can. **The Diebold, ES&S, and Zoomable systems performed the best in this regard, with 18, 24, and 22 percent**, respectively, reporting the need for assistance. **The Avante system came next, with 29 percent** stating they required some help. **Finally**, 36 percent stated they felt the need for assistance using the Hart system and **44 percent gave the same response regarding the Nedap system**."*

A recent report from the New Jersey Institute of Technology regarding testing performed on voter verified paper audit trail printers for Avante's Vote-Trakker EVC308-FF (the same DRE New York is slated to test) and for Sequoia's AVC Advantage (which is also the model New York will be testing) revealed numerous flaws. [58] The printers ran out of paper too fast, lacked concealed printer cables, and had problems alerting poll workers to malfunctions. These were all printers presumably of the highest quality since they were provided by the vendors for use with their DREs.

Both the Sequoia and Avante model DREs New York is planning on testing permitted voters to cast votes without producing a paper record. This malfunction occurred under a number of scenarios, essentially rendering these DREs that are required to have a paper trail, into paperless DREs.

As set forth at p 44, given all we now know about these unverifiable, theft-creating opportunities, the fact that in 2007 New York is still planning on using any DRE in our elections is beyond shameful.

Past Performance Failure: Security Flaws in Avante's Voting System

On June 15, 2007, I sent Commissioner Kellner a copy of the State of Pennsylvania's 2005 state exam rejecting the Avante DRE New York is planning on testing. [59] Commissioner Kellner forwarded that report to various people at the SBOE. Michael Shamos, a supporter of DREs, examined the Avante Vote-Trakker EVC308 SPR (EVC) for the Commonwealth of Pennsylvania.

Certification was denied because the DRE exhibited confusing behaviors such that the voter may not be able to understand and interact with the voting system; the write-in function allowed for the same candidate to be written in more than once for the same office; the system was unable to accurately tabulate the votes; the system did not comply with the straight-party voting provision of Pennsylvania's Code in that the voter has to first make a straight-party selection, then go back and deselect the candidate before choosing a candidate of another party; the system wasn't equipped to generate a zero tape; and the tracking number on the VVPAT allows individuals to identify the ballot.

Pennsylvania is a state that has been using DREs for many years. I must presume that the concerns enumerated in the Pennsylvania report are shared concerns of New York. To the extent these concerns remain unchanged, it should be unnecessary to test this already rejected DRE.

A final note on DREs. New York is scheduled to test three DREs: Avante, ES&S and Liberty). DREs have shown themselves to be a colossal disaster and as the documented evidence suggests, DREs are on their way out. For New York to even be considering using DREs at this late date is highly irresponsible. Aside from their failure rates, there is no way to verify that any vote was counted as cast or that an election was honestly run. There is nothing to observe and nothing to recount that can't be tampered with without detection. Even with a VVPAT, studies show that an adequate proportion of the voters don't check the VVPAT in detail such that discrepancies might be detected [60] and that even if voters were to check the VVPAT, both the paper trail on a DRE and the electronic tally can be rigged such that both would agree and both could be wrong. [61]

The Carter Baker report (referred to at endnote 19) had also found:

> *DRE software can be modified maliciously before being installed.*
> .....

If DREs can be manipulated.....the same can be done with paper audit trails

Finally, the report of the federal government's technical advisors, the National Institute of Standards and Technology (NIST)[62] found DREs:

...are vulnerable to errors and fraud and cannot be made secure.

The DRE provides no independent capability to detect whether fraud has not caused errors in the records..... a single... programmer ...could rig an entire statewide election.

The NIST research staff further stated that they:

do not know how to write testable requirements to satisfy that the software in a DRE is correct.

Conclusion

A reasonable interpretation of the State Finance Law and the Vendex rules should prohibit the State's entering into contracts with any of these voting vendors on the myriad of grounds set forth herein. The documented evidence provided in this memo, as well as in the article from Voters Unite referred to at footnote 1, entitled *Voting System Companies Fail to Meet New York State's Requirements for "Responsible Contractors"*, as well as the additional evidence available to the SBOE when it undertakes its investigation of these vendors, overwhelmingly establish these vendors ineligibility to do business in New York.

The issue of the constitutionality or propriety of privatizing elections is not the subject of this paper and while the issue does not need to be reached for New York to conclude that these vendors do not qualify as responsible contractors, I wish to offer the following observation.

One of the problems that becomes apparent from this type of examination of the vendors is that privatizing the electoral process results in a state's loss of control over the method and means of holding elections, thereby depriving its citizens of their right to safe, secure and reliable elections. The vendors not only claim proprietary rights to conceal essential information from the public, but because the vendors insist on this level of secrecy and control, the state becomes dependent on these private entities to run their elections. No longer can public officials be understood to be meaningfully accountable to the people given their ignorance of the vendor's voting system. No public official can independently say with any assurance that the election was fair and

honest. Nor can the public verify the results of the election.

New York must be free to abide by the rich democratic history in which the rights of citizens to oversee and monitor their elections, enabled by the State's providing the necessary transparency, has historically been recognized, respected and upheld as constitutionally required. This is rendered impossible when a state contracts with a private vendor asserting confidential proprietary rights, even a vendor who would otherwise be considered eligible to contract with New York. Secret proprietary rights prevent the very oversight and accountability citizens are entitled to.

Transparency and accountability are the life blood of a democracy. This is indeed consistent with the legislative declaration contained in New York's Public Officers Law, § 84:

> *The legislature hereby finds that a free society is maintained when government is responsive and responsible to the public, and when the public is aware of governmental actions. The more open a government is with its citizenry, the greater the understanding and participation of the public in government.*
>
> *The people's right to know the process of governmental decision-making and to review the documents and statistics leading to determinations is basic to our society.* ***Access to such information should not be thwarted by shrouding it with the cloak of secrecy or confidentiality.***
>
> ***The legislature therefore declares that government is the public's business and that the public, individually and collectively and represented by a free press, should have access to the records of government in accordance with the provisions of this article.*** (emphasis supplied)

It makes a mockery of our law, our values and our revolutionary heritage if we insist that government be open and accountable and transparent, but permit the means of choosing that government to be closed and concealed; the right to information as to how the elections are run and our votes counted, " *thwarted by shrouding it with the cloak of secrecy or confidentiality".*

> *A popular Government without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy or perhaps both. Knowledge will forever govern ignorance, and a people who mean to be their own Governors, must arm themselves with the power knowledge gives."*
> – James Madison

Governor Spitzer has made ethics reform and open government the hallmark of his governorship. This reflects our foundational understanding that governments exists by will of the people and its legitimacy is derived from elections people trust. As the Governor reminded us in his 2007 State of the State speech:

> *We are in danger of losing the confidence of those who elected us. To restore their confidence, we must overhaul our campaign finance, lobbying and election laws.*

No amount of open government, access to information and a free press can compensate for elections which are closed from public observation and oversight. The information about how computers are programmed to process, count and tabulate the people's vote cannot be concealed from the public in a democratic society. And yet, that is precisely what happens when elections are outsourced to private companies asserting secret proprietary rights to the very information that *belongs* to the people.

We cannot trust what we cannot see; and faith has no place in our secular republic. Votes counted within the guts of a computer are hidden. How that computer is programmed is only the beginning of the information the people need to maintain their hold over their public servants. Only a citizen-owned process can legitimize government through the consent of the governed.

These private voting vendors made a choice to build voting systems using Microsoft's proprietary software, and to insist on their own proprietary rights to the information about the voting systems they've created. These systems have no place in a free society. There is an inherent conflict which cannot be resolved when private interests are permitted to invade our democratic public elections. Indeed as the Code of Ethics of the Public Officers Law proclaims:

> *....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, Declaration of Intent § 74

The consequence of inviting private vendors, with their claimed entitlement to trade secrecy, to participate in our elections is both a fatal ethical violation and spells the end of democracy. The official duties of running a democratic election rely on the very ethical conflict NYS is required to avoid: NYS election officials are forced to depend on private vendors and their concomitant self interests.

It is not surprising that this conflict between private interests and a state's official duties in service to the people has been a huge problem for the nation that has permitted the privatization of their elections and is already a problem for New York as it proposes to embrace this irreconcilable conflict.

The example of North Carolina referred to earlier, is instructive of the very problem New York is dealing with now as vendors fight to rewrite New York's laws in their interests or appeal to the SBOE to relax its interpretation of our laws such that their machines pass certification and our constitutional rights are disregarded. The handwriting is on the wall and the stage set, should New York choose to ignore these lessons or its constitutionally imposed responsibilities.

In the closing week of the legislative session of the New York Legislature we were given a taste of this conflict and the arrogance of vendors trying to force New York to adapt its law to the vendors' needs. In order to accommodate Microsoft's interests and the needs of those vendors who choose to rely on Microsoft's products, Microsoft wrote legislation to amend New York's existing law and tried to have that slipped into some bill during the chaos of the final week.

Why should Microsoft be permitted to do this? The voting vendors aren't required to use Microsoft's software. The vendors are free to use open source software. These vendors chose to use software that renders them unable to comply with New York's laws. Of the systems New York plans to test, Avante's and Sequoia's DREs rely on MS Windows operating systems and Diebold, ES&S and Liberty, as well as Avante and Sequoia, all rely on Microsoft for their election management systems (EMS)[63]. As demonstrated in the various security reports cited in this memo, the EMS has been implicated in many of the election problems, including the opportunity for fraud.

The public response to Microsoft's efforts to rewrite our law brought the required openness and sunshine to bear. 3,000 New Yorkers called their representatives alerting them to be on the look out for the Microsoft amendment. The vendors' campaign to put private needs before democratic requirements will continue in other venues. They cannot be permitted to succeed in New York.

What was perhaps not apparent to the rest of the nation when they allowed the privatization of their elections and accepted the surrender of control to corporations asserting proprietary rights over the very information citizens need to prevent their disenfranchisement, is very clear now. New York cannot close its eyes to this conflict between the rights of its citizens to be able to verify their elections and the private corporate interest in secrecy. For all of the reasons stated herein, New York cannot

enter into contracts with any of the private vendors offering privately controlled, proprietary equipment.

There are alternatives available to New York that would protect this fundamental right of citizens in a democracy. That being New York's primary responsibility, this is precisely why New York cannot delegate its duty to conduct democratic elections to private corporations that control and conceal information the people must have if they are to fulfill their duties and responsibilities as citizens of a democracy. Conducting our elections with paper ballots and hand counting those ballots in an open, transparent and secure way, is the best means of providing free and fair elections. It is also HAVA-compliant, so long as we provide a means for the disabled to vote. Another alternative would be the use of New York state controlled, non privatized, open source optical scanners combined with the release of all ballot images, allowing the public to examine the physical ballots, as well as a partial hand count [64]to check the optical scanners' accuracy. (See my Memo II, *Alternative Voting Systems that are HAVA-compliant, NYS-compliant and Democracy-compliant).*

New York is the only state that has not permitted the privatization of its elections. We must lead the nation back to it fundamental democratic roots. We must insist that our elections remain open and transparent and accountable to the people or lose our right to be self-governing.

"If a nation expects to be ignorant and free ... it expects what never was and never will be."
-- Thomas Jefferson

ENDNOTES

1. New York State Procurement and Disbursement Guidelines, Bulletin No. G-221, http://www.osc.state.ny.us/agencies/gbull/g221.htm

2. http://www.votersunite.org/info/messupsbyvendor.asp

3. Much of the information which comprises the sordid history of how the three major voting vendors came to be is with grateful thanks and acknowledgment to Bev Harris, see her book Black Box Voting:Ballot Tampering in the 21st Century.

4. http://www.votetrustusa.org/index.php?option=com_content&task=blogcategory&id=77&Itemid=171

5. http://www.miamidadeig.org/annual%20reports/2003%20printable.pdf

6. http://www.commondreams.org/views03/0902-01.htm

7. http://www.bradblog.com/?p=4321
Excerpts from the letter in which ES&S attempts to direct the "independent" audit of ES&S's source code

and machines:

* No statements about "potential" situations
* No statements that discuss what "might" have occurred
* No statements about possible "vulnerabilities"
* No statements about the "style" of the source code
* No statements commenting on the use of less desirable techniques, instructions, or constructs
* No statements rendering opinions on proper uses, improper use, or correctness of source code
* No statements rendering opinions on security techniques employed or not employed
* No statements discussing relevance of any discoveries made in this review to any elections or contests outside the 2006 Sarasota General Election, U.S. House of Representative District 13 race.
* No statements regarding conformance to source code standards of any type or kind

8. http://news.com.com/8301-10784_3-6136123-7.html?part=rss&tag=2547-1_3-0-20&subj=news

9.http://www.bradblog.com/?p=4784

10. http://www.votersunite.org/info/ES&Sinthenews.pdf
see also Election Log for problems with ES&S for 2006/2007, reporting 99 incidents of ES&S machine failure reported in the media:
http://www.votersunite.org/electionproblems.asp?sort=date&selectstate=ALL&selectvendor=ESS&selectproblemtype=ALL
and for problems reported in the media on all machines, beginning in 2004:
http://www.votersunite.org/electionproblems2004plus.asp?sort=date&selectstate=ALL&selectproblemtype=ALL

11. **Unity EMS --March 2004 Unity Election Management Software** (p13 of Voters Unite partial list of failures)

Bexar County, Texas. Misprogramming causes the **Unity software to balk at accumulating votes from the optical scan machines** used to count absentee ballots.

Tabulation of the Bexar County votes was delayed for about 1 1/2 hours, beginning about 8 p.m.

– "They have big problems," said Nick Peña, a poll watcher for District 28 U.S. Rep. Ciro Rodriguez,D-San Antonio. "They look very worried."

– "They have a bunch of technicians in the tabulation room, and they are pulling out wires and reattaching them, and the computer screens are all frozen. You can tell that something is happening,"Peña said.

July 2004 Unity election management software (p 20 of partial list of failures)

All U.S. Counties that use ES&S voting systems. **More and more bugs surface in the ES&S software, but only in response to public records requests.**

In a June 3 letter to ES&S, obtained by The Herald in a public records request, Miami-Dade County Supervisor of Elections Constance Kaplan demanded answers to three problems with the iVotronic equipment that she said could take "labor intensive and costly" actions to fix. She asked ES&S to resolve these issues "expeditiously:"

♦ The central database machines used to tabulate votes are incapable of holding all the audit data at once, requiring a "labor intensive and costly" solution that could complicate a recount in a close race. Audit

data is used to back up the system.
♦ The optical scanners used to read absentee ballots have problems when information is merged from the three machines the county uses.

The response from ES&S: Fix it yourself by changing your election procedures to work around the bugs. (my emphasis- as it pertains to ES&S's sense of 'responsibility' and "integrity , required by NYS Law.)

ES&S Senior Vice President Ken Carbullido responded to Kaplan on June 14, noting that each of the problems could be resolved if the county alters its procedures, reconfigures its software or, if it wants to transmit data from the polling places, redo the programming code in the machines or retrain its staff

_____

August 2004 Unity Election Management System (p 21of partial list of failures)

Natrona County, Wyoming. The **Unity Election Management System, used to tally votes from both optical scan machines and paperless electronic voting machines, failed to tally votes correctly.**

Noticing that the totals for the city of Evansville seemed low, Natrona County Clerk Mary Ann Collins checked the printouts from the precinct voting machines in Evansville and found that the **totals didn't match the totals computed by the Unity software,** which combines all the totals countywide.

_____

November 2004 Unity 2.2 (p 27 of partial list of failures)

Guilford County, North Carolina. ES&S early voting machines had capacity problems, which affected anywhere from 6,000 to 20,000 ballots. The totals were so large, the **tabulation computer threw some numbers away.** Retallying changed two outcomes and gave an additional 22,000 votes to Kerry.

The biggest change in vote totals outside Mecklenburg was in Guilford County, which includes Greensboro. The computer that tabulates the totals choked when officials uploaded the early voting numbers, which was a particularly large batch of data.

"So it just threw some of (the votes) away," said Guilford County elections director George Gilbert.

The Guilford totals didn't change President Bush's win in the state, but did shift the vote total by 22,000.

In a letter to Guilford County, Ken Carbullido, Vice President of ES&S Product Development, explained in very technical language that **when the vote totals reached 32,767 (32K), it began subtracting from the totals. This same problem occurred in the 2004 general election in Broward County had.**

The 32,767 capacity limitation at a single precinct level is a function of the design and definition of the results database used by ERM. The data storage element used to record votes at the precinct level is a two byte binary field. 32,676 is 2 to the 15th power, which is the maximum number held by a two byte word (16 bits) in memory, where the most significant bit is reserved as the sign bit (a plus or minus indicator). Additionally, ERM precinct count level data is stored in a binary computer format known as two's complement.....

In the letter, Mr. Carbullido **admitted they knew about the problem but had not advised the county.** (My emphasis, again relating to ES&S's sense of 'responsibility' and "integrity" , required by NYS Law.)

_____

November 2004 Unity 2.2 (p 28 of partial list of failures)

Orange County, Florida. Among the election equipment foul-ups in Florida, **vote tabulating software reached its 32,767 capacity and began counting backwards.**

The cause of the error, Orange officials said Thursday, was a **software program that could not tabulate more than 32,767 votes in a single precinct**. On election night, officials anticipated the problem and adjusted for it, deputy election official Lonn Fluke said Thursday.

_____

November 2004 Unity 2.2 (p 28 of partial list of failures)

Broward County, Florida. A **software flaw** cause Broward County officials to initially report an inaccurate outcome for Amendment 4.

"The **software is not geared to count more than 32,000 votes in a precinct. So what happens when it gets to 32,000 is the software starts counting backward**," said Broward County Mayor Ilene Lieberman.

_____

November 2004 Optical scan and Unity (p 33 of partial list of failures)
Grays Harbor, Washington. Elections officials started recounting about 28,000 ballots on Tuesday after the **ES&S Unity reporting system showed too many votes**.

[County Auditor Vern] Spatz said unusually high turnout aroused suspicion that something might be wrong. On Monday, Grays Harbor County was reporting 93 percent turnout, much higher than anywhere else in the state. Officials checked the system and found the problem.

After ballots were counted, the results were saved on computer disks and downloaded into another computer to keep a running tally. Some of the disks were apparently downloaded twice by mistake, Spatz said.

The recount changed the outcome of the Governor's race in Grays Harbor County.

VotersUnite contacted Mr. Spatz and mentioned that **ES&S optical scanners had double-counted ballots in other states during the November election**. **He was surprised and interested. He was also concerned because ES&S Unity Election Management software is supposed to prevent cartridges from being downloaded twice**. (My emphasis)

_____

May 2006 Optech Eagles, Unity Election Management System, iVotronic printers (p 48 of partial list of failures)
Pulaski County, Arkansas. ES&S election software malfunctions, and ES&S programmed the ballots incorrectly.

[County attorney Karla] Burnette said the problems were two-fold, resulting from a malfunctioning opening and closing system of the electronic voting machines and mistakes in programming.

“The machines were programmed by precincts instead of polling sites. We have several precincts that go to the same polling site,” Burnette said. “The system did not know where to put those votes. The software couldn’t recognize those votes.”

Optical scan machines, referred to by election officials as “Eagles,” also **malfunctioned because of malfunctioning Unity Software** for the iVotronic electronic voting machines, supplied by ES&S.
A recount is required, and that, too, presents problems because of machine malfunctions.

The iVotronic paper tapes, that record the votes, will have to be unrolled and manually examined and counted.

12. Quotation is from the NYS Procurement Best Practices

13.The New Standard, http://newstandardnews.net/content/index.cfm/items/3180/printmode/true

14. http://evote-mass.org/Shamos_Security_Report.pdf
From the Voting System Security Review prepared for the Secretary of the Commonwealth of Massachusetts by Michael Shamos, September 28, 2006, emphasis supplied.

ES&S Unity 3.0.1.0. *Is a suite of* ***Windows XP programs*** *used to set up, manage and tally an election. Its components are written in various languages, including C, C++, VisualBasic, Java18 and COBOL. The master distribution disk for Unity is created during a witness build procedure by the ITA at ES&S offices in Omaha. It is not necessary to rely on the vendor for copies of the certified software, which can be obtained by authorized parties from the ITA.*

Unity *for Massachusetts and AutoMARK includes these components.* ***All are Windows applications****.*
• Election Data Manager (EDM). This is used for election setup and ballot definition.
• Ballot Image Manager. There are several image manager programs to format ballots for different devices. The relevant one for optical ballots is Ballot Image Manager.
• Hardware Programming Manager(HPM). This formats and burns media for use in the Optech.
• Election Reporting Manager (ERM). This is a tabulation program for unofficial results that offloads results from media to obtain vote totals from scanners.
• Audit Manager. A program to inspect event logs.
AIMS and Unity can run on the same computer, in which case files created by Unity are simply read by AIMS. If they are running on different computers, transfer of files is needed.

Unity Security (from page 43-43 of the reported security review)

Because Unity is a Windows application, it is difficult to maintain it and its data in a secure manner. *There is no real control over who may gain access to the laptop on which it runs, although certain physical security measures, such as keeping it locked in a safe when not in use, would help, along with administrative security means such as login passwords.*

Possibly for historical reasons, the Unity files vary greatly in their resistance to attack. For example, a result of running EDM is the creation of a file name Candidat.DBF in the election database. While it was not feasible ***to modify this file*** *using Notepad, it* ***was easy using a copy of Microsoft Access. We opened the file, changed the name of a candidate from "Sherry Smith" to "Sherry Jones," and closed the file. This modification was done outside Unity. The next time Unity was run, "Jones" had replaced "Smith" with no complaint from the software. This could be remedied by password-protecting the database or (better) by encrypting it.***

While the ability to modify election database files is disconcerting, it is not fatal. The reason is that the proper marking of ballots is verified at LAT and during the election by poll workers and voters. Any modification of database files before the election will be caught through diligent review. The next question is what night happen in Election Reporting Manager if votes for A are reported as votes for B through an intrusion into the database. The answer is confusion for a time but without permanent effect. The totals produced by ERM would not match the individual results produced at the polling location, and

the original optical ballots are available for manual or machine recount.

A continuing problem with Unity, which ES&S has not shown any inclination to correct, is that it offers a plethora of ballot setup options which even the vendor's representatives are unable to explain. If a jurisdiction uses Unity on its own, the possibility of setting up an illegal election is significant. The vendor counters that these operations are generally performed by experts who know what they are doing, but no such person has appeared at any examination I have conducted.

Unity's log files are unprotected and can be modified easily using Windows accessories. In Notepad, for example, it was easy to change the login ID of a person performing an operation or delete a log entry entirely*. Unprotected logs have some utility but are not effective against deliberate intrusions.* ***In Unity it is possible to insert or alter unofficial vote totals manually****.* ***These operations are logged. However, it is possible to modify the logs to eliminate any trace of the modification, making it impossible to audit the election or explain irregularities.*** *I did not find it possible to alter results files outside of Unity without corrupting the files. Therefore, if the log files were subject to the same level of protection the possibility of an unnoticed alteration would be reduced significantly.*

Unity security (from p 51): ***Unity provides insufficient security for election and log files. they are too easy to modify outside Unity using Windows.***

15. Robert F. Kennedy Jr's, **Will the Next Election Be Hacked**,
http://www.rollingstone.com/politics/story/11717105/robert_f_kennedy_jr__wil

The voting-machine companies bear heavy blame for the 2000 presidential-election disaster. Fox News' fateful decision to call Florida for Bush - followed minutes later by CBS and NBC - came after ***electronic machines in Volusia County erroneously subtracted more than 16,000 votes from Al Gore's total****. Later, after an internal investigation, CBS described the mistake as "critical" in the network's decision. Seeing what was an apparent spike for Bush, Gore conceded the election - then reversed his decision after a campaign staffer investigated and discovered that Gore was actually ahead in Volusia by 13,000 votes.*

Investigators traced the mistake to Global Election Systems, the firm later acquired by Diebold. Two months after the election, an internal memo from Talbot Iredale, the company's master programmer, blamed the problem on a memory card that had been improperly - and unnecessarily - uploaded. "There is always the possibility," Iredale conceded, "that the 'second memory card' or 'second upload' came from an unauthorized source."

As Kennedy also points out with regard to all elections and all vendors:

The United States is one of only a handful of major democracies that allow private, partisan companies to secretly count and tabulate votes using their own proprietary software. *Today, eighty percent of all the ballots in America are tallied by four companies - Diebold, Election Systems & Software (ES&S), Sequoia Voting Systems and Hart InterCivic. In 2004, 36 million votes were cast on their touch-screen systems, and millions more were recorded by optical-scan machines owned by the same companies that use electronic technology to tabulate paper ballots.* ***The simple fact is, these machines not only break down with regularity, they are easily compromised - by people inside, and outside, the companies.***

Three of the four companies have close ties to the Republican Party. *ES&S, in an earlier corporate incarnation, was chaired by Chuck Hagel, who in 1996 became the first Republican elected to the U.S. Senate from Nebraska in twenty-four years - winning a close race in which eighty-five percent of the votes were tallied by his former company.*

16. Harri Hursti, "SECURITY ALERT: July 4, 2005, Critical Security Issues with Diebold Optical Scan Design", BlackBox Voting, *available at:* http://www.blackboxvoting.org/BBVreport.pdf

17. "Election Whistle-Blower Stymied by Vendors", Washington Post, Mar. 26, 2006 http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500805.html

18. See New York Times, May 12, 2006 New Fears of Security Risks in Electronic Voting Systems, http://www.nytimes.com/2006/05/12/us/12vote.html?ei=5090&en=5b3554a76aad524a&ex=1305086400&partner=rssuserland&emc=rss&pagewanted=print

19.Carter Baker Report, http://www.american.edu/ia/cfer/

20. More E-voting Concerns Surface with State Primaries Underway http://newstandardnews.net/content/index.cfm/items/3180,
"Cold Shoulder for E-voting Whistleblowers", The New Standard, May 17, 2006 http://newstandardnews.net/content/index.cfm/items/3181

21. Harri Hursti, "SECURITY ALERT: May 11, 2006, Critical Security Issues with Diebold TSx", Black Box Voting, *available at:* http://www.blackboxvoting.org/BBVtsxstudy.pdf

22. http://arstechnica.com/news.ars/post/20051223-5831.html

See also the litigation papers in the Diebold, North Carolina cases: http://www.eff.org/Activism/E-voting/diebold_v_nc.php

23. Deibold's History in California: Misrepresentation, System Failure, Decertification and Security Vulnerability, http://voteraction.org/States/California/Documents/Information/dieboldhist.html .

California's SOS issued a **report highly critical of Diebold for its deceptive practices and dishonesty to state officials**. In April 2004, citing Diebold's misconduct, the SOS decertified Diebold's AccuVote-TSx machines.

24.http://www.votersunite.org/info/Dieboldinthenews.pdf
See also Election Log of Diebold machines for 2006/2007 listing 50 examples of machine malfunctions on Diebold machines that were reported in the media http://www.votersunite.org/electionproblems.asp?sort=date&selectstate=ALL&selectvendor=Diebold&selectproblemtype=ALL
See also full Election log of voting/machine problems reported in the media beginning in 2004 http://www.votersunite.org/electionproblems2004plus.asp

25. http://truevotemd.org/images/stories//diebold_pa_response.pdf

26. The Rubin Report, http://avirubin.com/vote.pdf

27. RABA TECHNOLOGIES LLC. TRUSTED AGENT REPORT: DIEBOLD ACCUVOTE-TS VOTING SYSTEM (report prepared for Department of Legislative Services, Maryland General Assembly, Annapolis, Md., January 2004) http://www.raba.com/press/TA_Report_AccuVote.pdf

28.California Security Analysis of the Diebold Accu Vote Optical Scanner and the touchscreen, http://ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf

29. University of Conn. Diebold Security Report, http://voter.engr.uconn.edu/voter/Reports.html

30.U Conn VoTeR center report: Diebold AV-OS is vulnerable to serious attacks http://avi-rubin.blogspot.com/2006/10/uconn-voter-center-report-d iebold-av-os.html

31.http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk3MTYyNTQwJnlyaXJ5N2Y3MTdmN3ZxZWVFRXl5Mg

32. Sequoia E-Vote Systems Found 'Hackable' in PA, Testing Shut Down After Machine Failures! http://www.bradblog.com/?p=2628

33. More Glitches Trigger Halt in Testing of New County Voting Machines, Post-Gazette, Harrisburg Bureau, March 30, 2006, http://www.post-gazette.com/pg/06089/678087-85.stm

34. SEQUOIA TOUCH-SCREEN VOTING MACHINES HACKED, FOUND VULNERABLE TO VOTE-FLIPPING BY PRINCETON UNIVERSITY! http://www.bradblog.com/?p=4141

From http://www.cs.princeton.edu/~appel/avc/:

I was surprised at how simple it was for me to access the ROM memory chips containing the firmware that controls the vote-counting. Contrary to Sequoia's assertions in their promotional literature, there were no security seals protecting the ROMs. Indeed, I found that certain information in the "AVC Advantage Security Overview" (from Sequoia Voting Systems, Inc., 2004) was untrue with respect to my machine. Sequoia's document states,

> "The vote counting instructions in each voting machine are written into integrated circuit chips during the manufacturing process. These chips are incorporated into each machine's circuit boards. Access to the machine should be limited by administrative procedures and is also limited by the physical design of the machines. Design features include door locks and a numbered seal on the CPU cover."

I found this to be incorrect, with respect to the machines delivered to me. I did not have to remove any seals, whether of tape, plastic, or wire. The sheet-metal panel covering the computer circuit board is the only component I found that could possibly be described as a "CPU cover", and it had no numbered seal. (If there ever was a numbered seal holding the CPU cover down, then Buncombe County's technicians would have to remove it and replace it every time they change the four AA batteries on the motherboard!)

The AVC Advantage can be easily manipulated to throw an election because the chips which control the vote-counting are not soldered on to the circuit board of the DRE. This means the vote-counting firmware can be removed and replace with fraudulent firmware. Under the sheet-metal panel (the "CPU cover"), I found the circuit board containing computer chips, other electronic chips, and four chips that--unlike most of the chips on the circuit board which are soldered in place--are mounted in sockets so that they can be removed and replaced. These are ROM (read-only memory) chips that hold

the computer program (firmware) that operates the voting logic. **These chips are not held in place by any seals. They can be removed using an ordinary screwdriver and they** (or other ROM chips containing other firmware) **can be replaced simply by pressing them into place**. You can see the ROM chips in the picture above; they have the white labels pasted onto them, and you can see me in the process of prying one loose with a screwdriver.

Like the purchasers of all the other lots sold by Buncombe County, I am now at leisure to examine the contents of the firmware on the ROM chips, and to modify it. If I had the inclination to cheat in an election (which I do not) I **could prepare a modified version of the firmware that subtly alters votes as the votes are cast, with no indication of the alteration made visible to the voter**. I would write this modified firmware onto new ROM chips. Then, if I had access to one of New Jersey's voting machines (for example, in an elementary school or firehouse where it is left unattended the night before an election), I could open the door of the machine, unscrew 10 screws, replace the legitimate ROM chips with my own fraudulent ones, reinstall the cover panel with its 10 screws, and close the door of the machine.

35. http://www.votersunite.org/info/Sequoiainthenews.pdf
See also Election Log of Sequoia machines for 2006/2007 listing 38 examples of machine malfunctions on Sequoia machines that were reported in the media
http://www.votersunite.org/electionproblems.asp?sort=date&selectstate=ALL&selectvendor=Sequoia&selectproblemtype=ALL
See also full Election log of voting/machine problems reported in the media beginning in 2004
http://www.votersunite.org/electionproblems2004plus.asp

36. Summary Report on New Mexico State Election Data. December 12, 2004. by Ellen Theisen and Warren Stewart. http://www.votersunite.org/info/NewMexico2004ElectionDataReport-v2.pdf ,
Undervote Rate Plummets 85% in New Mexico's Native American Precincts after Statewide Switch from Touch-Screen Voting to Paper Ballots, http://www.bradblog.com/?p=4193

37. HERE WE GO AGAIN: 'Just Push the Yellow Button and Vote as Many Times as You Want' on Sequoia Touch-Screen Voting Machines! http://www.bradblog.com/?p=3714

38.http://www.votetrustusa.org/pdfs/LibertyVoteCritique.pdf

39. First Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System, April 2004, http://www.cev.ie/htm/report/first_report.htm
Second Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System, July, 2006 http://www.cev.ie/htm/report/download_second.htm

40. Full Security Analysis Report on Nedap DRE,
http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

41. http://www.nyvv.org/newdoc/tcsd/NYSBOEGroenendaal042607.pdf, Voting Integrity Group Calls For Investigation of Liberty/Nedap, Voting Integrity Project Press Release April 26, 2007
http://www.nyvv.org/newdoc/tcsd/SCPPressRelease042707.pdf

42. Vendors Try an End Run Around NYS Election Law, http://nyvv.org/blog/2007_o4_01_archive.html

43. Public Materials from Troy City School District and Liberty Elections Systems**,** Troy City School District Press Release of 4/11/2007, http://www.nyvv.org/newdoc/tcsd/TCSD_PressRelease041107.pdf ,
http://www.troy.k12.ny.us/BoardofEd/LibVote6TroySm.pdf , Archive Copy of Liberty/Nedap/Troy Brochure

http://www.nyvv.org/newdoc/tcsd/LibVote6TroySm.pdf, NYVV Refutes Liberty/Nedap/Troy Brochure Misstatements, http://www.nyvv.org/newdoc/tcsd/RebuttalLibertyBrochure.pdf

44.LibertyVote/Nedap DRE:Dutch Group Successfully Hacks Nedap DRE http://votetrustusa.org/index.php?option=com_content&task=view&id=1850&Itemid=51

45. http://www.theregister.co.uk/2007/03/1704/foi_dutch/

46. http://www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal

47. http://www.heise.de/english/newsticker/news/print/79106

48. http://www.electricnews.net/print/9733904.html

49. Usability Concerns About the LibertyVote/Nedap DRE:Three Major Problems with the LibertyVote/Nedap DRE, http://www.nyvv.org/newdoc/tcsd/Liberty_VVPAT_Issues.pdf

50. Review- Second Report of the Irish Commission on Electronic Voting, http://www.mcdougall.org.uk/VM/ISSUE23/I23P4.pdf , see specifically sec. 8 entitled VVAT.

51. http://www.theregister.co.uk/2005/02/04/ireland_evoting_bill/

52.http://electricnews.net/article/9828620.html

53. IES or Integrated Election Software are referred to in the report as the same as what we refer to only as election management software (EMS), performing the same function.

54. Open Voting Solution (OVS) produces and open source optical scanner (see Memo II, entitled *Alternative Voting Systems that are HAVA-compliant, NYS-compliant and Democracy-compliant*) and had been attempting to obtain certification in 2006. When notified by the SBOE that New York's law required the escrowing of all source code, OVS undertook the revision of a great deal of source code to comply with New York's requirement. OVS had used open source software for much of their product, but because it had used Oracle in its voting system and Oracle would not escrow the source code, OVS removed all code dependent on Oracle and substituted an open source database. Thus OVS was the only vendor who respected New York's Law.

55. http://www.nyvv.org/newdoc/RGleimEmail062007.pdf

56. See Avante's (Not Very Good) Offer to New York Voters, http://www.opednews.com/maxwrite/print_friendly.php?p=opedne_andi_nov_070712_avante_s__28not_very_g.htm

57.http://www.usenix.org/events/evt06/tech/full_papers/herrnson/herrnson_html/

58. Test Reports prepared by the New Jersey Institute of Technology, July 2007 for printers attached to the DREs of theAvante DRE Vote-Trakker EVC308-FF http://www.state.nj.us/lps/elections/Hearing-Reports-7.07/NJIT-Avante-report-7.07.pdf and the Sequoia AVC Advantage http://www.state.nj.us/lps/elections/Hearing-Reports-7.07/NJIT-Advantage-report-7.07.pdf

59. AVANTE_PA_EXAM_072005.pdf

60. A 2005 study by the Caltech-MIT Voting Project, http://www.vote.caltech.edu/media/documents/wps/vtp_wp28.pdf , concluded the following:

no errors were reported in our post-survey data ... ... and over 60 percent of participants indicated that they were not sure if the paper trail contained errors.

See also Bruce O'Dell's referring to the Caltech study:

> *That's right: in test elections full of deliberately engineered VVPAT errors - including swapped votes and even missing races - no one reported a VVPAT error while voting, a majority were unsure whether there were any errors or not, and almost a third of the participants continued to insist that there no errors at all even after they were told otherwise by those who switched the votes.* Pull the Plug on E-Voting & Pull the Plug on E-Voting, Part 2:
>
> And as a recent paper, http://chil.rice.edu/research/pdf/EverettDissertation.pdf, reveals:
>
> *[A]s the situation currently stands, voters cannot be depended upon to check the validity of their vote. Many security experts and election reform groups are calling for VVPATs to be required on all DREs and as of the 2006 elections, nearly half of the states mandated that their DREs have paper trails (electionline.org, 2006). However, these studies show that solutions to DRE security problems that require voter verification of their ballots may not solve vote-flipping problems. Users are not even checking their ballots on the review screen that is presented directly in front of them.*
>
> *The findings here suggest that it is highly unlikely that voters will detect changes to their ballots on the VVPAT that prints out on a roll of paper next to the machine if they are not even noticing them on a screen presented directly in front of them.*

61. Technology Review: How to Hack an Election in One Minute: Princeton U. researchers have released a study and video that demonstrate the ease of altering votes on an electronic voting machine, http://www.technologyreview.com/Infotech/17508/?a=f And see the study at http://itpolicy.princeton.edu/voting/ts-paper.pdf

62.http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf

63. The election management systems (EMS) contain administrative functions, but they also contain the vote tabulation software. At endnote 14 numerous problems attributable to the ES&S EMS were identified including the potential for fraud in the vote count. The RABA report, endnote 27, found that because Microsoft lacked critical security updates, the team examining the system could upload malicious software into the EMS and modify or delete elections! The reports from the Irish Commission, endnote 39, found the EMS so vulnerable as to require a complete replacement before they would consider using the Nedap/Liberty DREs.

64. *Landslide Denied,*
http://www.electiondefensealliance.org/landslide_denied_exit_polls_vs_vote_count_2006

> The report describes the specific means of effectively conducting a public hand count of 10% of the paper ballot records in 100% of the precincts in federal and statewide races. The UPS is to be conducted "in-precinct" on election night, by citizens representing all concerned political parties, and open to general public observation. Because it is conducted in-precinct, the UPS avoids the difficult task of protecting the chain of custody of paper ballot records in 180,000 U.S. precincts. In fact, all the alternative after-the-fact "spot-audit" schemes impose this monumental burden – since in all those protocols, all precincts must safeguard ballot records until just a few percent are

"randomly chosen" some time after the election. Integrity of the chain of custody will be especially suspect, of course, in just those suspect elections which such audits are proposed to safeguard. Since a 10% hand-count sample would be drawn in 100% of precincts on election night, the UPS also eases the transition to decentralized, citizen-monitored hand-count verifications of elections, placing responsibility for the integrity of the vote count in the hands of the American people, where it rightfully belongs.

Most importantly, the UPS is inherently resistant to manipulation. The report describes how any attempt to systematically manipulate the UPS audit would be extraordinarily difficult to conduct and to conceal. Not only would it require a very large number of participants, any effort to skew the 10% paper hand count in favor of a candidate would be very likely to increase the overall discrepancy, not decrease it.

In order to restore and maintain citizen trust in the integrity of American democracy, it is critical that wherever electronic vote tallying is performed, paper ballot records must always be produced and must always be checked by the best possible "security mechanism" – the American people, working together in public.